
**GA2:** Social and Humanitarian

**Student Officer:** Giray Yılmaz

**Issue:** Regulating and developing the usage of facial recognition technologies in government surveillance

TIMUN '20

Turkish International Model United Nations

THIMUN Affiliated Conference

Committee: Social and Humanitarian Committee (GA2)

Issue: Regulating and developing the usage of facial recognition technologies in government surveillance

Student Officer: Giray Yılmaz – President Chair

# I. Introduction

Technological innovation is a prominent aspect of today's globalized world. To the general public, private enterprises -and their target-driven business models- motivated by fierce competition may seem to lead the way in technological advancement. However, throughout history, it has been repeated that some of the most seminal technological accomplishments and revolutionary inventions took place with the help of government activity within the technology/weapon industry. Perhaps the most obvious example of this phenomenon is the development of the world's first computer by the British engineer Tommy Flowers during World War II to decrypt Nazi ciphers (Lewin).

Today, similar to the very first computer, another technological advancement funded mainly by world governments is rapidly making its way towards our everyday lives. From unlocking your mobile phone to disease diagnosis, facial recognition technology is used in a spectrum of fields where the range of its applications are only getting wider each day.

The groundwork for facial recognition technology was laid by computer scientists Woody Bledsoe, Helen Chan Wolf, and Charles Bisson during the mid-1960s. Similar to the first computer, recognizing the great advantage a sophisticated facial recognition technology would provide, the American government invested a great number of resources in the development of facial recognition projects during the 90s and The Defence Advanced Research Projects Agency (DARPA) created the first database which was able to identify up to 800 people (Murooka).

Due to the very common nature of cameras in our daily lives from selfie cameras of our mobile phones to the traffic camera right around every street, today, facial recognition software has the most advanced infrastructure to record and store data in the form of the photo of a face. The ease of identifying people using facial recognition is unparalleled compared to any other method of surveillance. Therefore, many governments around the world have conducted, and are still conducting, research on the development of this technology.

This report will primarily focus on the use of facial recognition technologies in government surveillance in the United States and China because the former is the state in which the method first originated as a means of ensuring public security, and the latter is the state which most extensively utilizes facial recognition technology in Asia, the focus region of TIMUN '20.

The main dilemma surrounding the use of facial recognition technology as a government surveillance method can be summarized as a conflict between public security versus individual privacy. In addition to this, the argument that facial recognition technologies are an infringement upon people's right to assembly and the possibility of such systems being biased towards minority groups or certain ethnicities is what the advocates of banning facial recognition technology in government surveillance are commonly putting forward. These conflicts will be further elaborated on in the "Focused Overview of the Issue" section. While reading this report and thereafter drafting a resolution, delegates should look for solutions that not only develop the worldwide use of this technology to ensure public security but also do this under the umbrella of a multilateral regulatory framework that guarantees the personal privacy rights of individuals and the freedom to the assembly of civil society won't be infringed upon.

## II. Involved Countries and Organizations

### Office of the United Nations High Commissioner for Human Rights (OHCHR)

OHCHR is the main UN organization responsible for human rights. Its mission, as entrusted by the General Assembly (GA) is to indiscriminately promote human rights for all people. As the issue of facial recognition technologies (if left unregulated) leaves room for many human rights violations, the OHCHR takes a definitive stance regarding the matter. On June 25, 2020, the High Commissioner has said that "[facial recognition technologies] are being used to restrict and infringe on protesters' rights, to surveil and track them, and invade their privacy" (Colville). Based on this statement, it is clear that the High Commissioner and the OHCHR call upon all Member States to work collaboratively to form a regulatory framework for the usage of facial recognition technology in government surveillance.

