South Bay Model United Nations 2024

Commission for Science and Technology Development (CSTD)

cstd.sbmunviii@gmail.com

https://www.southbaymun.com/committees/cstd

Co-Chairs: Aarna Burji and Rohan Bodke

Table of Contents

Chair Bios

Co-Chair: Rohan Bodke

Hi delegates! I'm Rohan Bodke and am a junior at Homestead High School. I'm thrilled to be the co-chair for the CSTD committee of SBMUN VIII. This is my second year in Model UN and my first time chairing. Outside of Model UN, I do math olympiads, play the piano, and love to hike and play board games. I'm so excited to see all of you delegates working together to debate on pressing topics and solving the large issue of mass surveillance.

Co-Chair: Aarna Burji

Hi everyone! I'm Aarna Burji and I'm a junior at Monta Vista High School. I'm super excited to be a part of SBMUN's eighth annual conference as a co-chair of CSTD. I've been an avid member of Model UN since middle school and I'm eager to chair my first conference. Outside of Model UN, I dance, am an at home chef, and keep up with my interest in astrophysics. I'm most excited to chair a committee with a subject I personally have never participated in before. I look forward to meeting each delegation and hearing each country's unique stance!

Welcome Message

Delegates, welcome to SBMUN VIII! We're excited to be your chairs for the CSTD committee. We hope this background guide gives you a good starting point to conduct your research. While the guide contains plenty of information to begin, we expect the bulk of your research to be done on your own.

With this in mind, we wish for a wonderful committee, and we hope, with research, that you all can work together to find an effective solution to this serious problem.

Position Papers

You will not be eligible for any award if you do not submit a position statement.

In order to show your research into your topics, we request that each delegate submit a 2–5 page, typed, and double-spaced position paper, to be emailed as a PDF to cstd.sbmunviii@gmail.com by by **March 31 at 11:59** for research awards, or by **April 5 at 11:59** for any committee award.. In this research paper, we request that you write three sections: one on an overview of your topic, one on your country or individual's policies as extrapolated from the sources you evaluate, and one on the solution(s) you propose in your topic. We would also like for you to cite your sources in this paper to show that you have performed research.

The heading should look like this (please do not include your name OR your school name in the heading!):

Country Name
Committee Name
SBMUN VIII

If you have any specific questions about position papers, please feel free to email us!

Introduction to CSTD

CSTD is the United Nations Commission on Science and Technology for Development, and it is a part of the Economic and Social Council (ECOSOC). Created in 1992, the committee develops practices surrounding technology and ensures that no UN member is left behind. It is the main international platform for which all countries can work together to make the appropriate decisions relating to technological development.

In this quickly developing world, such a committee is of utmost importance so that modern technology is used positively and to benefit society. Now more than ever, with artificial intelligence and other technology on the horizon, CSTD is critical to ensure that all countries work together and take action.

Modern technology and recent developments have impacted the world greatly, both positively and negatively. With CSTD, these tools can be used to benefit both the environment and society.

Government Surveillance

In the rapidly evolving landscape of the digital age, the intersection of government and corporate surveillance through technology has become a focal point of concern and debate. As technological advancements continue to reshape the way individuals interact with the world, governments and corporations are leveraging sophisticated tools to monitor and collect vast amounts of data. This shift raises critical questions about the balance between security, privacy, and civil liberties. In this committee, we will examine the implications for individuals, society, and government, in a data-driven world.

Past International Action

The true size of the issue of digital mass surveillance has only been recently realized, and therefore not much action has been done to resolve it. In fact, most of the international action that has been done is malicious. For example, the Five Eyes (FVEY) intelligence alliance between Australia, Canada, New Zealand, the United Kingdom, and the United States, which was set up during World War II, has shifted to conducting global espionage through the internet. Similarly, Denmark, France, Germany, the Netherlands, and Sweden have formed their own Maximator alliance, which has stations in Curaçao that can pick up traffic from Cuba and Venezuela. It was also exposed that these alliances also conducted domestic surveillance on their own countries, sharing results with each other. The alliances are extremely secretive and almost certainly do not follow their own countries' laws, but such alliances greatly increase the power each country has, both on their own citizens and internationally. They may use the information they gain to direct their own agenda, such as fighting the War on Terror and China.

However, the United Nations has acted in protecting the privacy of people all around the world. For one, The United Nations Human Rights Council passed Resolution 28/16, declaring the "right to privacy in the digital age". The resolution has most recently been updated as Resolution 48/4. It calls upon all countries to protect the privacy of all their citizens, to end abuse of the right of privacy , to ensure that all means of counterterrorism comply with all domestic and international law, and to create an open and peaceful information and communications technology environment that the entire world can access. Furthermore, it encourages corporations that collect data to inform users about the data they are collecting and to ensure that data is collected lawfully and for a valid purpose.

Case Study: Bahrain

Bahrain is a country whose citizens struggle with government surveillance. A small country in the Middle East with a population of about a million, it is one of the most authoritarian countries in the world and ranks one of the highest when it comes to mass surveillance.

The internet has been accessible in Bahrain since 1995, which makes it one of the earliest Arab countries to do so. In 2015, it was estimated that 96.4% of the population is connected to the internet, and in 2020, there were 1.7 million mobile subscriptions, more than the number of Bahraini residents. So, the powerful government thought that surveillance through the internet could be effective in tracking the lives of the vast majority of citizens and ensuring that everything violating Bahrain's political beliefs is censored.

Since 2009, the Bahraini government has tracked phone calls, emails, and internet history of all people residing in the country, by requiring telecommunications companies to record calls and websites to register with the Information Affairs Authority. It has also blocked over a thousand websites, disallowing access from anyone in the country, and almost never unblocks one once it is blocked. In most cases, a website is blocked without a court order and cannot be appealed through a trial. For example, news outlet Awal was blocked in December 2018 because it criticized a government minister, and it has yet to be unblocked. However, the messaging service Telegram was banned in 2016 but has since become allowed for public use.

Content is also often removed from many websites, such as social media and video streaming services. In 2022, Bahrain threatened legal action if Netflix wouldn't remove content that it believed violated Islamic principles, such as films that depicted same-sex marriage. In another case, many people had sided against the assassination of Iranian military officer Qasem Soleimani, and posted their thoughts on Twitter. The Bahraini government responded by considering these acts cybercrime and questioned these people. In yet another extreme example of censorship, the government of Bahrain removed over 20 thousand pieces of Snapchat content in the first half of 2021 alone.

Bahrain is also known to use spyware technology to conduct mass surveillance upon the country. Between 2015 and 2017, the country has spent $500,000 on spyware from the United Kingdom, and has been found to use the Israeli spyware Pegasus which infiltrates mobile phones, in order to infringe on the privacy of many citizens. In October 2018, it was also revealed that Bahrain had bought espionage software from private companies, which had been used to target activists in several cases. By labeling acts against the government or its political views through the internet or social media as cybercrime, the Bahraini government has been successfully able to control almost anything any resident of the country can do online.

Because of the mass surveillance and censorship present in Bahrain, many people have resorted to self-censorship in fear of the consequences of speaking out. Since most virtual private networks (VPNs) are banned, using pseudonyms as usernames in social media platforms is futile, so most have given up trying to speak against the government and often stay quiet after controversial events. Ultimately, government surveillance in Bahrain has greatly affected the human rights and freedom of speech of all citizens in the country.

Key Issues

Each delegation should perform research to center their committee stance around their country's relevant interests. To help kickstart research, here are some nuanced key issues we would like to see brought up during the conference. (Also refer to questions to consider in tandem with the following topics):

1. Legal and ethical frameworks to protect human rights.
2. Civil Liberties and Privacy vs National Security.
3. Domestic vs International definitions of "the right to privacy".
4. Data Collection and Restriction Practices and Policies

   Define the boundaries of personal data collection and storage by both government and corporate entities.
5. Technology's rapid advancement/Role in Government Surveillance.
6. Cybersecurity and foreign surveillance.
7. Transparency and Accountability.

Possible Solutions

One possible solution to the abuse of human rights in this issue is to establish clear legal frameworks that regulate surveillance practices to prevent abuse and protect citizens' rights.

Developing and implementing comprehensive legal guidelines that govern the use of surveillance technologies by governments and corporations on an international scale is a vital step in addressing government surveillance and ensuring the protection of citizens' rights. How to do this while keeping national security as a priority in terms of government surveillance is another crucial aspect that requires careful consideration up to each delegation's country stance.

Questions to Consider

1. How do differing cultural and societal norms across countries influence the interpretation and application of the right to privacy on an international scale, and what international framework can be established to effectively regard government surveillance in the long term?
2. How can policies be designed to balance the need for data collection with the imperative to restrict access, ensuring that collected data is used only for its intended purpose?
3. In the case of expanding surveillance capabilities, how do countries safeguard fundamental human rights and civil liberties while doing so?
4. To what extent can we define the right to privacy as a human right, or a civil liberty, and what does an "international right to privacy" look like?
5. How do we balance individual privacy rights with the need for surveillance in the interest of national security or corporate interests?
6. In the age of cyber threats, how can governments balance the need for robust cybersecurity measures with the protection of individual privacy, especially when conducting surveillance on foreign entities?
7. What are the potential long-term societal implications of pervasive government surveillance, and how might it impact trust between citizens and the government over time?

Selected Sources

In order to help delegates begin their research, we have included a few resources that we believe could be helpful.

1. *Freedom House* Internet Freedom Status Map, https://freedomhouse.org/explore-the-map. Contains information about surveillance and internet freedom in many countries around the world.
2. The Office of the High Commissioner Special Rapporteur on the right to privacy, https://www.ohchr.org/en/special-procedures/sr-privacy. The primary resource for UN-based action on digital privacy issues.
3. The Office of the High Commissioner Special Rapporteur on spyware and surveillance, https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report. Provides background on the UN concerns of government and foreign surveillance.

Works Cited

"Bahrain: Freedom on the Net 2023 Country Report." *Freedom House*, 2023, freedomhouse.org/country/bahrain/freedom-net/2023.

"Commission on Science and Technology for Development | UNCTAD." *Unctad.org*, unctad.org/topic/commission-on-science-and-technology-for-development.

Deeks, Ashley. "Jessup 2024." International Law Students Association, 21 Dec. 2023, www.ilsa.org/jessup-2024/.

Haan, Katherine. "What Is the Five Eyes Alliance?" *Www.forbes.com*, 5 Oct. 2023, www.forbes.com/advisor/business/what-is-five-eyes/.

Jacobs, Bart. "Maximator: European Signals Intelligence Cooperation, from a Dutch Perspective." *Intelligence and National Security*, vol. 35, no. 5, 7 Apr. 2020, pp. 1–10, https://doi.org/10.1080/02684527.2020.1743538.

Schrepferman, Will. "Supervising Surveillance: International Law and the Surveillance State." Harvard International Review, Harvard International Review, 11 Nov. 2020, hir.harvard.edu/global-surveillance-state/.

Söderqvist, Emma. "Is Bahrain a Cyberauthoritarian State? Human Rights and the Digital Sphere." *Middle East Centre*, 18 May 2021, blogs.lse.ac.uk/mec/2021/05/18/is-bahrain-a-cyberauthoritarian-state-human-rights-and-the-digital-sphere/.

United Nations. "Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns." *OHCHR*, 16 Sept. 2022, www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.