Message from the Executive Board

Greetings! This is Kanav Garg, and I'll be the Co-chair for the United Nations Cyber Security Task Force along with Naman Anand. We are pleased to welcome you to JIRSMUN 2016.

In order to improve debate and assist you with research, we've prepared this background guide. We hope that you find this guide useful in finding some direction for your research and draft your position papers. The executive board strongly recommends that you use this guide only as a guideline and explore-in depth the agenda and your country's policies regarding the same. Note that position papers are to be submitted before committee begins in standard MUN format.

We look forward to committee and can't wait to see creativity bloom. Please feel free to contact any of us on Facebook for any queries or questions.

Agenda 1

The Right to Privacy in the Digital Age

"Combined and collective action by everybody can end serious violations of human rights…That experience inspires me to go on and address the issue of Internet [privacy], which right now is extremely troubling because the revelations of surveillance have implications for human rights…People are really afraid that all their personal details are being used in violation of traditional national protections."

With an astounding 2.9 billion users or approximately 40.4% of today's entire global population, the Internet has become a primary medium for sharing information, news, political debate, and activism in both the private and public sectors. The Internet has provided a platform for those who seek to exercise their human right of freedom to information, granting them global access to ideas and materials via real-time communications. However, though there are clear advantages to the Internet, technology is increasingly being used by national governments and private corporations in ways that infringe on the privacy of citizens all around the world, disregarding and restricting the fundamental right to privacy. Due to the increasing societal reliance on the Internet in our daily lives, there has been a continuous recognition and there is a growing need for the formation of privacy guidelines and enforceable international law to govern the use of technology. The importance, as well as the complexity, of establishing a cohesive international standard has become apparent through recent constitutional and legal violations, such as mass surveillance programs and data collection activities, which have failed to recognize individual privacy rights. To put it another way, there has been widespread failure to respect the human right to security of privacy and protection "online" in the same capacity that is afforded "offline." While international law holds Member States accountable for enforcing the protection of human rights online, corporations in the private sector must also play a supporting role by upholding these same protections. Internet usage is just one example of media protected by the human right to privacy, as defined in Article 12 of the Universal Declaration of Human Rights (UDHR) (1948). Violation of the human right to privacy, especially when committed by means of data collection and mass scale surveillance, also infringes on a crucial component of the right to freedom of expression, and has thus prompted Member States to present the topic for discussion in the United Nations (UN) General Assembly Third Committee (Third Committee). In 2013, this resulted in the first Internet-related resolution being adopted by the General Assembly, resolution 68/167 (2014) on "The right to privacy in the digital age." The Third Committee discusses all matters of social, humanitarian, and cultural affairs, and as such deals with human rights issues, such as the right to privacy. In order to address the challenges that remain on this topic, it is important to examine some key definitions and topics including the principle of privacy as a human right, the effectiveness of international and national frameworks currently in place, and the techniques that must be implemented to ensure a transparent balance between government data collection for the purposes of security versus unconstitutional surveillance.

Privacy and surveillance

Before venturing in to a debate regarding the right to privacy, it is beneficial to consider some definitions of what is thought to constitute privacy. According to the Oxford dictionary, privacy is "a state in which one is not observed or disturbed by other people". According to Cornell professor Daniel Solve, this defection can be expanded to encompass a much more detailed structure on what can be seen as privacy: "Privacy is about respecting the desires of individuals where compatible with the aims of the larger community. (…) Privacy is not merely an individual right – it is an important component of any flourishing community." Hence, the mere understanding of what privacy is varies greatly depending on who is asked. Therefore, it may be beneficial to consider what each country believes has the right to be protected (particularly, whether the right to privacy is a domestic concern or a more universal concern). Question legality of state-sponsored infringement of privacy "Unwarranted government

surveillance is an intrusion on basic human rights that threatens the very foundations of a democratic society." - Tim Burners Lee Wired "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." - Benjamin Franklin

Many consider surveillance a necessary practice for State security. Aside from defense, surveillance, specifically communications surveillance, is now being used for commercial purposes as well. This practice, however necessary or legitimate, interferes with certain fundamental human rights, particularly the right to privacy that each entity, whether individual or business, expects to be able to exercise .With the utilization of technology increasing, surveillance has reached a vast scope that has surpassed all previous expectations. Whereas technology has transformed the field of surveillance and monitoring, it has increased the risk of these actions infringing upon the right to privacy. Surveillance has risen dramatically in recent years as governments label it as necessary under the ever-present threat of terrorism but with no international framework or regulation for this surveillance, there is no guarantee that these state-sponsored acts are indeed following international human rights laws. After the leaks by Edward Snowden on the actual scope of the USA's National Security Agency's surveillance, an ongoing debate has started on whether or not the surveillance conducted is actually for the said purpose and whether a promise of safety can outweigh the compromising of fundamental human rights.

