Forum:	**Human Rights Council**
Question of:	**Discussing measures on preserving rights to one's own image**
Student Officer:	**Emil Schatz**
Position:	**Chair**
Contact:	emil.schatz@gyra.hamburg.de

Content

I. **Description of the Issue**
II. **Definition of Key Terms**
III. **Background Information**
IV. **Major Countries and Organizations Involved**
V. **Timeline of events**
VI. **Previous attempts to solve the issue**
VII. **Possible solutions**
VIII. **Questions delegates should consider during research**
IX. **Relevant UN Treaties and events**
X. **Useful links and sources**

I. Description of the Issue

Almost every person alive nowadays has at least once been photographed without ever being asked. Some appear in the background of a stranger's holiday picture, some on a selfie, in which they did not want to be, some are recorded by a shop's security camera, or are even featured in a friend's Instagram post. Fact is, this applies to almost everybody, but for most of human history, it was never a major concern. An image was difficult to copy and even more difficult to spread. Nowadays, any picture can be copied without limit, altered, be it with Photoshop or artificial intelligence, so that it shows something completely different from what it did before, and sent around the globe in seconds or less. The right to one's own image describes how every person is free to decide whether, how, and in what context their image, meaning their face, body, or voice, is captured, shared, and used. This freedom of decision is treated as a basic human right in a lot of countries, and not just as a preference. One's image is part of who they are, so preserving and controlling it is crucial for preserving human dignity

and privacy. It gives people the freedom to present themselves to the world in a manner that they choose for themselves. If an image of a person is taken or even published against their

wishes, the harm created cannot be limited to just personal embarrassment; it can damage reputation, expose intimate details, place one in a degrading light, or mislead people's opinions. For these reasons, this right is understood as part of the broader right to privacy, which is protected under Article 12 of *the Universal Declaration of Human Rights* and Article 17 of the *International Covenant on Civil and Political Rights.*

The right to one's own image, however, is not by any means complete. It coexists in contradiction with other rights, like, for example, freedom of expression and the freedom of the press. Photographs and recordings play an essential role in journalism, art, and public discourse. In a society where nobody can be filmed, photographed, or recorded, functionality and freedom would also be greatly compromised. This results in the right being applied differently across all situations. While a private person enjoys protection in their everyday life, a person of public interest, like a politician or a celebrity, has to accept their privacy being severely compromised if there is a matter of genuine public interest. This creates the need for a balance, and deciding where this balance should be is one of the major difficulties of this topic.

What makes this issue urgent today is how fast technology like artificial intelligence, social media, and smartphones shifts this balance, with the speed of change increasing daily. Through smartphones and social media, both the capturing and the sharing of an image have become increasingly easy, facial recognition is suddenly able to identify a person from just a single photograph, and artificial intelligence can create images and videos of people doing things they never actually did. Therefore, right now, this right matters more than ever before and, at the same time, has never been this hard to protect. One is less and less able to control where, when, and in what context their image appears, who can profit off of it, and whether it has been altered in any way.

Another major problem is created because these challenges are not confined within one border; the internet stretches worldwide, and so does access to social media and artificial intelligence. Some states offer strong safety and protection for this right, while many others offer zero to none. The laws protecting one's own image are deeply uneven and inconsistent across all nations. It is this combination of a universal need for the right and fragmented protection of it, rather than a unified, international and multilateral response, which brings this

issue before the Human Rights Council. We ask Delegates to consider not only how their country, but also how the international community, can preserve the right to their own image

in this time of rapid digital development, without undermining the freedoms of expression, information, and the press, and without breaching the sovereignty of any member nation.

