BOARD OF FACEBOOK

Topic A: Data Privacy

In modern times, an incredible amount of our lives is conducted, managed, and documented on the internet. Twitter knows what we think, Spotify knows what we listen to, and Google Maps knows our exact location. As consumers of technology, we hand enormous amounts of sensitive data to private companies, often with little legal regulation surrounding the use and protection of that data. Privacy scandals like the ones surrounding Cambridge Analytica, Equifax, and Yahoo have drawn the public's attention to issues surrounding privacy, and as governments around the world bear down on technology giants, they must adapt in order to survive.

Few companies have as large of a pool of user data as Facebook, one of the most popular social media networks in the world. Between Marketplace, Messenger, Instagram, Whatsapp, and a distributed network of tracking widgets on hundreds of websites, this company knows everything there is to know about its users' digital identities. While this trove of data is Facebook's secret weapon in designing personalized products, it is also its Achilles heel - over the past 15 years, Facebook has been plagued by data privacy scandals which have endangered its users and eroded the public's trust in the platform.

In this committee, delegates will represent the board and senior executive team of Facebook. Collectively, they will face crises regarding data privacy and attempt to keep Facebook secure, profitable, and widely used. Although Facebook is a technology company, this committee does not expect any level of technical expertise - instead, delegates will be expected to use their business savvy, creative problem solving, and understanding of digital privacy in order to dissect, dismantle, and defend against an onslaught of crises. Our learning goals for those in this committee are to gain deeper insight into the painstaking design behind consumer-facing technology products, understand Silicon Valley's corporate culture, and get a sense of what it would be like to be at the helm of a company at the center of the media's attention.

I chose this topic because of its relevance to everyday life. Many of this committee's delegates will have used Facebook's products, but few will have considered the consequences of giving the company so much data. This topic is also very current, and I feel that this topic will continue to be heavily covered by the media over the next

few years. I chose this company because Facebook is at a turning point, shifting its organizational focus from user growth to privacy—as it does so, it is particularly relevant to have a committee exploring how the company could face large privacy-related issues.

If you are in this committee, I am so very excited to read your position papers and to hear what you have to say! Please email me at npimpalkhare@bmun.org if you have any questions or comments about this committee, the topics, or research in general.

Topic B: Open Source Investigations

Open source investigations involve the collection, verification, exploration, and analysis of open source intelligence. Open source intelligence (OSINT) is any information that is stored in a public, persistent manner on the internet. Examples include public government records, news articles, data leaks, and even Facebook posts. Open source investigation is incredibly valuable because it enables governments and common people alike to use the power of the internet to bring criminals and human rights offenders to justice. In 2018, citizens around the world used OSINT to investigate the killing of Oscar Perez in Venezuela, revealing significant evidence that he had not merely died in a shootout with the police, but instead was captured and executed.

Social media sites must moderate their content in some way - the circulation of fake news, hate speech, and graphic images can propagate persecution and advocate violence. However, when companies like Facebook take down violent videos or images, they prevent such material from being used for open source investigations. Algorithms designed to scrub bloody videos from the platform could end up deleting evidence that could be used in a legal trial or could make it harder for law enforcement to locate an ongoing crime. How can Facebook and other social media platforms simultaneously enforce their existing content policies and enable conductors of open source investigation?

The reason I chose this topic is that preventing human rights violations is possibly the most optimistic use case of Facebook's platform. When implemented correctly, open source investigation has incredible benefits without any real downside. However, this topic will highlight how even when a particular result is desirable, defining a path to accomplish that result is hard. During committee, delegates will grapple with defining how to enable open source investigations, working with third party organizations, and questioning the obligation of social media platforms to enable such investigations in the first place. This topic should expand delegates' perspectives on what social media can do, and should provide for a fascinating and complex debate.

One final thing I would like to point out is that while these topics are certainly distinct, they are not necessarily exclusive. Over conference weekend, crises will not be specifically marked as "topic A" or "topic B." Instead, I aim to involve elements of both in each crisis, allowing delegates to be challenged by both topics at the same time. Again, feel free to email me about anything regarding this topic or research in general. Have fun exploring these issues! I know I did.