It has become evident that other more prioritized rights since have overshadowed the right to privacy even before surveillance has been conducted. A specific example of this would be the United States' Constitution, which does not mention a specific right to privacy but has the right exist in the 'penumbra' of several other rights. The general population, however, demands for an international legal framework that establishes a guide for surveillance and under which circumstances it can occur. Before the adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those barriers to surveillance have decreased and the application of legal principles in new technological contexts, as surveillance becomes more complex, has become unclear.

The explosion of digital communications content and information about communications, the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale. As technologies that assist State communications surveillance advance, nations are failing to ensure that laws related to communications surveillance adhere to international human rights and appropriately protect the rights to privacy and freedom of expression. The frequency with which States are seeking access to both communications content and communications metadata is rising dramatically but without adequate scrutiny. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection.

Role of Private Corporations in Digital Privacy:

Because a vast amount of digital data is housed by private multinational corporations, the role they play in the protection of data privacy is worth thorough examination. As of 2013, Google, Microsoft, Apple, and Facebook house a total of 1200 petabytes of data. Two distinct mechanisms threaten the privacy of data: (1) the ability of governments to arbitrarily request access to personal data and (2) insecure storage and sharing of this data with other corporations that could result in it being obtained by ill-willing individuals. As nations with developed infrastructure have become more aware of potential

problems with digital privacy, many have begun to develop a multitude of laws and regulations to be adhered to by data companies operating within their borders. Unfortunately, these regulations often contradict each other and are confusing.

Several large multinational companies like Facebook and Google have expressed the difficulty they face in adhering to these regulations. Companies sometimes try to alleviate this problem by setting their privacy standards to "the highest watermark" set by a country or region with the strictest privacy policies and applying this universally. This practice, however, is still open to flaws and contradictions. The recent heavily publicized case in which the U.S. Federal Bureau of Investigation attempted to gain access to gain access to the iPhone has broken open a massive debate about digital privacy. The U.S. government's request from Apple was inconsistent with Apple's own internal policies and contradicted certain regulations established by the EU and other nations. In recent years, companies have found themselves under scrutiny for practices regarding either collecting too much data or not releasing data, leaving them trapped in an essentially irresolvable two-sided tug-of-war situation. Alphabet Inc., for example, is undergoing several investigations by the European Union about failing to release email records to investigators while also being investigated for collecting too much information from individuals in the first place.

Another great risk to corporate collection of data is the mismanagement of data. Many large firms provide data to partners in order to better assess the tastes and preferences of their users. Along the way, critical identifying data is often stored insecurely, vulnerable to hackers, nation-states, and other entities. Large leaks of data are often publicized in the media, but significant, though smaller, and more frequent leaks—such as the inadvertent release to criminals of the private information of 100,000 individuals by data aggregation company ChoicePoint—highlights these problems. In South Korea, the start of 2014 was met with an enormous data breach in which 104 million data items were stolen from three major credit card companies despite South Korea having some of the most stringent privacy laws in the world. This highlights the significant problem of corporations continuing to subvert national and international regulations due to the costs and technical difficulties of keeping up with them. The increasingly complex techniques being used to steal data and the convoluted web of regulations digital companies must deal with point to the importance of establishing a universal standard on the storage and sharing of confidential information.

Types of Protections Needed:

Data collection and mass surveillance are the two major violations of privacy pointed to in both UN and civil society reports. Increased protections have been called for in regards to each, mostly involving clearer, stronger legislation at the national level.

Data Protection

Safeguarding the fundamental human right to privacy is increasingly difficult as information and communications technologies (ICTs) are becoming more accessible. However, by this same reasoning and due to rapidly changing technological capabilities, the right to deny access to personal data must be afforded. Personal data is simply "any piece of information or a set of information that can personally identify an individual or single them out as an individual." For example, information such as an Internet Protocol (IP) address used to identify individual computers or health records can be considered personal data.

Monitoring and Surveillance of Communications

Beyond collecting data, as alluded to above, what constitutes a legitimate monitoring activity and the limit of surveillance is one of the more controversial aspects of privacy rights efforts. Although many Member States have agreements that prevent interception of oral and digital communications without judicial approval, government agencies throughout the world continue to push for the expansion of surveillance capabilities via investigations that are either targeted or mass communications. Surveillance systems have prevented acts of terrorism and allowed

Role of governments:

There remain a number of practical challenges regarding the right to privacy in the technological era. The obvious obstacle is how to respect national sovereignty and security measures within the boundaries of a legal framework that successfully reaffirms the fundamental human rights of an individual. More specifically, Member States must define explicit and valid purposes for privacy breaches. To determine this, governments must adopt clear and precise legislation that continues to protect the right to privacy. Because technology is continuously advancing, Member States should review their legislation to ensure that it does not become outdated or irrelevant. To increase transparency and public awareness, Member States should be cautious in approaching third party corporations for assistance with mass surveillance and data sharing. Since the role of the private sector is crucial, international frameworks should incorporate language that addresses human rights privacy standards and the direct effect that corporations have.

Relevant documents:

Resolution 68/167:

http://www.ohchr.org/Documents/Issues/Privacy/NV.pdf

Right to privacy in the digital age report by the UNOHCR:

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf