AMIGMUN 2023

United Nations Human Rights Council

Agenda: The Right to Digital Privacy & The Weaponization of Data

Table of Contents

Letter from the Executive Board

Greetings Delegates,

It gives us immense pleasure to welcome you to this simulation of UNHRC with the agenda “The Right to Digital Privacy & The Weaponization of Data”

The aim of this background guide is to give you a starting point in your venture of participating in the conference. The background guide will equip you with an insight into the agenda and committee, and give you a direction for your research. Therefore, the rest of the BG systematically covers & intends to explain the role of each of the stakeholders involved with upholding & maintaining the right to digital privacy & the ways in which these stakeholders might weaponize data. The BG also has a section titled ‘Questions to Consider’, which will serve as a tool for you to think & explore potential directions for the committee.

However, you must not consider this an exhaustive document. That is, do not limit your research to the resources in this guide or restrict your debate to the topics in this guide. It is appreciated if you conceive your own ideas and bring forth new realms within the agenda in the committee.

Moreover, as the name “guide” suggests, this document will not provide you with all the information or analysis on the agenda at hand but a path for you to carry out your research. For the prior, you must carry out comprehensive research independently. Even more importantly, you must understand your research and be able to use it effectively. In other words, your research is not your argument. Instead, you use your research to form your argument. Therefore, in-depth research & facts must be complemented with logic & analysis to form a substantive & impactful argument. Therefore, try not to simply read from documents without really understanding what they mean. Instead, try forming your own arguments based on what you read in those documents.

Additionally, you might come across some opinionated articles in the background guide. Those are just to provide you with a perspective and in no way do they represent the personal opinions of the Executive Board.

We have put in a lot of thought and effort into drafting this guide and we hope you will take time to read it thoroughly before the committee.

Also, please note that as your Executive Board, we are only mandated to facilitate debate & discussion in the committee. The decision of what to discuss & how to proceed with the committee relies solely on the delegates. In no way would the Executive Board substantially intervene in such decisions.

As your Executive Board, we will do our best to ease the learning curve and create an inclusive environment that encourages you to express your skills and potential. We are confident that the conference will be an enriching, and, even more importantly, a fun experience for all delegates.

That being said, please feel free to get in touch with us any time before, during, or after the conference in case you have any questions or require any assistance. All the best!

Regards,

Pranav Aggarwal
President

Samarth Bhargava
Vice-President

About The Committee

The United Nations Human Rights Council (UNHRC) was established by the UN General Assembly with the passing of resolution 60/251 in 2006 as a 47 member “intergovernmental body within the UN system responsible for strengthening the promotion and protection of human rights around the globe and for addressing situations of human rights violations and making recommendations on them”. Therefore, the council's work includes reviewing human rights violations, creating human rights standards, and promoting human rights education and awareness.

The creation of the UNHRC was seen as a significant step forward in the global effort to protect human rights. It has been praised for its more balanced and objective approach to human rights issues, as well as its increased focus on human rights education and awareness, in comparison to its preceding organization, the UN Commission on Human Rights

However, the UNHRC has also faced criticism. Some argue that it has become politicized, with some countries using their membership to deflect criticism of their own human rights records. Others argue that the council has been ineffective in addressing some of the world's most pressing human rights issues, such as the ongoing crisis in Syria, the conflict between Israel & Palestine, and the situation in Russia & Ukraine.

Despite its challenges, the UNHRC remains an important institution in the global effort to protect and promote human rights. Its work helps to raise awareness of human rights issues around the world and provides a forum for countries to discuss and address these issues collaboratively.

Mandate of the United Nations Human Rights Council

The council has a mandate to promote and protect human rights around the world. The council is responsible for identifying human rights violations, creating human rights standards, and promoting human rights education and awareness.

Review & Document the Status of Human Rights: The primary function of the UNHRC is to review human rights situations in countries around the world. The council's independent experts monitor human rights violations and abuses, and provide recommendations to the countries in question to improve their human rights records. The

council may also establish special procedures, such as commissions of inquiry or special rapporteurs to investigate and report on specific human rights situations.

Creation of Human Right Standards & Promotion of Implementation: The UNHRC is also responsible for creating human rights standards and promoting their implementation. The council works to develop international human rights law and standards, such as the Universal Declaration of Human Rights (UDHR), and encourages countries to ratify and implement these standards. The council also works to ensure that national laws and policies are consistent with international human rights standards, and provides technical assistance to countries in need of support to implement these standards. The council also works to strengthen regional and international human rights mechanisms, such as the International Criminal Court (ICC), and to ensure that they are effectively addressing human rights violations and abuses.

Education & Awareness: In addition to its work on country-specific human rights situations and standards, the UNHRC also has a mandate to promote human rights education and awareness. The council works to raise awareness of human rights issues and promotes human rights education in schools and universities around the world. The council also encourages the media and civil society organizations to play an active role in promoting human rights and increasing public awareness of human rights issues.

Forum for Cooperation & Discussions: Another key function of the UNHRC is to promote international cooperation and dialogue on human rights issues. The council provides a forum for countries to discuss human rights issues and share best practices. The UNHRC meets three times a year in Geneva, Switzerland, to discuss human rights issues and make recommendations to the UN General Assembly.

Accountability & Facilitation of Prosecution: The UNHRC also plays an important role in promoting accountability for human rights violations. The council works to ensure that perpetrators of human rights violations are held accountable for their actions, and that victims of human rights abuses receive justice and reparations. This includes advocating for the establishment of truth and reconciliation commissions, as well as supporting the work of international tribunals and domestic courts in addressing human rights violations.

The UNHRC also has a mandate to address specific human rights issues and challenges. For example, the council has established special procedures to address issues such as freedom of expression, torture, and the rights of indigenous peoples.

Overall, the mandate of the UNHRC is to promote and protect human rights around the world. The council's work is guided by the principles of universality, impartiality, objectivity, and non-selectivity, and it seeks to address human rights violations and abuses wherever they occur. Despite the challenges that the council faces, such as politicization and limited resources, it remains an important institution in the global effort to protect and promote human rights.

Introduction To The Agenda

Our interactions with others within a private setting where we presume no one is watching make up a large part of what makes us human. We may withhold important aspects of ourselves if we feel that our thoughts and behaviors may not be entirely our own. Privacy is therefore a crucial component of an individual's autonomy. The right to privacy is defined as "the freedom from unjustified interference and the right to keep some things private."

While laws exist in most nations to protect the right to privacy, such laws often do not govern the digital environment. The right to ‘digital’ privacy, therefore, refers to the need for the protection of an individual's personal data and online activities from unwarranted and unauthorized surveillance, intrusion, & access.

Enforcing & upholding the right to digital privacy differs from the right to privacy in general because it specifically addresses the unique challenges and concerns associated with the digital environment. These challenges include, but are not limited to:

Scope: The right to privacy traditionally applies to various aspects of an individual's life, such as their physical spaces, personal conversations, and correspondence. In contrast, the right to digital privacy focuses on the protection of information and activities carried out through digital devices, online platforms, and communication networks.

The Dynamic Nature of Technology: The right to digital privacy acknowledges the impact of advancing technologies on individual privacy. These technologies have significantly increased the ability of governments, corporations, individuals to collect, store, and analyze personal data. The law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for the invasion of digital privacy.

Cross-border Implications: The right to digital privacy raises complex issues when it comes to cross-border data transfers, international surveillance cooperation, and jurisdictional conflicts. As data flows across national borders, the protection of digital privacy becomes a global challenge, requiring international collaboration and frameworks.

Balancing Other Interests: The right to digital privacy often involves a delicate balance between privacy rights and other competing interests, such as national security, public safety, and law enforcement. Governments may need to strike a balance between ensuring individual privacy and maintaining societal order.

Identification: Collection of data & its weaponization is difficult to police. There are multiple challenges that are related to identification: How do you know if someone is collecting & using your data? How do you know who is collecting & using your data? How do you deal with governments, companies, and other third party entities when they collect & use your data?

Lack of Awareness: We don't spend more than 8 seconds before accepting a terms and conditions agreement file on any app where we are giving our details including number and email address and a permission to use our phone's camera, microphone and even our location. This is all how surveillance can be put up and that too which has been already allowed by you. The main factors contributing to this are the complexity of legal frameworks & technology and the fear of repercussions by the government or by tech companies.

State Surveillance

The right to privacy is not absolute. That means it is subject to certain restrictions which might be projected by the lawmakers. However, an attempt to infringe a person's right to privacy, without authorization, might be considered as a criminal offense. Despite this fact, invasion of an individual's right to privacy is a common phenomenon. Even in the most developed of states, people continue to be eluded from exercising their right and, counter-intuitively, it is the national governments which continue to be the biggest perpetrators.

State surveillance refers to the systematic monitoring and gathering of information by governmental entities on individuals, groups, organizations. It involves the collection, analysis, and storage of data for various purposes, including but not limited to national security, law enforcement, and intelligence gathering. State Surveillance is the act of observing persons or groups either. This may either be done with notice or knowledge i.e 'overt surveillance' or done without notice and knowledge i.e 'covert surveillance'. Such surveillance on citizens by governments may give rise to claims of invasion of privacy.

There is a general perception that every citizen is vulnerable to snooping. Mandating sweeping powers to so many agencies of the government without proper institutional oversight will amount to muzzling the freedom of citizens. Moreover, the violation of digital rights to acquire personal data about behavior has led to abuses in the physical world such as arbitrary detention and forced disappearances Recent scandals in which vast amounts of data is collected on millions of citizens, demonstrate the need for governments to be open and transparent about the data that they are collecting and for what purpose.

