Cerritos Novice Conference 2020

Commission on Science and Technology for Development (CSTD)

Topic: Privacy in the Digital Age

Director: Naman Satish

October 10th, 2020

To Delegates of CHSMUN Novice 2020

Dear Delegates,
Welcome to CHSMUN Novice 2020!

It is our highest honor and pleasure to welcome you all to our 2020 online novice conference here at Cerritos High School. On behalf of the Cerritos High School Model United Nations program, we are proud to host our very first virtual novice conference, where you will become more knowledgeable on international issues, participate in intellectually stimulating discussions, and create new and everlasting friendships.

The CHSMUN program continues to compete around the world as a nationally ranked MUN program. Our delegates utilize diplomacy in order to create complex solutions towards multilateral issues in the global community. Our head chairs are selected from only the best seniors of our program, undergoing a rigorous training process to ensure the highest quality of moderating and grading of debate. Furthermore, all the topic synopses have been reviewed and edited numerous times. We strongly believe that by providing each and every delegate with the necessary tools and understanding, he or she will have everything they need to thrive in all aspects of the committee. We thoroughly encourage each delegate to engage in all of the facets of their topic, in order to grow in their skills as a delegate and develop a greater knowledge of the world around them.

Although this wasn't what we expected, our advisors and staff have put in countless hours to ensure delegates have an amazing experience at the online conference. Our greatest hope is that from attending CHSMUN 2020, students are encouraged to continue on in Model United Nations and nevertheless, inspired to spark change in their surrounding communities. CHSMUN Novice 2020 will provide a quality experience for beginner delegates to develop their speaking and delegating skills.

If you have any questions, comments, or concerns, please contact us! We look forward to seeing you at CHSMUN Novice 2020!

Sincerely,

Anjali Mani and Karishma Patel

sg.cerritosmun@gmail.com

Secretary-Generals

A Note From The Director

Delegates,

My name is Naman Satish, and I am really excited to be directing this year's CSTD committee. I have been in MUN from the first opportunity I had, starting way back in 7th grade. Each year has been better than the last, and I'm sure that this committee is going to be another great experience for all of us. I'm really excited to see your understanding of the issues I have chosen, and what kind of solutions you can find to address them. Since this is an advanced conference, I hope that you will spend some time learning the nuances of both topics. Some more fun information about me, my name means Hello! At school, I am part of the Maza Club, I serve as the Director of Technology, and I'm also part of our school's Cross Country team. I also help out on the science olympiad team, specifically working with arduinos. I'm usually introverted, but MUN is my one exception. I've also specifically chosen these topics because I believe that they relate very well to our current situation, and might end up teaching all of us more about the world we are in.

Sincerely,

Naman Satish

Director, CSTD

Committee Introduction:

The Commission on Science and Technology for Development, CSTD, is one of the nine Economic and Social Council, ECOSOC, Commissions . These Commissions report back to ECOSOC about their specific field, and influence ECOSOC's position on key policies. The Commission on Science and Technology for Development was founded in April, 1993, and replaced the Intergovernmental Committee on Science and Technology for Development. The initial purpose of the CSTD was to provide an open platform where member states could collaborate with NGOs and actors in the science, technology and medical space. The CSTD was to provide the UN with high-level information through analysis and policy advice to guide the future work of the UN, to develop holistic and future proof policies, and to create reasonable regulations regarding technology. In a world that is developing at different rates, the CSTD aims to help those who are left behind to benefit from science and technology to address challenges. Today, the CSTD comprises of 43 member states from each region of the world. The CSTD's specialization is its role in improving the UN's ability to solve problems with technology, and specifically identifying technologies to assist the humanitarian crises, or the UN in achieving the SDG Goals.

TOPIC: Privacy in the Digital Age

Background:

The digital age has revolutionized the way that humans interact with the world around them. Constant technological advances in social media, phones, computers, and WIFI have allowed for the creation of more sophisticated technology. These advances have also led to digital technologies dropping in price and becoming widely affordable, leading to nearly 60% of the global population being active users of the internet. It would be logical to think that since such a large portion of the global populace uses digital technology, it would be regulated and people's privacy would be protected. However, the reality is the opposite.These technological advancements have also created an environment in which it is easier for individuals, modern information and communications technologies (ICTs), companies, and even governments to breach your sense of privacy.The Universal Declaration of Human Rights creates and ensures the human right to protection from the interference of your "privacy, family, home, or correspondence", the ongoing malicious evolution of digital technologies and nefarious practices have occurred so frequently over the past decades that numerous private, national, international, and UN agencies have displayed concern and undertaken efforts to protect these rights. However, the digital age has brought more than one practice that threatens our right to privacy. There are multiple dangers to this right to privacy including data collection practices, facial recognition technology, lack of transparency, and nationalized data collection programs. The most common of these practices is data collection. Data as minute as the location of a cursor during page reloads to the time between keystrokes to the user's location can be logged and collected with ease. From this data, companies can identify numerous traits about users, breaching their trust. There is no foreseeable end to this practice of data collection, and under current practices it will continue to be used with oversight with unknown protections. This practice of data collection also frequently occurs without the explicit consent of the individuals it targets, and has been known to target vulnerable communities. Additionally, with national oversight still developing, it is mostly up to the private sector on how to both regulate and shape the evolution of data collection. These data collection schemes can be international, as was revealed by Edward Snowden in 2013. The classified documents he provided proved that the NSA, the U.S National Security Agency, was collecting emails and messages, searching their content, mapping the location of electronic devices, and pinpointing targets for further investigation. Data Collection is dangerous, even when the data is not processed due to the ability for it to become leaked. For example, Clearview AI, a facial recognition company, had been collecting user face data to develop better algorithms. In 2020, its data center was breached, allowing hackers to have access to 3 billion personal photos. Numerous others have faced similar attacks and exposed thousands of user records to hackers. This can even extend to national espionage, as shown in Huawei's activities in Italy, where Huawei fixed-line network equipment was found to have unspecified backdoors. However, this danger doesn't just apply to data from when users use their digital devices. This danger exists anytime a person is in the vicinity of a camera. In recent years, facial recognition has grown from a science fiction fantasy, to being