### United States of America (USA)

Even though the United States is not located in the focus region of TIMUN '20, it is critical to the agenda item for several reasons. Firstly, as aforementioned, the use of this technology as a security measure originated in the US, which means that by far the US cabinet is the most experienced government with its use. Consequently, the use of technology in government surveillance has been common in the US during the past decade. On the contrary, some states including San Francisco, Somerville, and Oakland have passed regional laws that ban the use of the technology (Ghaffary). Although regional authorities are

showing commitment to the call for ending the technology's use, no federal law has yet addressed the issue. While both parties have their take on the issue, the federal government has taken great advantage of the legislative process slowing down due to party conflicts and the debate surrounding the ethics of facial recognition. Although the exact scale is unknown, many assume that the US government has been using the technology extensively over the past decade, and they will continue to do so until a regulatory framework is established or the practice is federally banned all around the country.

Secondly, establishing itself as the epitome of democracy and human rights on the international stage has been an essential aspect of the US foreign policy for more than a century; therefore, the stance the delegation will take on the issue of facial recognition in regards to possible infringements upon personal privacy will be very influential for the members of the United Nations (UN), especially for the ones that will be present in this committee. The absence of any federal law addressing the issue makes the stance of the US ambiguous. However, delegates must be reminded that whatever stance the US takes, its primary objective would most likely be in favor of multilateral cooperation between the Member States so that a possible solution to the issue at hand can be achieved.

### National Security Agency (NSA)

The NSA is the United States' intelligence agency under the Department of Defense that is responsible for communications and information in regards to national security matters. While the main focus of the NSA is foreign intelligence, the agency still has a strong infrastructure that monitors domestic activities. Even though its exact assets are classified for security purposes, it is widely believed that the NSA has the most advanced infrastructure to gather intelligence. The most important role of the NSA comes to light when its extensive reach to any data is examined. Since how the agency operates is mainly disclosed to the public, **the agency could have access to every database that is owned by US-based private companies.** The combination of such a massive database with advanced facial recognition algorithms developed by the US probably accounts for the world's most advanced facial recognition system. Even though the limits of the NSA's database(s) are unknown, delegates should keep in mind that the US government might have access to a database that is much greater in size than any database documented in official reports.

### Department of Motor Vehicles (DMV)

According to the Arizona Dept. of Transformation, a DMV (or sometimes a Bureau of Motor Vehicles) is a state-level organization that administers driving tests, registers vehicles, and driving licenses (Pacey). Even though DMVs are not actively involved in the issue of the usage of facial recognition technology in government surveillance, they are of utmost importance because they have very large databases consisting

of the photos of millions of drivers. Some DMVs in several states allow their local police departments and/or the Federal Bureau of Investigation (FBI) to access these databases during investigations; therefore, DMVs are huge suppliers of data for facial recognition systems, and the databases they provide are important parts of the infrastructure that is needed in any advanced facial recognition based government surveillance program.

### People's Republic of China

Since its creation in 1949, every Secretary-General of the Chinese Communist Party (CCP), therefore the President of the People's Republic, has been employing top-down policies to enact their will. Given the authoritarian nature of the regime, the Chinese government has followed numerous collectivist practices including the implementation of a command economy and restrictions of individual liberties in the name of public interest. Restrictions of civil liberties are so common in China that It wouldn't be inaccurate to simplify the Chinese approach to governing as prioritizing the public interest over the individual at all costs. As one may understand, it is quite understandable why such an authoritarian regime would feel no restraint while using a technology such as facial recognition. The justification of the technology is already there; it is the same justification that the government has been using for decades. The benefits of public security attained by the usage of facial recognition technology far outweighs the detrimental effects of its use on civil liberties.

Perhaps what makes China special in the context of facial recognition technology is its unique **social credit project**. Many people are already familiar with the project; therefore the report will only superficially address it and then move on to its relation with facial recognition technology. Resources for further reading on the social credit project are provided in the "Useful Links" section of the report. The social credit project was put forward during 2014 and was set to achieve a state-wide level before 2021, however, COVID-19 probably pushed that to a later date. The project utilizes *big data analysis* to assign each citizen a social credit score that is updated depending on the actions of the person. A downgrade of this social credit is planned to result in a deduction of the civil liberties of the respective person. Nicole Kobie explains how the social credit score of a citizen might downgrade as "It can range from not paying fines when you're deemed fully able to, misbehaving on a train, standing up a taxi, or driving through a red light" (Kobie). Given how easy, wide, and successful implementation of facial recognition technology would make identifying people and accelerate the success of the social credit system, it is very obvious why the Chinese government has invested so much in facial recognition and installed a camera in every corner around the country. As illustrated below in Figure 1, China has the world's most monitored cities. It is for this reason that China's stance on the usage of facial recognition technology in government surveillance is very strict: China is

against any regulatory framework that would limit their usage of the recently established surveillance infrastructure.

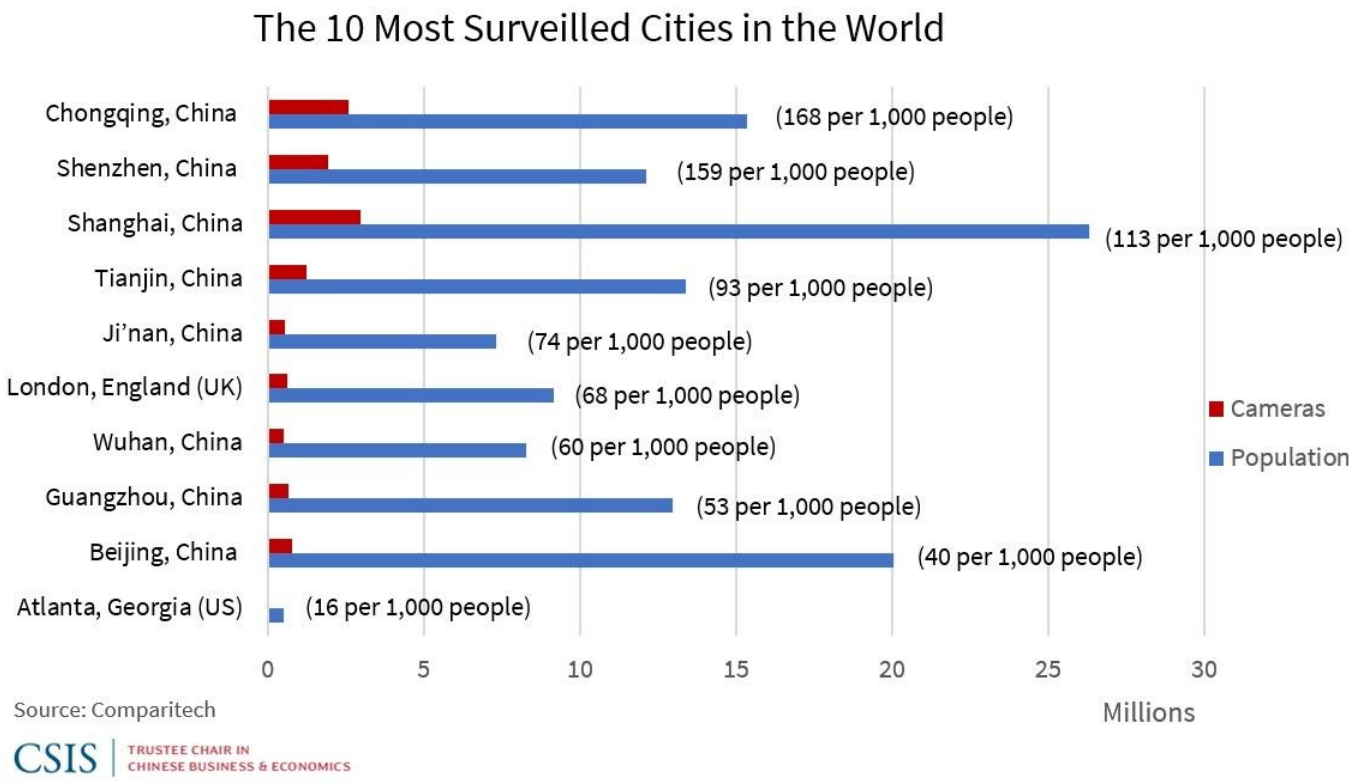


Figure 1: The 10 Most Surveilled Cities in the World (CSIS)