Many countries perform such surveillance under the concept of State security. This means that if something has to be done for national security, even if it is illegal and unlawful, it can be and will be done. In other words, the constitutional rights of individuals may be violated or taken away from them to make sure national security is maintained. But till what limit is this valid? This is one question that comes up as a debate in our agenda.

The implications of such actions, however, are far reaching.

Apart from the consequences mentioned above, internet users may self-censor their behavior if they are aware of widespread data collecting and surveillance because they are afraid of unanticipated repercussions. In other words, because of this perceived threat of excessive data collection & surveillance, a person may voluntarily choose not to exercise their right to free speech and expression or may not act as they would otherwise.

Additionally, from the most developed countries to the least, examples are prevalent of bloggers, activists, and political opponents being harassed and silenced. In the name of internet security, users are analyzed for characteristics that predict problematic behaviors. Data which can be used to profile individuals or groups who appear rebellious, is often saved. During major protest movements around the world, governments are able to extract data from individuals. During major protest movements around the world, such as the Arab Spring Crisis, The Occupy Protests, & The Umbrella Movement, governments were able to extract data from mobile phone users. Moreover, communication and other online correspondence were routinely blocked or tracked to dissuade protesters. While laws exist in most nations to protect search and seizure of physical property, such laws often do not abide by digital property. Therefore, governments may also utilize such data to curb dissent and shape public opinion through censorship.

The recent trend in countries to survey their populations with the excuse of preventing violence from terrorist groups has allowed governments worldwide to monitor the activity of their citizens online. The legality behind these actions will depend from state to state.

Government officials have noted the importance of monitoring systems in order to be able to gain evidence of potential threats and keep us safe. They have also expressed the need for such a system to gather and analyze vast amounts of data that can help uncover patterns or identify potential threats to national security. They have also invoked the argument that “in order to find the needle in the haystack, you need access to the whole haystack” i.e in order to find the details of the threats, you need to access the data of all individuals at (almost) all given times

While on the other hand, privacy advocates have voiced their concerns that such activities might be used as an excuse for a further expansion of the already extensive surveillance powers enjoyed by intelligence agencies worldwide and then might be used for exploitation. They worry that such powers may infringe upon individuals' digital privacy rights and be used for purposes beyond legitimate national security concerns.

Therefore, the debate surrounds the balance between privacy and security in the context of surveillance and data

In 2018, reports began to emerge that Facebook, one of the largest social media platforms in the world, was a tool for spreading hate speech and inciting genocide in Myanmar. From fake information aimed at inciting rage against minority communities, to posts calling for 'ethnic cleansing', Myanmar was quaking under the weight of Facebook's wide reach and misuse in the country. Similarly, social media also played a role in the violent protests under the label "Stop the Steal" in the USA. India wasn't far behind either, when protests against the Citizenship (Amendment) Act took a drastic turn when several social media accounts were created to incite hatred against minority groups. Soon, governments began voicing their concerns and initiating action against misinformation, incitement and criminal activity on social media. In the midst of situations like these, several countries stirred the need for content moderation, regulation of social media and balancing free speech with harmful content.

However, the question arises: Is this need actually legitimate? Or is it just a way of suppressing opposing views?

It is critical that approaches to surveillance & data collection are revisited to increase efficacy. In doing so, it is also imperative to keep in mind transparency and fairness for all to achieve the ultimate objective: foster individual freedom, fight potential threats, and harness accountability of all stakeholders.

The Government's approach to surveillance & collection of data is fueled by the increase in fake news, corporate rivalries, use of abusive language, defamatory and obscene content, disrespect to religious sentiments, 'anti-national' elements, public order, and the like.

Multiple provisions within the law allows governments to directly or indirectly (by issuing orders to intermediaries) to collect & share user data or take down information hosted by them on certain specific grounds – interest of sovereignty and integrity of the State, defense of the State, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offense relating to these grounds. Such provisions have been vastly criticized for the imbalance they inflict on the power of the government and the right to freedom of speech and expression and the right to digital privacy.

While such provisions sought to increase transparency in the way governments & companies collect & use user data, they must be understood in the backdrop of the allegations of bias levied against prevention of arbitrary censorship & collection of data. The usage of the unfettered power under such provisions essentially circumvents the procedural safeguards provided for data collection & usage – if any of them even exist in the first place. Moreover, while such provisions encourage fairness and transparency, these safeguards become questionable when they do not apply to government-action. In such a scenario, when surveillance & collection of data is done on the basis of arbitrary directions issued by the government, procedural safeguards are lowered, and the underlying purpose of such safeguards may be lost.

Mass surveillance also obstructs the separation of powers, as the executive branch is able to carry-out its operations without sufficiently stringent oversight from the two other powers - the legislative and the judicial. Mass surveillance powers lack effective independent authorisation, as the ability to surveil is authorized in bulk instead of with regard to each instance of wrongdoing. It creates an environment of threat and suspicion that is incompatible with democratic values and principles, where in the eyes of the state, all individuals become guilty until proven innocent.