miniaturized enough to be placed in a phone. This technology poses large threats to your physical privacy, as it allows for your identification in nearly any scenario. Facial recognition can, and has been, expanded to recognizing people from nearly any action. General privacy of location is threatened from these technological advancements. Another issue facing the right to privacy is the lack of transparency from the private sector and other groups involved with digital technology. Although there is no defined way for a group to act transparent, it is clear that under the current regulation and situation, the general public has little to no way of understanding what specific information is collected and what actions are being performed with it. For example, companies such as Facebook have been routinely caught violating the privacy of their users by collecting and selling large volumes of their data. Studies show that upwards of 70% of users were not aware of the companies Facebook was selling their information to. Transparency would entail companies disclosing data collection practices, how it is processed, and who it is given to and for what price.

United Nations Involvement:

There have been multiple attempts from the United Nations to resolve this issue. The first of these attempts was a resolution in 2014 which called on nations to protect their citizen's right to privacy. This was done by specifically asking for member states to take a look at procedures and policies that they previously had in place, and to reform ones that might negatively impact surveillance for citizens. However, this resolution was not followed by many member states, who have refused to review their policies and ensure they are compliant with the UDHR. The United Nations already possess the legal framework required to ensure that member states follow this resolution, the ICCPR, however they have not used it to this day to protect citizens. Instead on November 16, 2016, the United Nations passed yet another resolution asking member states to comply with the ICCPR and ensure that their domestic policies are compliant. This resolution goes a step further in actually highlighting the role of the private sector in this debacle. This resolution calls for member states to place and maintain sanctions to prevent the private sector from committing their numerous violations of this right to privacy. This call for action was justified from the United Nations Guiding Principles on Business and Human Rights, which requires member states to protect against companies who frequently abuse human rights. It additionally calls for companies to begin to respect the right to privacy, and properly inform users about what data is collected, and how it affects their right to privacy. There have also been global suggestions to the United Nations from data protection authorities around the globe. One of these groups is the International Conference of Data Protection and Privacy Commissioners, which is made up of high ranking data privacy enforcement members from individual nations. Every one of their proposed protection frameworks have been implemented for the past 15 years, and they created a resolution specifically for ensuring privacy in the digital age in 2014. The United Nations has also created their own special rapporteur on the right to privacy in the digital age. This rapporteur conducts visits to nations to examine their specific protections in regards to privacy. Additionally this rapporteur collects information and complaints about alleged

violations of privacy, and then takes actions if it falls within its jurisdiction. This action is specifically done through Allegation Letters which allow them to send reports to member states asking for them to explain these actions. This is then taken back and used in their report to the General Assembly and Human Rights Council. The CSTD has also taken action by publicly mapping international policies regarding internet use. In their document, the CSTD highlights mechanisms that can be used to protect the right to privacy and what the current international situation is. This information is then taken by UN Agencies to create more effective legislation that can address gaps in international policy.

Bloc Positions:

Western:The Western Bloc has access to specialized digital technology, and it is heavily integrated in their daily life. Additionally, the Western Bloc leads in the development of these technologies, and therefore has control over what kind of safety requirements devices should have for users. However, the Western Bloc also has nations that frequently commit right to privacy abuses, and frequently fails to subdue and punish companies who skirt regulations and abuse these rights as well such as the U.S. Certain regions of the Western Bloc have developed legislation that takes a step in the right direction, namely the GDPR (General Data Protection Regulation) which enforces its guidelines with strict fines. However, some members of the Western Bloc have passed this responsibility to preexisting commissions, such as the U.S's Federal Trade Commission. The Western Bloc's policy will be to expand current frameworks which protect the right to privacy, however it will also place guidelines to protect national security.

Latin America and Caribbean: The Latin America and Caribbean Bloc will find parts of itself lacking access to digital technology, however it is rapidly modernizing which is exposing more of its citizens to the internet than ever before. This new influx of users poses a large threat to this bloc as many of them will be under informed on the dangers of losing their privacy. The Latin American and Caribbean's position will be to further expand informational programs for their citizens and create national policies to protect the data of their own citizens.

African: The African Bloc is similar to the Latin American bloc in the way that parts of the bloc lack access to digital technology, but modernization is bringing technology to them at affordable prices. This new technology has great potential for this bloc as it allows for its members to improve their quality of life through numerous programs that assist them digitally. However, many of these programs also collect data from their users to improve their platform. Therefore, this bloc's focus will be to place restrictions and create frameworks to prevent private companies from abusing the right to privacy, while still being lenient enough to not turn away helpful companies.

Asian-Pacific: The Asian-Pacific Bloc serves as an example of how modernization can impact nations differently. Members of this bloc are spread out on their own nation's policy for the right

to privacy, however the majority of them currently have little to no legislative protection for the right to privacy. Members from this bloc have openly demonstrated their capacity to violate these human rights, however others will be focused on creating national policies to reduce or create transparent national surveillance systems. Additionally, members from this bloc may be focused on the anonymization of digital technology users, effectively rendering data collection techniques useless as they cannot be attributed to a single user.

Basic Solutions:

Although the right to privacy has been under attack for the last two decades, there has been little to no effective action taken by the UN, member states, or the private sector. There is no all-encompassing solution to ensuring the right to privacy for every citizen, nor can it be achieved immediately. It is important that there is a sloping transition from our current situation to protecting the right to privacy of every citizen. There is no one NGO which will make every company compliant with privacy regulations, nor is there a holistic technology that will be accepted by every nation. Instead, the solution should come from bloc requirements and situationally specific goals, focusing on reversing the policy in certain nations, while being flexible in assuring nations have the capability for some sort of transparent surveillance. Some solutions that will set you on the correct path of where to look are legislation reform, public awareness, stronger penalties, and whistleblower protections.Legislative reform is one way that we can protect the right to privacy. Creating effective international and domestic laws against abusing the right to privacy will create awareness about the issue while also reducing the amount of bad actors. These legislative reforms would need to be updated frequently, as technology advances rapidly, it is important that the law reflects those new changes. Another way to protect the right to privacy would be to inform individuals who are learning how to use digital technologies, and those who already have their data collected. By spreading public awareness about the collection of data, citizens can learn about the dangers to their privacy and begin to take action to prevent it.Whistleblower protections are key to ensuring that future abuses of the right to privacy are revealed. There is currently little international protection for these whistleblowers, and corporations frequently go unpunished after their actions have been revealed. Some ways that we could protect whistleblowers is by providing international anonymity, protection, financial aid, or allowing them to take part in preventing a future abuse that is similar.

Questions to Consider:

1. What current private sector companies have been known to skirt regulations, and what actions should they take to change?
2. What methods can be employed to speed the creation of legislation to protect these rights?
3. How will countries be encouraged to create domestic legislation when it might interfere with their own surveillance operations?
4. Which emerging technologies have potential to protect the right to privacy?

5. How will your solutions address the sovereignty of countries, and what legal frameworks can be used to enforce countries to make changes.
6. How can your solutions be better adapted to take into account the variety of economical constraints that countries may have?
7. What solutions are already in place in your country, and can they be expanded globally?

Sources:

1. Chin, Caitlin. "Highlights: Setting Guidelines for Facial Recognition and Law Enforcement." *Brookings*, Brookings, 9 Dec. 2019, www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/.
2. Clement, J. "Digital Users Worldwide 2020." *Statista*, 24 July 2020, www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Almost 4.57 billion people were,percent of the global population.
3. "Commission on Science and Technology for Development." *Commission on Science and Technology for Development | Digital Watch*, dig.watch/actors/commission-science-and-technology-development.
4. "General Assembly Backs Right to Privacy in Digital Age | | UN News." *United Nations*, United Nations, news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age.
5. "International Covenant on Civil and Political Rights." *OHCHR*, www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
6. Kerry, Cameron F. "Why Protecting Privacy Is a Losing Game Today-and How to Change the Game." *Brookings*, Brookings, 25 Oct. 2019, www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.
7. "New UN Resolution on the Right to Privacy in the Digital Age: Crucial and Timely." *Internet Policy Review*, 22 Nov. 2016, policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436.
8. "New UN Resolution on the Right to Privacy in the Digital Age: Crucial and Timely." *Internet Policy Review*, 22 Nov. 2016, policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436.
9. "Right to Privacy in the Digital Age." *OHCHR*, www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.
10. Savage, Charlie. "How the Law Protects Intelligence Whistle-Blowers, and Leaves Them at Risk." *The New York Times*, The New York Times, 3 Oct. 2019, www.nytimes.com/2019/10/03/us/politics/whistleblower-complaint.html.
11. "Special Rapporteur on the Right to Privacy." *International Justice Resource Center*, 25 July 2018, ijrcenter.org/un-special-procedures/special-rapporteur-on-the-right-to-privacy/.
12. "United Nations Recognition of Privacy." *United Nations Recognition of Privacy* |

Privacy International, privacyinternational.org/impact/united-nations-recognition-privacy.
13. "Universal Declaration of Human Rights." *United Nations*, United Nations, www.un.org/en/universal-declaration-human-rights/.