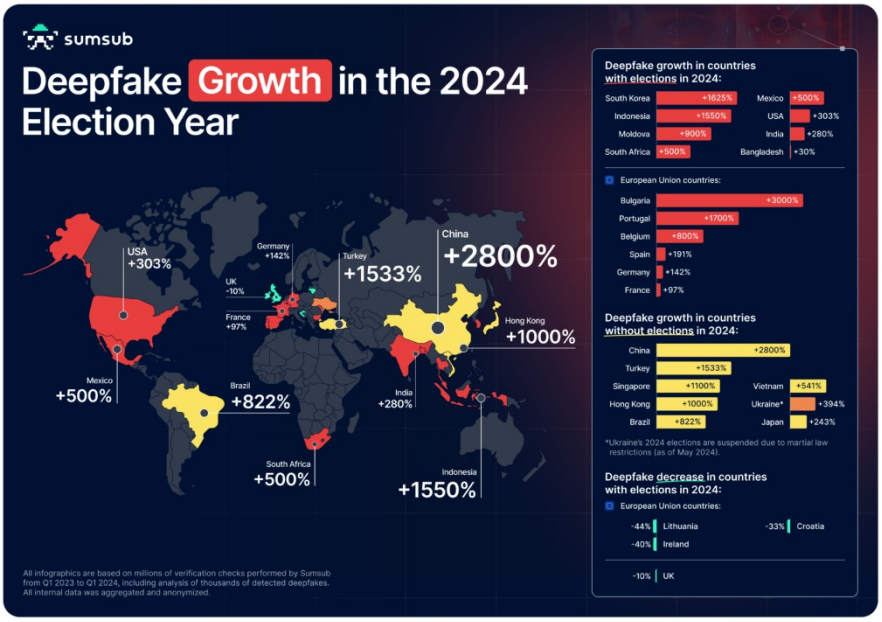
II. Definition of Key Terms

When defining a specific legal instrument, the source is stated in brackets. All other terms are explained in plain language to be clearer and avoid misunderstandings.

Biometric data: Information about a person's body that is unique to them and can be used to recognise them, such as their face, fingerprints, or voice. Because you cannot change your face the way you can change a password, this kind of information is extra sensitive and needs extra legal protection (for example, under the European Union's data protection law, the GDPR, Article 4). A normal photograph turns into biometric data in the moment when it is used to actually identify who is in it.

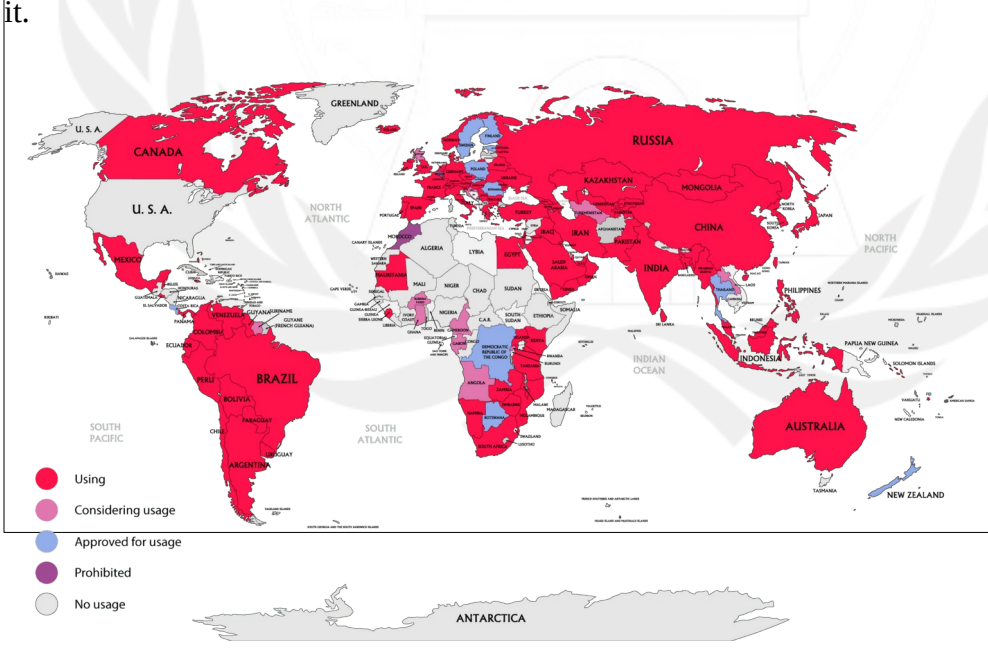
Consent Permission. In this topic, it means a person freely agreeing to their image being taken, used, or shared, while properly understanding what they are agreeing to. Most cases are about consent: using someone's image is usually acceptable if they said yes to one's using it, and a violation if they did not.