Finally, mass surveillance negatively affects other human rights and freedoms, as unjustified interferences with privacy prevent the enjoyment of other rights and they often provide the gateway to the violation of the rest of human right, including freedom of assembly, freedom of expression, freedom of movement, principle of non discrimination, as well as political participation.

Regulation of Intermediaries

Over the past decade, tech companies have risen to become some of the most large & valuable organizations in the world, all while operating with little formal, structured government oversight. But this lack of oversight has come at a cost. Today's patchwork of privacy laws and industry self-regulation lack transparency and coherence: The combination doesn't go far enough to protect the billions of people worldwide who now rely on the products and services tech companies produce.

A growing chorus of businesses, lawmakers, and regulators are now calling for big tech companies to be broken up, while tech executives are asking for closer government regulation.

Increased regulation can provide clearer guidelines and rules for companies to operate within, offering more stability and predictability. Moreover, it can address public concerns about privacy, data protection, and other ethical issues, enhancing trust and accountability. Lastly, closer government regulation may also help alleviate some criticism and pressure from lawmakers and regulators, potentially reducing the likelihood of drastic measures such as breaking up companies.

So, what is the right way to regulate the tech industry?

One way that governments can put tech companies on a level playing field, would be to introduce a regulator for the tech industry in their country. Having a regulatory regime with nationwide statutes and clearly defined rules of engagement would also cut the cost of innovation while holding companies accountable for mitigating abuses of their inventions, ranging from criminal acts like recruitment of terrorists and child pornography to socially harmful acts like sharing user data and facilitating the spread of fake news. For a national tech regulator to be effective, it would need to adopt regulations and new supervision methods capable of staying ahead of the potential threats posed by accelerating technological change. The first country to figure out the best way to regulate the broader tech industry could become the focal point for the next chapter of the world's digital revolution. Drawing on lessons from other regulated industries, we propose several ideas for how to accomplish this with big tech.

To regulate tech, governments first need to determine the appropriate regulatory scope for the industry. Defining what is within the regulated perimeter, what is outside, and how

new companies and their activities are brought in is crucial in establishing how to engage with both regulated and unregulated areas. It provides clarity for both individuals and companies on what is protected and what is not.

We must also tackle the most pressing issues facing the industry: Establishing understandable and consistent parameters for data privacy and monetization. This regulatory goal needs to be reinforced by metrics that will enable an agency to judge if tech companies are complying with national statutes. If they are not in compliance, the agency should be empowered to carry out a specific range of disciplinary measures to encourage appropriate behaviors.

Innovations coming out of tech companies and the risks that accompany them are evolving so rapidly that it's easy for regulators to fall behind. Standards-based regulatory regimes capable of adapting to technological and social change can help regulators get out in front and stay there. Standards can be reworked for new risks, but changes to regulations and laws require extensive public consultation.

Tech companies constantly introduce new apps, other software, and hardware globally, and there's a real chance that even if cash-strapped governments implement new regulations, they won't be able to afford adequate staffing to properly enforce them. So regulators should use a risk-based approach to prioritize the companies and activities that put the most people at risk and rank the spectrum of potential threats.

Cyber Warfare

Cyber warfare refers to the use of digital attacks to disrupt the computer systems, with the aim of creating damage, death and destruction.

In a world dominated by technological growth and advancement, espionage & attacks on information systems have become a legitimate cause of concern for security. With the increasing importance of cyberspace, a number of risks have become concurrent which not only jeopardizes the benefits that cyberspace can offer but also pose a threat to the national security of a country. Cyber warfare may include attempts to access, damage, undermine and sabotage another nation or organization's information through means including but not limited to metadata acquisition, computer viruses, and denial-of-service attacks.

Cybercriminals route their communications through a variety of jurisdictions to avoid the detection of their crimes and identities. Cyber counterintelligence is important in keeping sensitive information safe and preventing subversion and sabotage. Another rising trend is the perpetuation of cyber-attacks by nationalist groups who want to spread propaganda or polarize the public towards certain topics.

These threats are multi-polar in nature and can be motivated from several directions and they may include nation states, non- state actors, proxies, and intelligence agencies. It must be noted that these attacks may also be politically, socially or religiously motivated. Additionally, according to experts, such activities when seen from a long-term perspective, can potentially cripple economies, change political views, instigate conflicts among or within states and also equalize technological capacities of nations. With the betterment in technology and information processing, hackers and other third-party entities are also benefiting. Therefore, cybersecurity and the right to digital privacy has become more central to security than ever before.

Governments are increasingly aware that modern societies are so reliant on computer systems to run everything that using hackers armed with viruses or other tools to shut down or disrupt those systems could be just as effective and damaging as a traditional military campaign using troops armed with guns and missiles. Moreover, unlike traditional military attacks, a cyber attack can be launched instantaneously from any distance, with little obvious evidence of any build-up, unlike a traditional military operation. Such an attack would be extremely hard to trace back with any certainty to its perpetrators,

making retaliation harder. As a result governments and individuals worry that digital attacks against vital infrastructure will give attackers a way of bypassing traditional defenses, and are racing to improve their security & privacy. However, they also see the opportunity that cyber warfare capabilities bring, offering a new way to exert influence on rival states and individuals without having to put soldiers at risk. The fear of being vulnerable to the cyber weapons of their rivals plus a desire to harness these tools to bolster their own standing in the world is leading many countries into a cyber arms race. These issues have been troubling the international community for years.

Future wars may see entities using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles. Therefore, a shadowy world that is still filled with spies, hackers and top secret digital weapons projects, cyber warfare is an increasingly common and dangerous feature of international conflicts. The combination of an ongoing cyber warfare arms race and a lack of clear rules governing online conflict means there is a real risk that incidents could rapidly escalate out of control.

The different viewpoints of states concerning the complexity of technology, the wide ownership of cyberinfrastructure, and the applicability of international law in cyberspace are relevant in the States' inability to reach consensus about the right to digital privacy.

What is the definition of a cyber-attack and under what conditions can it be labeled as an armed attack? As aforementioned, terms such as self-defense, cyber-attack and cyber war must be agreed upon by the international community. The thresholds must be set to define when a cyber-threat is a mere sabotage and when it constitutes a cyber-attack which can be considered an armed attack.

Some of the most common forms of cyber crimes are listed below:

Unauthorized Access: It refers to access of someone's data without the right authorization of the owner and disturbs, alters, misuses, or damages the data or system. In the physical world, acts of unauthorized access might be compared to trespass. In 2016, the Democratic National Committee (DNC) in the United States was hacked. The breach involved unauthorized access to the DNC's email server and led to the release of sensitive emails and documents during the U.S. presidential election campaign. The U.S. intelligence community attributed the attack to Russian state-sponsored hackers.

Espionage: It can be defined as the use of information technology systems and networks to gather information about an organization or individual that is considered secret or confidential without the permission of the holder of the information. Cyber espionage is conducted by a wide range of actors, including individuals, groups, companies, and even States.

Sabotage: Committing sabotage can be as simple as deliberately infecting a computer with a virus to keep authorized users from logging in. Although not always, much computer sabotage involves the use of malware, such as bots, worms, viruses and other spyware, which enables hackers to gain illegal access to personal data. Apart from theft of services and wire fraud, such sabotage facilitates pedophiles who stalk children online at school and at home, identity thieves who duplicate fake IDs for illegal immigrants, and home invasion rings and other criminals who use malware to identify potential victims.

Case Studies

NOTE: This following is a non-comprehensive and non-exhaustive list of case studies related to the agenda. If you want to get a better understanding of them, it is recommended that you conduct yourself independently.

Cambridge Analytica Case

In March 2018, Facebook was caught in a major data breach scandal in which a political consulting firm – Cambridge Analytica – pulled out the personal data of more than 87 million Facebook users without their consent. The data was allegedly used in favor of the US Presidential candidate, Donald Trump, during the 2016 elections. Further, it was found that the data was also misused to influence the Brexit referendum results in favor of the Vote Leave campaign. The tech giant's reaction to the scandal was reportedly clumsy, defensive, and confused. When Facebook got to know about the data breach, it allegedly did not do anything and waited for months to send orders to Cambridge Analytica to delete all the data. Further, the company did not follow up to check whether the illegally acquired data had been deleted. The scandal put Facebook in a situation where it was left facing the ire of millions of Facebook users, lawmakers, and advertisers. Further, the company's share value also dropped after news of the data breach broke out. There were several challenges facing Facebook, including hate campaigns running against it and lawsuits filed for the breach of users' privacy protection. After the data debacle, analysts believed that it would take a few years to fix the problems caused by the leakage of users' private data**.**

Pegasus

In 2019, Facebook sued the NSO Group, an Israeli technology firm. They alleged that NSO's spyware, Pegasus, was used to spy on users of Facebook's messaging platform, WhatsApp. The spyware could be downloaded onto a mobile device, without the user knowing and compromising his/her privacy. The NSO Group claims that they only sell this spyware to governments. During a 2019 lawsuit, it was alleged that at least 40 Indian citizens were on the list of potential snooping targets including journalists and Dalit and Adivasi activists. This implied that the Indian government had purchased and used this spyware. On July 18th, 2021, new allegations were made by the 'Pegasus Project' – an international consortium of 17 media organizations and Amnesty International. They leaked a list of 50,000 phone numbers which were potential targets for the spyware. In

India, The Wire, an online news reporting agency, published the Project's findings. They alleged that traces of the spyware were found on the devices used by the editors-in-chief of The Wire. Such traces were also found on the device of Prashant Kishor, a political strategist who most recently worked with the Trinamool Congress in West Bengal. Another potential, though unconfirmed, targets in this list included opposition leader Rahul Gandhi, Supreme Court judges Ranjan Gogoi and Arun Mishra and Union Minister Ashwini Vaishnaw.