# III. Focused Overview of the Issue

## 1. Public Security vs Individual Privacy

Looking at the root cause of any problem associated with the use of facial recognition technology in government surveillance, one sees the concept of civil liberties. This conflict in regards to where the line should be drawn between public security and individual liberties have been debated for almost 500 years by moral philosophers and political theorists. The application of this debate to the agenda item is that people are getting recorded and photographed by cameras in the Member States and then these photographs are later stored in databases where facial recognition is used as a means of government surveillance. The argument for the pro-facial recognition governments is that the system allows for better monitoring of every-day crime and **keeps the streets safer**. On the other hand, digital privacy activists argue that people recorded by a facial recognition system have never consented to their photos being stored in databases therefore this use of facial recognition technology in government surveillance **is an infringement of personal privacy**. In the end, delegations' stances on the issue boil down to how authoritarian their governments are;

the more authoritarian, the more collectivist their argument will be; the more (politically) liberal, the more individualistic their approach will probably be.

### 2. The Issue of Bias Against Minority Groups

Another criticism of facial recognition systems is that it is biased towards minority groups or some ethnicities. According to the Washington Post, "Asian and African American people were up to 100 times more likely to be misidentified [by facial recognition systems] than white men." Besides, the article also suggests that the faces of "African American women were falsely identified more often" in the investigations conducted by the police (Harwell). This federally confirmed bias towards minority groups and African Americans is among the reasons why many believe that facial recognition technologies should not be used without proper regulation.

### 3. Facial recognition and COVID-19

Lastly, in this subtopic of the third section, the report (by the theme of TIMUN '20, *Crisis, and Global Governance*) will touch upon the use of facial recognition technology during the COVID-19 pandemic. Beginning in March 2020, many governments have increased their use of facial recognition to monitor public activity and spot quarantine evaders. China, for example, installed cameras in over 100 neighborhoods due to COVID-19 (Shen). The ease the technology provides in spotting quarantine evaders may be appealing to some and lead them to see the technology as a necessity to effectively enforce self-quarantine and other isolation rules. However, the pandemic still does not provide the conditions for a world where the 500-year-old debate is finally settled.

## IV. Key Vocabulary

Facial recognition: According to the American Civil Liberties Union, facial recognition systems are defined as "built on computer programs that analyze images of human faces to identify them".

False-negative: "When it comes to errors, there are two key concepts to understand: A *false negative* is when the face recognition system fails to match a person's face to an image that is contained in a database. In other words, the system will erroneously return zero results in response to a query" (Face Recognition).

False-positive: "A *false positive* is when the face recognition system does match a person's face to an image in a database, but that match is incorrect. This is when a police officer submits an image of "Joe," but the system erroneously tells the officer that the photo is of Jack" (Face Recognition).

Collectivism: "Emphasis on collective rather than individual action or identity" (Collectivism). Policies of the Chinese government regarding the prioritization of public security -by the use of facial recognition- over personal privacy is a relevant example of collectivism.

Big Data: Big data analytics is the use of advanced analytic techniques against very large, diverse big data sets that include structured, semi-structured, and unstructured data, from different sources, and in different sizes from terabytes to zettabytes (Big Data Analytics). Big Data is relevant to the agenda item as the Chinese social credit project is based on implementing big data practices to data collected by China's nation-wide facial recognition system.

## V. Important Events & Chronology

| Date (Day/Month/Year) | Event |
|---|---|
| 1964 | Woody Bledsoe, Helen Chan Wolf, and Charles Bisson started researching facial recognition technologies |
| The 1990s | DARPA created the first facial recognition database which was able to identify up to 800 people |
| 2010 | Facebook implemented facial recognition to identify who was in photos. This marked the debut of facial recognition in social media |
| The 2010s | The US started implementing facial recognition in collaboration with regional police departments |
| 2019 | China's facial recognition systems are reported to be almost completed and ready for nationwide implementation |
| 2020 | In February, India first used facial recognition to identify 1,100 individuals at a riot |
| 2020 | UN human rights chief Michelle Bachelet calls for a moratorium on the use of Facial Recognition technology |

## VI. Past Resolutions and Treaties

- United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism

Although not directly related to facial recognition, this document touches upon the recommended use of biometrics -including facial recognition- by the UN.

- A/HRC/44/24 - Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General

Even though it is not a resolution nor a treaty, this report published by the High Commissioner is of prime relevance because the report is very recent and directly addresses the issues pointed out in the

previous sections of this report (Introduction and Focused Overview of the Issue) regarding facial recognition technologies. It highlights the possibility of mismatches between individuals and photographs (false positives) and also the possible human rights violations caused by the unregulated use of the technology.

- Resolution 2396 (2017)

Once again, this resolution also does not directly relate to the monitoring of facial recognition technology but calls for the Member States to develop such technologies to prevent acts of terrorism.

## VII. Failed Solution Attempts

Since the UN has not yet directly addressed the issue regarding the monitoring of facial recognition systems, there are no failed solution attempts to monitor facial recognition systems on an international basis. However, the UN has addressed and failed in promoting the development of these technologies. Both resolutions aforementioned in section VI have called for the development of such technologies but the initiation of multilateral cooperation to do so has not been demonstrated by any Member State.

On the other hand, some Member States have tried implementing federal or regional frameworks in order to regulate the use of facial recognition. These legal frameworks, in an attempt to prevent people from being part of a database in which they haven't consented to take a part in, required surveillance programs to ask for the consent of people before initiation. However, the biggest shortcoming of such a solution attempt, according to Nature, was that people were not aware of the significance of giving consent to be used in such databases (Roussi). In order to address this delegates may include a clause to raise public awareness on the importance of facial recognition and consent in their draft resolutions.

## VIII. Possible Solutions

Delegates should bear in mind that since the use of facial recognition technologies in government surveillance systems is for the most part not addressed by an international framework, whatever solution they manage to come up with would be a step further to tackle the issue. That being said, below are some ideas you might want to incorporate in a draft resolution:

1. The creation of an international body that would be responsible for monitoring (and regulating) the use of facial recognition systems in the Members States. Delegates may consider having this body under the UN or supervised by UN-appointed impartial experts. Inclusive multinational cooperation rather than an exclusive union of a few Member States should be favored.

2. The size and the exact way how photos are used by algorithms to be publicly disclosed to raise public awareness on the issue and address civil privacy concerns. Having an elaborate public awareness clause is pivotal for a comprehensive resolution that tackles all aspects of the agenda item. Awareness raised by such a clause may allow people to make more informed decisions regarding how their data is being used by their government.
3. Ask for governments to engage in multilateral cooperation in developing facial recognition systems in Member states which have not conducted significant research on the issue. Global cooperation to innovate the technology may prevent only a few nations from using technology in any way they may like. Removing the barriers for developing countries to work with technology is important for addressing the "developing" aspect of the agenda item.

## IX. Useful Links

- This map of the United States is frequently updated and shows the states in which facial recognition technology is used for government surveillance. Also, the website provides updates regarding any state laws (or bills) which are concerned with the usage of facial recognition. While using this website delegates should bear in mind that the organization controlling the website (Fight For The Future) is a group of digital activists who demand political action from their respective legislatures in regards to digital privacy, and to this end, the organization is advocating for the ban of facial recognition technology as a means of ensuring public safety as they argue that it is an infringement upon citizens' privacy. Therefore, the content on the website is most likely biased towards the use of this technology. https://www.banfacialrecognition.com/map/
- This article by Vox addresses an aspect of facial recognition that is only briefly touched upon by this report: the effect of the private sector on the development and the use of the technology. Since the agenda item is regarding the use of technology as a tool for government surveillance, the private sector is not elaborated on in this report. Similar to any market economy where the built-in competition to derive profit compels innovation, the facial recognition technology industry is no different. Any delegate wishing to further read about the collaboration of Ring, a service offered by Amazon (the perfect example of an expansive private enterprise), and local police departments are encouraged to read the second half of this article. https://www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future
- The state of facial recognition technology in government surveillance is not as prominent in Europe as it is in the United States or China, therefore this report did not detail the use of the system over Europe and the European Union (EU)'s stance on the matter. Delegates of European Member States

should be well informed regarding their individual delegation's stance, however, any delegate who wishes to further research on the stance of the EU and the use of facial recognition technology by European governments and how it relates to EU law may look to the report provided in the link above.
https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

