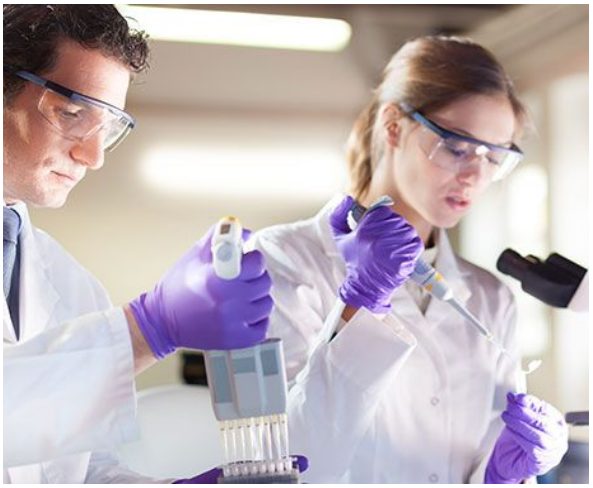
Cerritos Advanced Conference 2020

Commission on Science and Technology for Development (CSTD)



Topic A: Accelerating the Development of Medical Technologies

Topic B: Privacy in the Digital Age

Director: Naman Satish

POSITION PAPERS DUE on October 17th by 11:59 pm to Committee Email

October 24-25, 2020

To Delegates of CHSMUN Advanced 2020

Dear Delegates,
Welcome to CHSMUN Advanced 2020!

It is our highest honor and pleasure to welcome you all to our 2020 online advanced 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 advanced 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. With this strong circuit consisting of 6 schools and over 500 delegates, CHSMUN Advanced 2020 will provide a quality experience for intermediate delegates to enhance their speaking and delegating skills.

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

Cstd.CHSMUN@gmail.com

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 A: Accelerating the Development of Medical Technologies

Background:

Infectious diseases are a significant threat to the modern world due to their ability to cause widespread damage to the inhabitants of a nation with little to no warning. Even worse, oftentimes the populations most affected by these diseases live in developing nations with underdeveloped medical infrastructures, specifically due to their sparse access to medical equipment, deprecated medical technology, slow development times, and religious and economic constraints. These infectious diseases contribute to a harmful cycle that makes it hard for nations to develop medical infrastructures that can help prevent future infectious diseases. Additionally, without quick actions, infectious diseases can cause irrevocable economic damage, as in Peru's case losing $770 million when this situation could have been avoided with quick deployment of cholera medication. This problem doesn't only apply to developing nations. While they might be adversely affected by infectious disease, developed nations also frequently are not able to develop medical products quick enough to supplement other nation's requirements, develop medical solutions and technologies quick enough, and share important data. This problem is more apparent and important to solve than ever before, as the world faces an international pandemic with no solution. Currently, it takes on average 12 years and $1 billion to develop and approve medical drugs in the United States. Despite the medical field advancing greatly over the past century, the development of its products is still lagging behind. These products don't just include medicine, but treatments, new detection technologies, and information systems. Developing nations lack any incentive to develop medical technologies within their nations which is leading to a larger gap in healthcare sectors. The growing price of developing and approving medicine has locked development to certain large corporations. Therefore, it is important to find how the global community can encourage the acceleration of the development of medical technologies and what kinds of policies will help achieve this goal. Numerous studies have identified areas where current medical technologies have the capability of improving on. Some actions taken by nations specifically focus on improving development time, reducing the cost of development, and providing incentives to develop. Additionally, there are key areas where improvement will lead to the faster development of medical technologies, those improvements being to accelerate cost savings, personal healthcare, big data, mobile health and education, and technology integration. Accelerated cost savings is a development strategy that emphasizes reducing human input and simplicity, allowing for rapid and cost effective production. Personal Healthcare is a field in which medical technologies can be customized per patient, allowing patients to get treated faster and more effectively. Mobile Health and Education is a method to improve nation's with developing medical infrastructure by allowing qualified doctors to address issues around their nation and provide area specific medication and advice. Technology Integration is another development strategy that focuses on using technology that consumers already have to diagnose and provide new treatments, for example using your phone's

camera and internet connection to receive a diagnosis. There are numerous challenges that come in the way of accelerating the development of medical technologies including economic constraints. Some nations do not have the capital to support the development of medicine, which is why it may take prolonged amounts of time to develop solutions. For example, the Ebola Epidemic in West Africa in 2014 demonstrated a clear need for a vaccine, however development of this vaccine was difficult because no major pharmaceutical company had an interest in developing it.Additionally, religious views might hinder development of medical technologies in certain nations. For example, in certain nations medicines may only contain specific ingredients, or may outright be discouraged due to their origin and production. While it is important to respect religious views, it can allow for certain nations's inhabitants to act as hosts for infectious diseases.However, there is a danger that comes with accelerated medical development. Although it can lead to solutions that have outstanding short term qualities, their long term effects will not be understood. This is currently the case with the AstraZeneca Vaccination, which has been granted protection from future liability claims from its vaccine in many of the countries it plans to deploy in. There is an important balance to find between encouraging the development of medical technologies, and to also ensure that they are safe and trustworthy.

United Nations Involvement:

The United Nations has taken some bold actions in the case of the developing medical technologies. One way the United Nations has focused on this has been through supporting the development of health technologies that have the potential to address key medical issues in developing Nations.In 2003, United Nations Secretary-General Kofi Annan brought up the commitment and investment to push the limits of Information and Communications Technology, ICT, in respect to the Millennium Development Goals. The MDGs were reached partly due to the implementation of technology that had not been used before. Specifically in developing countries, the utilization and development of ICT health systems was sparse and relatively non-existent prior to the Secretary-General's interest in the field. In the following years, this greatly shifted as this technology began to be implemented in the nations even when its potential was not fully realized. Drawing upon support from the UN, aid agencies, and the private sector, e-health projects began to grow and spread. Although nations were not convinced of their success, however years after their initial implementation, these nations are benefiting from these ICT systems.The UN was able to encourage countries to begin developing their own ICT systems through providing capital for these endeavors. In return, these ICT systems have revolutionized healthcare in their regions by improving the connectivity between patient and doctor, increasing access to health information to develop better health policies, improving the training and education of doctors, and bringing further investment for e-health innovations in their region. More recently, the United Nations has pushed for this acceleration in their Tech Access Partnership program. Established on May 13, 2020, the TAP program helps address the lack of medical goods in countries with limited resources. The TAP program is accelerating the development and fabrication of medical technologies in these countries by pairing emerging manufacturers and development companies with those who have expertise in these specific regions. The TAP program's primary purpose is to address the critical shortage of medical goods

and technologies in developing countries, however it provides a broad basis upon which it can be expanded. One of TAP's current roles is maintaining product information, which means developing nations can have access to design specifications that they can improve upon. Additionally, TAP provides technical guidance to companies in overcoming manufacturing problems and avoiding regulatory hurdles. The TAP program also provides partnerships between companies in developing nations and countries that have expertise. This partnership is currently focused on developing medical supplies that are in need, however it has the greatest potential for expansion. Over the past two months, this specific part of the TAP program has increased innovation of medical devices, and has begun to fill the technological gap between both companies. The UN Technology Bank is another UN organization dedicated to improving the access to science and technology in the world's least developed nations to spark innovation. The UN Technology Bank works with groups such as the SDGIA to actively support these new innovations and medical technologies. These groups will often offer grants, professional assistance, partnership opportunities, and field tests to companies with innovative medical technologies.

Case Study: Democratic Republic of the Congo

One country most impacted by the lack of accelerated medical technologies has been the West Africa Region. With nations such as Guinea, Sierra Leone, and Libera facing upwards of 30 thousand cases and 11 thousand deaths, it is clear that something went wrong in the response to the Ebola Epidemic. Over the past 5 years, it has become clear what went wrong in West Africa, and what went wrong more recently in the Democratic Republic of the Congo.

The problem lies in the response from nations focusing on the disease and not those affected by it. Immediate response teams worked to secure the area and shut down ports, but they did not work on developing vaccines or treatments. International Aid funded a community surveillance system, monitoring for any sign of disease, but ignored the necessity to provide new medical tools and develop tools to create a sanitary environment. This security based approach to the Ebola Epidemic that emphasized deterrence, compliance, and punishment are contrary to the fundamental goals to public health. There were failures in the decision making process, slowing down response times and development of medicine. Additionally, there was little transparency and no accountability to the financial resources provided to solve this crisis.However, this experience taught the global community the importance of accelerating medical development, and what does work in the middle of an epidemic. It was clear that the correct steps were taken to establish leadership at different levels of governance. There was national leadership that focused on addressing the issue through working with neighboring countries to develop and create medical solutions, and regional leadership that focused on improving their own communities and encouraging the use of these technologies. Additionally, the importance of high-quality medical treatment became clear as prior to the introduction of blood transfusion machines to Ebola Holding Centers, it was common for children with severe malaria to die even if they tested negative because these centers could not accommodate their illness. It also demonstrated the requirement for Accelerated Research and Development Blueprints, created by WHO, which

helped provide information on how to improve research and development readiness against infectious disease threats through technology development.

Bloc Positions:

Western Bloc: The Western Bloc has access to medical technologies that are able to address the effects of modern day medical issues. Additionally, the Western Bloc is leading in the development of technology, medicine, vaccinations, and research. For example, Western Nations lead in the participation in One Health, a collaborative effort to connect multiple fields of health to develop better solutions. Additionally, both the United States and EU have drug evaluation commissions, FDA and EMA respectively, and development funds such as Horizon 2020. The Western Bloc's position will be to expand in place frameworks to provide greater incentives to nations with developing technologies, and for the expansion of partnership programs. However, this Bloc will also be focused on protecting their own intellectual property, and ensuring that products pass rigorous testing. Particular NGOs from the Western Bloc will specialize in providing assistance to companies, and assist in technological research.

Latin America and Caribbean Bloc: The Latin America and Caribbean Bloc will find parts of itself lacking medical technologies, which leads to devastating impacts when they are really needed. However due to the lackluster healthcare infrastructure, developing economies, and an overall lower standard of sanitation, developing medical technologies will have initial rough starts, but will often gain public support once they begin to reform these issues. The Latin American and Caribbean's position will be to further research medical technologies when they have the incentive to do so, and to also expand partnership programs.

African Bloc: The African Bloc diversity is apparent in its different take on medical technologies. While regions most affected by disease will often accept these technologies easily, the implementation of medical technology and its development will be more difficult elsewhere. This Bloc's position will be to use monetary aid to help develop health care infrastructure, as well as fund medical technologies that can be used in rural regions. This bloc will also find itself with innovators creating resources for health care workers from the few resources they have, which can be expanded across the world when in need.

Asian-Pacific Bloc: The Asian-Pacific Bloc has the greatest capability to rapidly develop medical technology, however it isn't common due to the regulations in place. This region will focus on the technological and medical advancements to preexisting technologies instead paired with research studies into what technologies might be most effective. This Bloc's position will be to expand medical technologies that they already have in place to developing countries, while also pushing for regulatory reform.

Basic Solutions:

There is no all-encompassing solution to the problem of accelerating the development of medical technologies . There is no NGO that has been storing all of the health care resources the world needs, nor is there a technology that can save lives for free, nor is there a solution that will work in every country. However, that is not saying there is no way to solve the problems that come with accelerating medical development. It will take a multitude of specialized groups, each focused on specific areas of research and partnerships. NGOs that have a previous history of closing technological gaps, and groups willing to fund the creation and distribution of medical technology will be key elements in any solution. Some solutions that will set you on the correct path of where to look are accelerated cost savings, personal healthcare, big data, mobile health and education, technology integration, and privacy. Accelerated Cost Savings are one way to address the acceleration of medical technology development. By reducing the amount of tasks that a user has to complete to utilize a medical product, companies can accelerate their product's approval time as well as reduce possibilities for error. Additionally, as companies invest in making their products easier to use and easier to manufacture with technology, they will be able to lower the price and invest in other technologies.Another way to accelerate the development of medical technologies is to utilize patient data anonymously. Patient data can range from X-Ray tests to simple checkups, however it provides the capability of identifying which technologies are most instrumental in improving a patient's life, and allows for future developments to improve upon previous designs constantly. Regulatory Reform is another way to accelerate the development of medical technologies. Current regulations make it difficult for nations to practically share devices across borders, because they might not be supported there. Consider what it might take to create an international standard, and what new regulation it would have, or what currently common regulations it might get rid of.

Questions to Consider:

1. What solutions used in previous world crises have been successful, and how do we replicate their success?
2. What methods can be employed to speed the development of vaccines for infectious diseases?
3. How will countries be encouraged to fund medical technology development when they have no immediate benefit?
4. Which emerging technologies have potential to address the spread and treatment of infectious diseases?
5. How will your solutions keep the country's religious and political views in mind as many of these viewpoints and lifestyles can be against the introduction of new technologies and/ or methods of medicine?
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 there to ensure that technologies are ready in case of another global pandemic for the future?

8. How will you ensure that technologies that are being created can be shared globally and that the methods and ways to use said technologies are taught to medical professionals in a short period of time?

Sources:

1. "1 June Is the Last Day to Apply for Consultative Status with ECOSOC." *Welcome to Csonet.org*, csonet.org/?menu=123.
2. "ABOUT UNCTAD." *UNCTAD*, unctad.org/en/Pages/aboutus.aspx.
3. Ministerie van Economische Zaken, Landbouw en Innovatie. "Encouraging Innovation." *Enterprise and Innovation | Government.nl*, Ministerie Van Algemene Zaken, 31 July 2020, www.government.nl/topics/enterprise-and-innovation/encouraging-innovation.
4. "SDG Impact Accelerator: Home Page." *SDGIA*, www.sdgia.org/#about.
5. Thimbleby, Harold. "Technology and the Future of Healthcare." *Journal of Public Health Research*, PAGEPress Publications, Pavia, Italy, 1 Dec. 2013, www.ncbi.nlm.nih.gov/pmc/articles/PMC4147743/.
6. "UN Agencies Launch Tech Access Partnership in Joint Effort to Scale up Local Production of Life-Saving Health Technologies for COVID-19 | Technology Bank for the Least Developed Countries." *United Nations*, United Nations, www.un.org/technologybank/content/launch_tech_access_partnership.
7. "UN to Explore Role of Science and Technology Policies in COVID-19 Recovery." *UNCTAD*, 9 June 2020, unctad.org/en/Pages/CSTD/CSTD-and-COVID-19.aspx.

TOPIC B: 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. Even though Article 12 of the Universal Declaration of Human Rights and Article 17 of the ICCPR, both create and ensure 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, including everything from what their dominant hand is to their political affiliations. 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. This scheme designed to improve the surveillance capability of the United States violated the right to privacy of its own citizens and citizens of other nations. Data Collection is dangerous, even when the data is not processed due to the ability for it to become leaked. Wiki Leaks demonstrated this danger by exposing the ways in which common devices would siphon data, how governments, specifically the U.S government, were able to use this data, and the extent of these data collection schemes. 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.

Yahoo, Facebook, Microsoft, Equifax, Tik Tok, and 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 in optical nodes and broadband gates, modified networking OS, and vulnerable OpenSSL versions. 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 walking gaits, voice, clothing, and even locational data. Your privacy of your 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.

Case Study: Clearview AI

Facial recognition is a computer program that has the ability to identify a face and correlate it to a database automatically. Facial recognition is one of many biometric methods that can identify an individual human from just being in front of a camera. This technology, once though to be extremely difficult to create and implement, now exists in the consumer space. In 2017, Samsung unveiled the Galaxy S8 with facial recognition technology, Apple followed suit with its Face ID. Along with common devices such as phones have the ability to process faces and identify humans, this territory is now being filled with numerous companies offering their service. Amazon has its Rekognition service, Microsoft has Face API, and Facebook has implemented it into pictures. Each year investment in this field grows, and each company strengthens its product. Many civil liberties groups argue that facial recognition has grown faster that legislation, and that existing laws cannot effectively regulate this technology. Certain cities, such as San Francisco agree, as they were the first major US city to restrict their police force from using facial recognition software. The danger lies in the ability for facial recognition to be used to track down individuals. The power that would lie in a hypothetical system could easily be abused by rogue officers to track down others. But each year, facial recognition gets closer to this hypothetical system. Leading the effort is Clearview AI, previously noted as having major data breaches. Clearview AI sells its facial recognition technology to law enforcement and private companies. All it takes is a single photo of a face. Clearview AI mines publicly available photos, including those from data breaches, for the person's appearance. Clearview AI will search everything, public traffic cameras, mugshots, the background of instagram photos, and even school photos. This service is sold to private companies such as the NBA, Best Buy, and Macy’s.Nations such as China don’t have a need for these systems, as they have developed their own surveillance systems, nearly nationwide. Additionally, they sell their systems, as they did in 2018 to the Nation of Zimbabwe. It is clear that these nations do not differentiate between authoritarian regimes and democracies, so it isn’t unbelievable to think that this technology could be used in the Hong Kong Demonstrations, or in the Belarusian Protests. Dubai for example uses facial recognition in their airports to track travellers who walk through a tunnel. By

automatically identifying the person, and being able to identify whether or not they are dangerous, Dubai has eliminated the possibility for human error. However, with these systems being inherently discriminatory to people of color, women, and minority groups due to their training data, mistakes can be extremely severe.

Bloc Positions

Western Bloc: 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 Bloc: 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 Bloc: 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 Bloc: 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. One specific focus of this bloc will be China's overreaching effect on the privacy of its neighboring countries from its

manufacturing of most electronic devices, growing influence in app creation and networking technology. Members from this bloc will be focusing on actions that can be taken to prevent this overreach, and might follow India's example of blocking specific apps and limiting Chinese networking infrastructure. 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/.