Deepfake: A deepfake is normally an image or a recording that makes it seem like a real person said or did something they never actually did, for example, a video of a politician giving a speech they never gave. These deepfakes are becoming so convincing that it is often nearly impossible to tell the difference between a real and a fake recording.



https://sumsub.com/newsroom/deepfake-cases-surge-in-countries-holding-2024-elections-sumsub-research-shows/

Facial recognition technology (FRT) is an advanced technology that can recognize a person from their face. It works by measuring the features of a face, such as the distance between the eyes and turning them into a kind of a digital fingerprint, which it can then compare against other photographs and videos. It is mostly used by police, governments, and companies, and it is one of the main ways in which a person can be identified and tracked without ever knowing it.



https://reclaimyourface.com/articles/

Likeness: Is what makes a person recognizable as themselves: their face, body, voice, and any other features. When this report refers to the "right to one's own image," then it actually

means the right to control your own likeness, meaning the right to decide where and how the image of you is used.

Non-consensual intimate imagery (NCII): Sexual or nude images of a person that are shared without the affected person's permission, often to humiliate or even threaten them. It is sometimes called "revenge pornography." The images may be real photographs or fake ones created by artificial intelligence (deepfakes), and either way, it is considered one of the most serious and damaging violations of a person's right to their own image.

Personality rights: The wider group of rights that protect the things that make you who you are: your name, your face, your voice, and your reputation. The right to one's own image is one part of this group. Personality rights cover two different concerns: protecting a person's dignity and privacy on one hand, and protecting the commercial value of a famous person's identity on the other. As a rule, these rights cannot be permanently sold or given away, because they are seen as part of the person themselves.

Public figure and private individual: A public figure is someone in the public eye, such as a politician, a public official, or a celebrity, who, because of their role, has to accept more attention and less privacy whenever the public has a genuine reason to be informed. A private individual is an ordinary person who is not in that position and who is entitled to much stronger protection of their image in everyday life. This difference matters because it decides how far a person's right to their own image can be pushed aside by the freedom of the press: far more easily for a president than for a random passer-by.

Right to one's own image: The right of every person to decide whether, how, and in what setting their likeness is captured, used, and shared. In simple terms, it is the right to have a say over what happens to pictures, videos, and recordings of you. It has long been recognized in some countries; Germany calls it the *Recht am eigenen Bild* and France the *droit à l'image*, and it is generally treated as part of the broader right to privacy and of human dignity.

Right to privacy: The right of every person to a private life that is not interfered with unfairly, covering their family, home, communications, and reputation. It is promised to everyone by Article 12 of the Universal Declaration of Human Rights and Article 17 of the

International Covenant on Civil and Political Rights. It is the larger right that the right to one's own image grows out of.

Model United Nations Vocabulary

Amendment: A suggested change to a resolution. During the debate, delegates can propose adding, removing, or rewording part of a resolution, and the room then votes on whether to accept the change.

Co-Submitter: A delegate who signs a resolution so that it is allowed to be debated. Signing only means "I think this is worth discussing," and does not mean the delegate actually agrees with it.

Delegate: A participant who represents a country or organisation and works with others to solve the issues on the agenda. If you are reading this as a participant, this is you.

Lobbying The stage before formal debate, where delegates talk through their ideas, combine their draft resolutions into stronger ones, and gather enough co-submitters for a resolution to reach the floor. It can be thought of as the negotiation phase.

Main Submitter: The delegate who leads a resolution, presenting it to the room and giving the first speech in its favour. Unlike a co-submitter, the Main Submitter has to actually support it.

Operative Clause (OC): The "action" part of a resolution. These are the numbered clauses near the end that state what should actually be done about the problem.

Position Paper: A short document a delegate writes before the conference, setting out what their assigned country thinks about an issue and which solutions it would support.

Preambulatory Clause (PC): The "background" part of a resolution. These opening clauses describe the problem and point to relevant facts, past actions, or treaties before any solutions are proposed.

Resolution: The main document of an MUN debate. It is built from preambulatory clauses (which describe the problem) and operative clauses (which propose the solutions), and it is what delegates ultimately vote on.

III. Background information

The right to one's own image is far older than the technology that is now threatening it. Its foundations were laid in Germany in 1898, when two photographers entered the room in which the former Chancellor Otto von Bismarck lay dead, and took pictures of his dead body without receiving permission. A scandal followed, which then, in 1907, led to the Kunstuhrhebergesetz, in which Paragraph 22 established that an image of a person may not be shared, displayed, or used in any way without that person's consent. This then became known as the Recht am eigenen Bild, the right to one's own image, and it still acts as the main orientation on which countries base their legal frameworks concerning this right. After World War 2, the protection of private life was taken into international human rights law. Both Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966) guarantee that nobody shall be confronted with interference with their privacy, honour, or reputation, and while neither article mentions images concretely, courts and human rights bodies have always interpreted control over one's own image as part of this right to privacy.

Moving on to a bit more modern background, the most influential statement of the right came from the European Court of Human Rights in Von Hannover v. Germany (2004), where Princess Caroline of Monaco spent years attempting to stop German scandal newspapers from publishing pictures of her private life, taken by paparazzi. While German courts argued she had to tolerate such attention due to her public role, the European Court disagreed, saying that publishing images of her private life violates her right to respect for private life under Article 8 of the European Convention on Human Rights. This case made two different ideas apparent: a person keeps the right to their image even in public space, and the right to one's own image always has to be balanced with the freedom of the press, where the question is whether an image genuinely contributes to the public interest.

Now, looking at the issue today, for most of the 20th century, this right was mostly something to be thought about by celebrities or the press, since taking images and then publishing them always required money, cameras, and access to either a printer or a broadcaster. In this digital

Age, however, completely changes this. Billions of people carry a camera, with which anyone can take a picture in just seconds. In general, there have been three main factors that have shifted the balance previously explained, more toward or against the ordinary individual. First, it is just the volume of images; almost anything can be recorded and shared by anyone, often, of course, without the knowledge of all the people in the picture or video. Second, it is facial recognition. It allows not only companies but also governments to identify a stranger just from a single photograph. The best example for this would be Clearview AI, a company that, as was revealed in 2020, copied billions of images from social media and the internet in order to establish a search engine for faces, which was then sold mainly to police forces. People in this database never knew that their images had been taken, and there was no way to have them removed again. The third and last factor is artificial intelligence. Since 2017, it has made it possible to generate really convincing fake images and videos of real people; simply put, what once required expertise and a studio can now be made on an ordinary phone. Socially, the most severe result of this is the spread of non-consensual intimate imagery, which includes AI-generated deepfakes. There have been studies which repeatedly found that the majority of harmful deepfakes online are sexual images created without any consent, and that women and girls are targeted far more than anyone else. A recent example would be when, in 2024, explicit deepfakes of the singer Taylor Swift spread across the internet and were viewed millions of times before they were taken down. This drew attention to the issue and to how quickly fakes can spread and how little protection exists. Falsified images and videos of politicians, displaying misleading events that were altered or made up as a whole, threaten public trust. They can spread misinformation, even if it appears to come from a good source, and just the possibility of a source being altered can also lead to a genuine recording being dismissed as a fake. Economically, a person's image and reputation actually hold measurable value. Misuse is estimated to have caused financial damage in the hundreds of millions.

Two features about this issue make it a matter for the international community rather than for single states on their own. Firstly, as previously explained, the harmful results do not stop at borders; an image could be taken in one country, altered in a different one, and then published in a third country within an alarmingly short time span. This cross-border challenge makes it even harder for the person responsible to be discovered. Secondly, legal protection is incredibly uneven; some countries offer strong and well-developed image rights, while others

offer little or none. And even where strong regulations exist, enforcement is really difficult. When multiple countries fined Clearview AI an estimated total of 100 million euros, the company simply ignored the fines, saying they lay beyond its control. All of it results in a global gap between the universal need to protect one's own image and a fragmented protection system that often finds itself powerless. This gap is what the Human Rights Council is going to address.

IV. Major Countries and Organizations Involved

Primary Countries

Germany: This is where the right to one's own image was first written into law, so Germany tends to lead on strong protection. Through the European Union, it backs tough privacy rules (the GDPR) and the new AI Act, and German regulators have been among the most willing to challenge companies that misuse people's images. If you represent Germany, you are arguing from a long tradition of treating control over your image as a matter of dignity.

United States: The United States protects free speech very strongly, which has historically made it cautious about limiting how images can be used. At the same time, it is home to most of the world's major technology and AI companies, and after a wave of deepfake scandals it has started to act, passing the TAKE IT DOWN Act against non-consensual intimate images. Your country sits at the centre of both the problem and the technology behind it.

China: China uses facial recognition more widely than almost any other country, especially for state surveillance, while also having some of the earliest rules requiring AI-generated content to be labelled. If you represent China, you will likely defend a state's right to manage technology within its own borders and resist outside interference.

Denmark: Denmark has put forward one of the boldest ideas anywhere: giving every person a form of copyright over their own face, body, and voice, so that deepfakes could be removed like stolen property. For a small country, it has placed itself at the front of the debate and is a natural ally for anyone pushing strong protection.

Secondary Countries

United Kingdom has moved quickly on online harms, making it a crime to share, and in some cases create, sexual deepfakes through its Online Safety Act.

South Korea: Hit by a serious wave of deepfake sexual abuse in its schools and universities, it has toughened its laws and is one of the clearest examples of how badly this affects young people.

India and other large digital nations: Enormous online populations and growing deepfake problems, but rules that are still catching up to the technology.

Many developing countries: A large number of states have little or no image-rights law at all. They are affected by these harms but often lack the resources to respond, and may worry that international rules will be written without them in mind.

NGOs and IGOs

UN Human Rights Council and OHCHR: Your own committee, and the UN office that has produced the main reports on privacy and human rights in the digital age.

Council of Europe and the European Court of Human Rights: The court behind the landmark *Von Hannover* ruling and the Article 8 right to a private life.

European Union: Not a country, but a powerful bloc whose laws (the GDPR and the AI Act) set standards that companies around the world end up following.

Privacy International, Article 19, and Access Now: Campaign groups that research abuses and push for stronger protection. Article 19, in particular, speaks for free expression, a useful reminder that not every actor wants image rights strengthened without limits.

The major technology companies, the platforms where most of this actually happens, are discussed in the section "How to prepare as a delegate."

V. Timeline of events

1898 – 1907 The right is born in Germany: Photographers secretly take pictures of the dead Chancellor Otto von Bismarck. The scandal led to Germany's 1907 *Kunsturhebergesetz*, which bans using a person's image without their consent, the first clear "right to one's own image."

1948 & 1966 Privacy enters international law: The Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17) protect everyone from interference with their privacy, honour, and reputation.

2004 *Von Hannover v. Germany:* The European Court of Human Rights rules that publishing paparazzi photos of Princess Caroline of Monaco's private life breaches her right to a private life, confirming that people keep image rights even in public.

2013 The Snowden revelations: Mass digital surveillance is exposed, pushing privacy in the digital age onto the UN agenda and leading to the first UN resolutions on the subject.

2017 The first deepfakes appear: AI-generated fake videos of real people surface online, showing that anyone's face can now be convincingly faked.

2018 The GDPR takes effect: The European Union's data protection law treats facial and biometric data as especially sensitive, setting a global benchmark.

2020 Clearview AI is exposed: It is revealed that the company scraped billions of faces from the internet to sell to police, sparking lawsuits and fines worldwide.

January 2024: The Taylor Swift deepfakes: Explicit AI deepfakes of the singer spread to millions of viewers before removal, drawing global attention and speeding up new laws.

2024: The EU AI Act: The world's first broad AI law is passed, requiring AI-generated content such as deepfakes to be labelled.

2025 A wave of new protections: The United States passes the TAKE IT DOWN Act against non-consensual intimate images, and Denmark proposes giving people copyright over their own face, body, and voice.

VI. Previous attempts to solve the issue

There have been numerous attempts to solve this issue at the United Nations
the clearest UN action has come through a series of resolutions on the right to privacy in the digital age. The first major step was General Assembly Resolution *68/167 (2013)*, adopted after the Snowden surveillance revelations, which affirmed that the rights people hold offline, including privacy, must also be protected online. This was followed by a run of Human Rights Council resolutions on the same theme, most recently *HRC Resolution 54/21 (2023)*, which increasingly addressed new technologies such as artificial intelligence, biometric identification, and the tracking of individuals.

- General Assembly Resolution 68/167: https://undocs.org/A/RES/68/167
- Human Rights Council Resolution 54/21: https://undocs.org/A/HRC/RES/54/21

Alongside these, the Office of the UN High Commissioner for Human Rights (OHCHR) has published detailed reports on privacy and technology, and since 2015 a Special Rapporteur on the right to privacy has investigated surveillance and digital threats, at times calling for strict limits on the most dangerous uses of these tools. The main weakness of this work is that it is not legally binding, and that it treats privacy and surveillance broadly rather than the right to one's own image specifically.

At the regional level, Europe has gone furthest. The Council of Europe, through the European Court of Human Rights, built up the case law (including *Von Hannover*) that protects a person's image as part of private life, while the European Union's GDPR (2018) gave strong protection to facial and biometric data and its AI Act (2024) now requires AI-generated content to be labelled. These measures are powerful, but they only cover part of the world, which limits their effect on a global, borderless problem.

At the national level, A growing number of states have passed their own laws, from Germany's long-standing image right to the United States' TAKE IT DOWN Act, the United Kingdom's Online Safety Act, South Korea's tougher deepfake rules, and Denmark's proposal to give people copyright over their own likeness. Together, these show real momentum, but

they also create a patchwork of very different rules. Because the internet crosses borders, national laws are often hard to enforce against offenders and companies based abroad, as shown when Clearview AI ignored the fines issued by several European regulators.
Taken together, these attempts have achieved a great deal, yet they remain fragmented, non-binding at the global level, and focused mainly on privacy and data rather than on the right to one's own image itself. No single international standard exists to tie them together. Closing that gap is the task now before this committee.

VII. Possible solutions

There is no single fix for this issue, and every measure involves a trade-off, usually between protecting people's images and protecting freedom of expression, security, or state sovereignty. The following are directions delegates may wish to explore and combine. The strongest resolutions will be those that address the harm without silencing legitimate journalism, art, and debate.

A shared international standard. Delegates could work towards a common definition of the right to one's own image and a set of minimum protections that all states agree to uphold. This would help close the gap between countries with strong laws and those with none. The difficulty is persuading states with very different legal traditions, especially on free speech, to accept the same baseline.

Faster removal of harmful images. Building on laws such as the TAKE IT DOWN Act, delegates might call for platforms to remove non-consensual intimate images and malicious deepfakes quickly once they are reported. The challenge is designing this so it does not lead to the over-removal of lawful content, and so that smaller platforms can realistically comply.

Labelling of AI-generated content. Following the model of the EU AI Act, delegates could support requirements that deepfakes and other synthetic media be clearly marked. This helps people know what is real, but it does little against bad actors who simply ignore the rules, so it works best alongside other measures.

Protecting biometric data and limiting misuse of facial recognition. Delegates may consider rules on the scraping of images from the internet and on how facial recognition is used,

particularly by private companies. Here the tension is sharp, since states often defend facial recognition for security and law enforcement, and will resist limits on their own use of it.

Support for developing countries. Because many states lack any image-rights framework, delegates could propose funding, training, and model laws to help them build one. This directly addresses the North–South gap and makes any global standard fairer, though it requires wealthier states to provide resources.

Cross-border cooperation. Since a single image can cross many borders in seconds, delegates might create ways for states to cooperate on investigations and enforcement, so that offenders and companies cannot simply hide in another country. The obstacle is that stronger international enforcement can raise concerns about national sovereignty.

Education and awareness. Finally, delegates could promote programmes, especially for young people, to help individuals understand their rights and protect their own images online. This is less confrontational and widely acceptable, but on its own it places the burden on victims rather than on those causing the harm.

The real task for the committee is to combine several of these approaches into a balanced package, one that genuinely protects people's images while preserving the freedoms of expression and information, and respecting the different positions of member states.

VIII. How to prepare as a delegate

Firstly, all delegates are obligated to write at least one draft resolution and a minimum of two, preferably three, position papers so that all topics of the forum are fully covered.
The deadline to send in the documents is 27.08.26. After the deadline, documents will not be corrected by Student Officers. By then, all delegates should have sent in their document; documents turned in later than that should not be included in decision-making when it comes to awards **(**as for that, it is important to see how much work the individual delegates put into preparation).

The best preparation is to understand your own country's position before the debate begins. Find out what laws, if any, your country has on image rights, deepfakes, and facial recognition, and whether it tends to prioritise protecting people or protecting free expression

and technology. From there, think about which other delegations share your view and which will oppose it, so you arrive ready to build alliances during lobbying.

The role of technology companies

Although companies cannot sit in this committee, almost every solution depends on them, so you should know the main players. Clearview AI built a face-search engine from billions of images scraped online and became the clearest example of image rights being ignored on a massive scale. Meta (Facebook and Instagram), Google (including YouTube), and X (formerly Twitter) are the platforms where most images are shared, reported, and, when things go wrong, spread; the explicit deepfakes of Taylor Swift, for instance, went viral on X before they were removed. Companies that build AI image generators also matter, because their tools are what make convincing deepfakes so easy to create. Any workable resolution will have to decide how much responsibility these companies carry and how they can realistically be held to it.

Questions to consider during research

- What protection, if any, does my country currently give to a person's right to their own image?
- Does my country lean towards stronger protection, or towards defending free expression and the press?
- Is my country home to major technology, AI, or social media companies, and how does that shape its interests?
- How does my government itself use facial recognition and surveillance, and would it accept limits on that use?
- Would my country support binding international rules, or resist them as interference in national sovereignty?
- How can victims, especially women and young people, be protected quickly without giving governments a tool to censor legitimate content?
- What responsibility should technology companies carry, and who should enforce it?

- How can any global standard be made fair to developing countries that currently have little protection?

Keeping these questions in mind while you research will help you write a strong position paper and speak confidently in committee. The delegates who succeed are usually not those with the most extreme demands, but those who understand the other side well enough to build a solution the whole room can accept.

Also do have a look at this website, it was really useful when learning about deepfakes: https://deepstrike.io/blog/deepfake-statistics-2025

IX. UN resolutions

Core human rights instruments

- *Universal Declaration of Human Rights (1948), Article 12:* Protects everyone from arbitrary interference with their privacy, family, home, and correspondence, and from attacks on their honour and reputation. The foundation of the right to privacy.
- *International Covenant on Civil and Political Rights (1966), Article 17*: Turns the same protection into binding treaty law for states that have ratified it.
- *Convention on the Rights of the Child (1989), Article 16*: Gives children specific protection against interference with their privacy, which is increasingly relevant to images of minors online.

Key UN resolutions

- *General Assembly Resolution 68/167 (2013), "The right to privacy in the digital age":* Adopted after the mass-surveillance revelations, it affirmed that the rights people have offline must also be protected online. The starting point for all later UN work on the topic. https://undocs.org/A/RES/68/167
- *Human Rights Council Resolution 28/16 (2015):* Created the mandate of the Special Rapporteur on the right to privacy, an independent expert who investigates privacy threats worldwide. https://undocs.org/A/HRC/RES/28/16

- *Human Rights Council Resolution 42/15 (2019), "The right to privacy in the digital age":* Specifically asked the UN to examine how artificial intelligence, profiling, and automated decision-making affect privacy. https://undocs.org/A/HRC/RES/42/15
- *Human Rights Council Resolution 47/16 (2021):* On the promotion and protection of human rights on the Internet, addressing new and emerging digital technologies. https://undocs.org/A/HRC/RES/47/16
- *Human Rights Council Resolution 48/4 (2021), "The right to privacy in the digital age":* Warned against pervasive surveillance and called for stronger safeguards. https://undocs.org/A/HRC/RES/48/4
- *Human Rights Council Resolution 54/21 (2023), "The right to privacy in the digital age"*: The most recent resolution in the series, focusing on the risks of large-scale data collection and processing, including discrimination. https://undocs.org/A/HRC/RES/54/21

The two resolutions most directly useful to cite in debate are **68/167**, which began the UN's work on digital privacy, and **54/21**, which represents its current position.

X. Useful links

- UN Digital Library: resolution finder. The official search tool for every UN resolution and document. Type in a topic (for example, "right to privacy in the digital age") or a resolution number to read the full text. https://digitallibrary.un.org
- UN Official Document System (undocs.org) The fastest way to open a specific resolution: simply add its symbol to the address, for example undocs.org/A/HRC/RES/54/21. https://undocs.org
- OHCHR: The right to privacy in the digital age. The UN human rights office's own hub, gathering its key reports and resolutions on this topic in one place.- https://www.ohchr.org/en/privacy-in-the-digital-age

XI. Sources

https://www.un.org/en/about-us/universal-declaration-of-human-rights
https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
https://gdpr-info.eu
https://undocs.org/A/RES/68/167
https://undocs.org/A/HRC/RES/28/16
https://undocs.org/A/HRC/RES/42/15
https://undocs.org/A/HRC/RES/47/16
https://undocs.org/A/HRC/RES/48/4
https://undocs.org/A/HRC/RES/54/21
https://www.echr.coe.int/factsheets
https://medium.com/sensity/mapping-the-deepfake-landscape-27cb809e98bc
https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en
https://techcrunch.com/2024/09/03/clearview-ai-hit-with-its-largest-gdpr-fine-yet-as-dutch-regulator-considers-holding-execs-personally-liable/
https://schjodt.com/news/owning-the-self-denmarks-copyright-turn-against-deepfakes
https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf
https://artificialintelligenceact.eu
https://www.ohchr.org/en/privacy-in-the-digital-age
https://deepstrike.io/blog/deepfake-statistics-2025

Images:
https://recfaces.com/articles/what-is-facial-recognition-used-for
https://recfaces.com/articles/what-is-facial-recognition-used-for