Edward Snowden Case

Edward Snowden is a former National Security Agency (NSA) contractor who made headlines in 2013 by leaking classified documents revealing the extensive surveillance programs conducted by the US government. Snowden's disclosure unveiled the scope of mass surveillance activities, both within the United States and abroad, conducted under the umbrella of national security. Snowden's revelations exposed programs like PRISM and Boundless Informant, which collected vast amounts of personal data from phone calls, emails, and internet communications. The leaked documents triggered a global debate on the balance between national security and privacy rights. Supporters view him as a whistleblower who exposed government overreach and violations of privacy rights. Critics, on the other hand, argue that his actions endangered national security. The impact of Snowden's disclosures has been far-reaching. They prompted legal reforms, such as the USA Freedom Act, which aimed to curtail bulk data collection. The revelations also led to increased public scrutiny, demands for transparency, and calls for stronger privacy protections. The Snowden case raised significant questions about the role of surveillance, the power of intelligence agencies, and the protection of individual privacy rights in the digital age. It highlighted the need for ongoing discussions on striking a balance between national security and civil liberties, as well as the evolving nature of government surveillance practices in the modern era.

Israeli Hackers Conduct DDOS Attacks Against Palestine

10 Israeli hackers organized together to launch an attack against Palestine in October 2000 during a period of conflict. DOS attacks were launched on computers owned by Palestinian resistance organizations (Hamas) and Lebanese resistance organizations (Hezbullah). Anti-Israel hackers responded by crashing several Israeli web sites by flooding them with bogus traffic. In March 2013, South Korea's cyberspace came under a wave of cyber-attacks. Information systems of major broadcasting corporations and banks were hacked. According to an estimate, it cost South Korea £500m. The European

Defense Agency (EDA) is progressing towards a more consistent level of cyber defense capability across the European Union.

People's Republic of China (PRC)

China is one of the countries with the largest amount of internet filtering nationwide. All internet trafficking in China is monitored and can be subjected to interruption by the PRC authorities. In China, there are a few requirements for internet providers such as that they must all maintain records of up to 60 days about internet access that can be requested at any point by the Chinese authorities, they are required to establish specific censorship and have got to monitor content. All these things could be considered breaches of the right to privacy as the Chinese authorities are constantly reviewing and analyzing the internet usage of citizens and could potentially have access to personal information. China is the major party in Internet censorship worldwide. They are known to be strict and controlled in what they are allowing their citizens to see. In 2002, The Internet Society of China, a non-governmental organization (NGO) that includes members from all over the Internet business including researchers and schools, launched the Public Pledge of Self-Discipline for the Chinese Internet Industry. It was set in place as an agreement between the Chinese Internet Industry and companies who operate sites in China to prevent transmission of information to do with breaking laws or suspicious threats. It has been enforced strictly, as without signing on to this agreement you may not receive an official license to post Internet content. China is therefore constantly reviewing and analyzing citizen's use on the internet, perhaps having access to personal information which could be seen as breaking laws of privacy.

Privacy International

It is a London based Non-Governmental Organization (NGO) which was founded in 1990. The organization works with a few European Union (EU) and United Nations (UN) agencies with the goal of helping mitigate infringements on personal privacy through examining the actions of governments and surveillance technologies. F) Open Rights Group

The Open Rights Group

It is another UK based NGO which focuses on the actions of governments, particularly that of the UK, regarding their collection and distribution of personal information. The group embodies a legitimate campaign to help governments better understand privacy

issues facing individuals. The organization is mainly funded by individuals who pay a subscription fee.

Alibaba

In November 2019, an attack hit Alibaba's Chinese shopping website Taobao that impacted more than 1.1 billion pieces of user data. The attack happened over eight months as a Chinese software developer trawled the site, secretly scraping user information until Alibaba noticed what was happening. The stolen data included user IDs, mobile phone numbers, and customer comments. While the hacker didn't get ahold of encrypted information like passwords, the breach was severe enough that the company notified the police. Because it happened in China, the full consequences of this attack will likely never be made public. But it's an example that makes a strong case for better monitoring of systems and networks.

Existing Legal Frameworks & Documentation

NOTE: It is recommended that you read these documents independently yourselves thoroughly. It will not only familiarize you with best practices but also highlight gaps which you can bridge through the arguments you present in committee. Additionally, you may read existing legislation, not only domestic but also international & multilateral, related to the right to digital privacy & the process of data collection & surveillance. Again, a strong understanding of these will enable you to form better arguments in the committee

Universal Declaration of Human Rights, 10 December 1948

The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected and it has been translated into over 500 languages. The UDHR is widely recognized as having inspired, and paved the way for, the adoption of more than seventy human rights treaties, applied today on a permanent basis at global and regional levels (all containing references to it in their preambles).

International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, 16 December 1966 (A/RES/21/2200)

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty that commits nations to respect the civil and political rights of individuals, including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial. It was adopted by United Nations General Assembly Resolution 2200A (XXI) on 16 December 1966 and entered into force on 23 March 1976 after its thirty-fifth ratification or accession. The ICCPR is considered a seminal document in the history of international law and human rights.

UNGA Resolution 53/70 on IT & Communications in Relation to International Security (1999)

The 1999 GA resolution 53/70 recognized the importance of information technology and communications in international security. It highlighted the potential benefits of utilizing these technologies while acknowledging the need to address associated risks and threats. The resolution called for international cooperation and the development of norms and principles to guide states in using information technology and communications responsibly. It emphasized the promotion of confidence-building measures and capacity-building efforts to enhance security in cyberspace. Furthermore, the resolution encouraged member states to strengthen their national capabilities to prevent and respond to cyber threats and attacks.

Budapest Convention on Cybercrime (2001)

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation. It also contains a series of powers and procedures such as the search of computer networks and lawful interception.

Resolution on the Right to Privacy in the Digital Age, 18 December 2013 (A/RES/68/167)

The resolution affirmed the importance of protecting privacy in the context of digital technologies. It recognized that the right to privacy applies offline as well as online. The resolution emphasized the need for states to respect and protect individuals' privacy rights while ensuring the free flow of information. It called for the review of legislation, practices, and procedures related to surveillance and data collection to ensure their conformity with international human rights standards. Additionally, it stressed the importance of international cooperation in addressing privacy challenges in the digital age.

African Union Convention on Cyber Security and Personal Data Protection (2014)

The African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014, is a regional treaty designed to address cyber security and protect personal data

within Africa. The convention establishes a legal framework to combat cybercrime and harmonize legislation across member states. It emphasizes the importance of privacy rights and the responsible use of personal data in the digital sphere. The convention encourages the establishment of data protection authorities and promotes principles such as consent and data minimization. It calls for regional cooperation, information sharing, and mutual legal assistance to combat cyber threats effectively. Capacity-building initiatives are also emphasized to enhance technical capabilities in preventing and responding to cyber incidents. Ultimately, the convention aims to create a safer digital environment and foster economic development in Africa.

Developments in The Field of Information and Telecommunications in The Context of International Security, 9 January 2014, (A/RES/68/243)

It recognizes the increasing significance of information and telecommunications technologies for global security. The resolution highlights the potential benefits of these technologies while acknowledging the associated risks and challenges. It emphasizes the need for states to promote a safe, secure, and stable information and telecommunications environment. The resolution calls for international cooperation in addressing cyber threats, enhancing national capabilities, and promoting the responsible use of these technologies. It encourages the development of confidence-building measures, capacity-building initiatives, and the sharing of best practices. Additionally, the resolution stresses the importance of respecting international law and human rights in cyberspace.

Report on Privacy in the Digital Age by the UN High Commissioner for Human Rights (UNHCHR), 2014 (A/HRC/27/37)

It examines the implications of digital technologies on privacy rights. The report emphasizes that privacy is a fundamental human right and should be protected both online and offline. It raises concerns about mass surveillance, data retention, and the impact of new technologies on privacy. The report calls for transparency, accountability, and proportionality in surveillance practices, urging states to align their laws and practices with international human rights standards. It highlights the need for robust legal frameworks, independent oversight mechanisms, and effective remedies for privacy violations. The report also emphasizes the role of private sector entities in respecting privacy and encourages international cooperation to address privacy challenges in the digital age.

Panel on the Right to Privacy in the Digital Age, 17 March 2014 (A/HRC/25/L.12)

It focused on examining the implications of digital technologies on privacy rights. The panel recognized privacy as a fundamental right, both offline and online. It discussed the challenges posed by mass surveillance and the need for effective safeguards and legal frameworks. The panel emphasized the importance of transparency, accountability, and proportionality in surveillance practices. It called for greater international cooperation, dialogue, and sharing of best practices to address privacy concerns in the digital age. Additionally, the panel stressed the importance of respecting human rights and promoting privacy-enhancing technologies.

The Right to Privacy in The Digital Age, 18 December 2014 (A/RES/69/166)

It reaffirms the importance of protecting privacy rights in the context of digital technologies. It emphasizes that privacy is a fundamental human right that applies both offline and online. The resolution calls upon states to respect and protect individuals' right to privacy, while also ensuring the free flow of information. It stresses the need for clear and effective legal frameworks that safeguard privacy in the digital age. The resolution highlights the role of technology in promoting privacy and encourages cooperation among states and relevant stakeholders to address privacy challenges.

UNGA Resolution 58/32 in 2003

It created a Group of Governmental Experts (GGE) to assist the Secretary-General in drafting a report on cooperative measures to combat cyber threats and strengthen cyber security measures. The GGE has been renewed for several terms and is key in providing recommendations and guiding the work of the General Assembly and the UN Secretariat in addressing this issue.

UNGA Resolution 68/167 in 2013

It emphasized on “the right to privacy in the digital age.” The resolution notes that while states and international organizations should take measures to combat cyber warfare, cyber crime, and serious informational breaches, these should not be allowed to violate human rights, particularly one’s right to privacy

The International Telecommunication Union (ITU)

The UN agency focused on information and communication technology, is heavily involved within this topic. The ITU writes reports and recommendations on increasing technological and telecommunications access, as well as identifying emerging threats and challenges. In 2007, the ITU launched the Global Cybersecurity Agenda (GCA), a collaborative platform to encourage cooperation and information-sharing on cyber-security centered on the following five pillars: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation. The GCA is guided by the High-Level Experts Group (HLEG), a group of cyber-security experts, which provides information and recommendations on strengthening cyber security to Member States and relevant stakeholders working on this issue. The ITU also hosts the World Summit on Information Societies (WSIS), an intergovernmental forum established in 2001. While the fundamental goal of WSIS is to universalize access to ICTs, it also notes that to build a global information society, there must be “a global culture of cybersecurity” to protect users and encourage broader use and applications. In 2005, WSIS agreed to a set of outcome goals contained within the Tunis Agenda for the Information Society. The goals include expanding access to information technologies, encouraging international and regional cooperation, including capacity-building and information-sharing, and building confidence and enhancing security measures in the use of ICTs.

The General Data Protection Regulation (GDPR)

It is a comprehensive privacy regulation adopted by the European Union (EU) in 2016 and became enforceable in 2018. It aims to strengthen data protection and privacy rights for individuals within the EU. GDPR establishes a set of rules and requirements for organizations that collect, process, and store personal data of EU residents. It grants individuals greater control over their personal data and enhances their rights, including the right to access, rectify, and erase their data. The regulation imposes strict obligations on businesses, such as obtaining clear and informed consent for data processing, implementing appropriate security measures, and notifying authorities and affected individuals in the event of a data breach. The GDPR's introduction has led to significant changes in data protection practices, with organizations implementing privacy-by-design principles and conducting thorough data protection impact assessments. It has also fostered a greater emphasis on transparency and accountability in data processing operations.

Questions to Consider

- How does the right to privacy differ from the right to digital privacy? Is the right to digital privacy absolute in nature?

- How can governments strike a balance between protecting national security and respecting individuals' right to digital privacy?

- Does such surveillance prioritize other interests over that of an individual? Are those interests legitimate?

- What are some of the mechanisms or procedural safeguards in place to prevent governments from abusing the ability to conduct surveillance and collect data?

- Can governments coerce private tech companies into giving them data & then use it to serve their own purposes?

- Can the government use surveillance & data to create a political monopoly by suppressing & censoring opposing views? How can this be prevented or stopped?

- How can private tech companies balance the right to digital privacy of its users with its commercial interests, considering that targeted ads are also beneficial to the users, to an extent

- Are there any new organizations or bodies that need to be created to uphold the right to digital privacy? How do we ensure that they function in an independent & unbiased manner? What should be the mandate of such entities?

- How can governments & private companies strengthen their systems to prevent third party intervention & hacks?

- Does there need to be a difference in the way the government regulates big tech companies and small tech companies?

- How can regulations adapt and keep pace with rapidly evolving technologies and business models in the tech sector to effectively protect digital privacy rights?

- What mechanisms can be put in place to ensure that individuals have the right to control and delete their personal data held by governments & private tech companies, as well as the ability to rectify inaccuracies or inconsistencies?

- What measures can be implemented to ensure transparency and accountability in the data practices of tech companies, such as providing clear privacy policies and facilitating user access to their own data?

- Even if legislation to uphold & enforce the right to digital privacy is passed, how do we ensure accountability & track whether governments & private companies follow the legislation?

Answer the following questions and you'll understand the concerns one will have while surveillance is kept or debated

- Does the technique cause unwarranted physical or psychological harm?

- Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, spatial border)?

- Does the technique violate trust i.e assumptions that are made about how personal information will be treated such as no secret recordings?

- Is the tactic applied in a personal or impersonal setting?

- Does the technique produce invalid results?

- Are individuals aware that personal information is being collected, who seeks it and why?

- Do individuals consent to the data collection?

- Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?

- Do the principles of minimization, necessity, and proportionality apply?

- Are people aware of the findings and how exactly they were created? Are there means for discovering violations and penalties to encourage responsible surveillance behavior?

- Are there procedures for challenging the results, or for entering alternative data or interpretations into the record?

- If the individual has been treated unfairly and procedures are violated, are there appropriate means of redressal? Adequate data stewardship and protection: can the security of the data be adequately protected?

- Is it likely to create precedents that will lead to its application in undesirable ways? Is the right to privacy absolute or conditional?

- Are there negative effects on those beyond the subject?