- Further reading for a better understanding of China's social credit project may be done with the aforementioned link. https://www.wired.co.uk/article/china-social-credit-system-explained

## X. Works Cited

"Ban Facial Recognition." Ban Facial Recognition, Leaflet, www.banfacialrecognition.com/map/. Accessed 22 Aug. 2020. Map.

“Big Data Analytics.” IBM, IBM, www.ibm.com/analytics/hadoop/big-data-analytics. Accessed 12 Dec. 2020.

“Collectivism.” Merriam-Webster, Merriam-Webster, www.merriam-webster.com/dictionary/collectivism. Accessed 12 Dec. 2020.

Colville, Rupert. "New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States." Office of the United Nations High Commissioner for Human Rights, OHCHR, 25 June 2020, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E. Accessed 22 Aug. 2020.

CSIS. The 10 Most Surveilled Cities in the World. csis.org, Center for Strategic & International Studies, www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations#:~:text=This%20past%20February%2C%20China%20introduced,a%20slightly%20lower%20accuracy%20rate.&text=In%20October%202019%2C%20China%20had,use%20of%20facial%20recognition%20technology. Accessed 23 Aug. 2020.

"Face Recognition." Electronic Frontier Foundation, EFF, www.eff.org/pages/face-recognition. Accessed 23 Aug. 2020.

"FACE RECOGNITION TECHNOLOGY." American Civil Liberties Union, edited by Anthony D. Romero, ACLU.org, www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology. Accessed 22 Aug. 2020.

Facial recognition technology: fundamental rights considerations in the context of law enforcement. FRA, 29 Nov. 2019. European Union Fundamental Rights Agency, fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf. Accessed 22 Aug. 2020.

Ghaffary, Shirin, and Rani Molla. "Here's where the US government is using facial recognition technology to surveil Americans." Vox, Vox Media, 10 dec 2019, www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future. Accessed 22 Aug. 2020.

Harwell, Drew. "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use." The Washington Post, 20 Dec. 2019. The Washington Post, www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/. Accessed 23 Aug. 2020.

Kobie, Nicole. "The complicated truth about China's social credit system." Wired, 7 June 2019, www.wired.co.uk/article/china-social-credit-system-explained. Accessed 23 Aug. 2020.

Lewin, Dan'l. "Timeline of Computer History." Computer History Museum, 2020 Computer History Museum, www.computerhistory.org/timeline/1944/. Accessed 22 Aug. 2020.

Murooka, Mitsuhir, editor. "A Brief History of Facial Recognition." NEC Orchestrating a Brighter World, edited by Mitsuhir Murooka, NEC New Zealand, 26 May 2020, www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/#:~:text=The%20earliest%20pioneers%20of%20facial,to%20recognise%20the%20human%20face. Accessed 22 Aug. 2020.

Pacey, Doug. "Why does Arizona have an MVD and not a DMV?" ADOT, Arizona Department of Transportation, 28 Apr. 2015, azdot.gov/adot-blog/why-does-arizona-have-mvd-and-not-dmv. Accessed 22 Aug. 2020.

Roussi, Antoaneta. “Resisting the Rise of Facial Recognition.” Nature News, Nature Publishing Group, 18 Nov. 2020, www.nature.com/articles/d41586-020-03188-2. Accessed 12 Dec. 2020.

Shen, Xinmei. “China Embraces Facial Recognition Even as Data Leaks Are Rampant.” South China Morning Post, 8 Oct. 2020, www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes.