SILICON VALLEY SUMMIT

TOPIC BULLETIN

JESYLN ZHNAG
SASKIA TROMMELEN
CHAIRS

Contents:

Academy Model United Nations

- THE TWENTY-SECOND ANNUAL CONFERENCE -

SECRETARIAT

AARON THAMMAVONGXAY
SECRETARY GENERAL

KAYLYN LU
CHARGÉE D' AFFAIRS

EMILY HASHEM
ALISHA MERCHANT
DIRECTORS OF EXTERNAL AFFAIRS

CATHERINE PARK
JIWON SON
DIRECTORS OF INTERNAL AFFAIRS

ESTEBAN MEDINA
VIDIT SHAH
DIRECTORS OF OPERATIONS

LAETITIA PARK
DIRECTOR OF BUSINESS

MICHAEL PAPADOPOULOS
DIRECTOR OF TECHNOLOGY

ELLIOT LEE
DIRECTOR OF COMMITTEES

ETHAN DONOVAN
CHIEF OF STAFF

ANDREA BUCCINO
FACULTY ADVISOR

MARK KRAMER
FACULTY ADVISOR

Dear Honorable Delegates,

It is my pleasure to invite you all to participate in AMUN XXII! My name is Jeslyn Zhang, and I will be serving as your Co-Chair of the Silicon Valley Summit. I am currently a junior in the Academy for the Advancement of Science and Technology, and have been an avid participant in Model UN since my freshman year here at BCA. In this committee, you will fill the shoes of various heads of major corporations to resolve pressing issues in today's world of technology. Use this background guide as a starting point for your research into tackling these problems and formulating ideas.

I hope that each and every one of you will be able to take away something valuable from this experience, whether it be your first Model UN conference or your tenth. Regardless of the outcome, AMUN never fails to be a great place to expand your public speaking skills and practice cooperation, communication, and leadership. I wish you all the best in your preparations and look forward to seeing you in committee!

Best of luck,
Jeslyn Zhang, Co-Chair, Silicon Valley Summit
jeszha22@bergen.org

Dear Honorable Delegates,

Welcome! Jeslyn and I are so excited about your participation in AMUN XXII! I am Saskia Trommelen, your Co-Chair for the Silicon Valley Summit committee, and I am a junior in the Academy of Science and Technology at BCA. I have been a part of Model UN since the later portion of my Freshman year, and am honored to chair at AMUN. I am also a part of my hometown's marching band and some of the arts programs at BCA as well as Spring Track. That being said, the Model UN program at BCA has been incredibly rewarding and I can not wait to share some of that experience with you.

This Topic Guide will give you some of the background information you need to get started with your personal research, and gives somewhat of a starting point. No matter how experienced you are in Model UN, each conference builds up the skills needed to succeed in the future. Hopefully, you will see your own skills improve over the course of this conference and we all benefit from the experience of AMUN. If you have any questions or concerns do not hesitate to reach out to Jeslyn or me so we can clear up any information. Thank you for signing up for Silicon Valley Summit and good luck in committee!

Take care,
Saskia Trommelen, Co-Chair, Silicon Valley Summit
sastro22@bergen.org

Silicon Valley Summit

Overview:

The Silicon Valley Summit is set in modern day Silicon Valley, the global center for high-technology, innovation, and social media. Currently, numerous global issues are plaguing the world of technology, from data privacy and security to internet content policing. As the heads of various multinational technology and electronics companies, it is your job to find resolutions to these problems while still upholding your company's own interests and adhering to your character portfolios. Additionally while discussing such topics, do not lose sight of your company's country of origin and its individual policies on the relevant issues, such as freedom of speech.

The structure of this committee is similar to that of a General Assembly, as delegates will be expected to follow the same parliamentary procedures. However, rather than passing working papers, you will be passing bills, which will be your solutions to the issues discussed. While there is

no limit to how many you can pass, we would like to see around 5-10 in total.

Parliamentary Procedure:

This committee will follow the standard parliamentary procedure. A majority of the time spent in committee will be in moderated caucuses, but there will also be unmoderated caucuses as the committee sees necessary, motioned by delegates. The chair reserves the discretion to make final calls before voting on motions. Resolutions will be passed in the form of "bills," which are essentially shorter draft resolutions that cover a specific topic more in-depth. There is no limit to the number of bills the committee may pass.

Topic History:

As the world continues to advance in technological developments, the demand for and profit of the tech market has only skyrocketed. At the end of fiscal year 2019, the multinational technology company Apple Inc. reaped over $265 billion in revenue — a staggering increase from its mere $8 billion revenue just twenty years ago. However, with this rise in popularity came a multitude of concerns and issues from consumers and regulators alike surrounding privacy, disinformation, and even human rights. The discourse between whether to prioritize profitability or ethicality is one that can not go unaddressed by the technology community, especially after a long, laborious history of controversy and conflict..

Consumer Data Privacy:

In recent years, the issue of consumer data privacy has become an increasingly growing topic of concern. Many view the digital collection of user data by private corporations as unethical and immoral, and have voiced their concerns over this practice. In fact,

in early 2018, a scandal erupted between the social media company Facebook and the British political consulting firm Cambridge Analytica over an alleged data breach, in which the data of over 50 million Facebook users were collected without their knowledge for political advertising. Cambridge Analytica then sought to sell these analytics to political campaigns, directly assisting in the campaigns of Ted Cruz and Donald Trump. The spread of this news led to major backlash from users, resulting in the testitification of CEO Mark Zuckerberg in front of Congress. This data breach has since been deemed the largest known leak in Facebook history.

The Facebook and Cambridge Analytica data scandal exemplifies a larger issue on the topic of consumer data privacy: to what extent does the legal collection of user data start infringing upon consumers' personal information? While millions were outraged over this breach of privacy, Facebook denied the accusation, arguing that researchers were allowed access to user data for academic purposes and that users had consented to this by signing Facebook's user agreement. However, the selling of this data was widely prohibited by Facebook, meaning Cambridge Analytica had in fact violated their regulations. Regardless, whether the fault lies on the corporation itself, loose and unenforced regulations, or unclear Terms and Agreements, it is up to these companies to ensure the privacy and security of their consumers.

After a series of congressional hearings and data breaches, the past several years have seen some of the most wide-ranging privacy legislation to date. On May 25, 2018, the General Data Protection Regulation (GDPR) was approved and enforced by the European Union, replacing the former Data Protection Act of 1998. The regulation outlines seven principles for the lawful processing of personal data, including subjects of transparency, purpose limitation, accuracy, and accountability. The same year, the California Consumer Privacy Act (CCPA) was signed into law, giving California residents a myriad of new rights, including the right to be informed of what personal data is collected and why.

Similarly, regulators worldwide have since tightened their statutes on data protection, while continuing to increase the stakes for data privacy enforcement. In fact, on January 21, 2019, the French National Data Protection Commission (CNIL), in one of the largest global privacy fines to date, imposed a €50 million ($56.2 million) penalty against the tech giant Google LLC for multiple violations of the GDPR. The recent widespread push for accountability by the government and by legislators may change the world of technology indefinitely.

This spike of interest in consumer data privacy extends beyond the legislative world and into the daily lives of regular citizens and users. As a result of the publicization of data protection, there has been a recent explosion in consumer privacy tools, including, but not limited to, secure emails systems, secure browsers, and virtual private networks (VPNs). The popularization of alternative options for users, such as DuckDuckGo in place of Google, may affect the strategies and interests of major technology corporations.

Internet Content Policing:

Internet content policing has been a topic of discourse and debate since the popularization of the internet itself. Today, this issue remains controversial at best, with one major question at the forefront of every discussion: do private companies have the right to control and police the internet content of individual users? Although the instinctive response may be simple and self-explanatory, several issues have complicated the answer.

The year of 2019 has seen a rise in the publicization of disinformation, more commonly referred to as “fake news”. While the amount of unreliable and untrustworthy online sources is rampant, greater concerns have been raised over attempts of election interference by external forces. The infamous 2018 Mueller Report, published after a two-year-long investigation by special counsel Robert Mueller, accused Russia of interfering in the 2016 United States presidential

elections in a “sweeping and systematic fashion”. In July 2019, Mueller stated that Russia, among other countries, has continued to interfere with US elections by developing disinformation campaigns. In fact, between January and July of 2017, social network company Twitter identified and shut down over 7,000 fraudulent accounts by Iranian influence operations. The awareness of this disinformation has prompted several other social media companies to quickly take action in preventing such interference. By August of 2019, Facebook, Twitter, and Microsoft alike had both banned advertisements featuring misinformation and reinforced security updates for users. Despite these actions, tech companies continue to face scrutiny over their handling of this disinformation, with many criticizing their role in helping to spread fake news.

In a similar vein to the control of disinformation, online harassment and cyber abuse has become another topic of focus in recent years. With the development of modern technology, physical harassment and threats of violence have largely moved online, manifesting in a multitude of different forms of online harassment with varying degrees of severity, including doxing, cyberstalking, and hate speech. As found by the U.S. State Department of Justice, approximately 850,000 American adults are targets of cyberstalking per year, and 40 percent of women have experienced online dating violence. Despite the widespread prevalence of these criminal offenses, there remains little to no accountability for the offenders, with poor enforcement of the already vague legislation. In fact, cases of online harassment and cyber stalking are often dismissed by police due to improper education on whether it constitutes a civil or criminal matter.

The minimal legal protection of victims, in combination with the rampant spread of disinformation, leaves a bulk of the responsibility to the tech companies themselves. The vast majority of technology and social media companies have already implemented regulations in order to limit inappropriate online content. Large companies, such as Facebook and Google, use tens of thousands of content moderators, as well as artificial intelligence and

machine learning technology, to filter out hate speech and false information on their sites. In addition, users are given the option to report any content that may violate their terms of service, aiding in the filtration of internet content.

However, once the severity of these cases begins to decrease, the line between policing online content and outright censorship becomes more and more difficult to distinguish. While hate speech is generally defined as "public speech that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation", there currently exists no legal definition of the term, making the phrase dangerously open to interpretation. Concerns over censorship become especially prominent with the social networking platform TikTok, owned by the Chinese parent company ByteDance. Since its popularization, the app has been consistently criticized for its unnecessary censorship of content, especially concerning social and political discussions. While the global platform does not directly censor political content or take instructions from ByteDance, the regulation of content on TikTok ultimately falls under the jurisdiction of its Beijing-based moderators, and must comply with Chinese censorship restrictions. As a result, many have voiced their concerns over the restriction of their free speech and political expression, leading the US Department of the Treasury's inter-agency committee, Committee on Foreign Investment in the United states, to investigate the deal that brought TikTok under ByteDance's control.

Despite being a more extreme case of censorship, this issue is not exclusive to the one singular company. As numerous multinational technology companies push to the forefront of the international community, it is imperative that they reach a consensus over the handling of both internet content policing and consumer data privacy.

Character Profiles:

Due to the nature of the Silicon Valley Summit, instead of representing countries, CEOs will be represented looking out for the interests of their respective

companies. There are a wide range of companies represented, so it is important to figure out which companies share common interests and which you may be interested in working with on bills. Below are more detailed descriptions of each CEO featured in committee, which may serve as a starting point for individual research.

Tim Cook:
Tim Cook is the chief executive officer of Apple Inc. and previously served as the chief operating officer under the company's co-founder Steve Jobs up until August 24, 2011. Throughout his duration as CEO, Tim Cook has advocated for the reform of systems regarding international and domestic surveillance and cybersecurity. However, Apple does collect consumer data to target advertisements towards users based on their past device news and app-store history. Apple Inc. is based in California, meaning that it is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Jeff Bezos:
Jeff Bezos is the founder, chief executive officer, and president of the multinational technology company Amazon. Besides being an e-commerce and online retail titan, Amazon also owns over 40 subsidiaries such as Whole Foods, Audible, and IMDb. Due to the number of services provided by the companies in Jeff Bezos' control, he has access to a large amount of consumer data, used to fuel item recommendations. There are also concerns over home devices that are run by Amazon, such as Alexa, which may serve to collect information or data through conversations. Amazon is based in Seattle, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Mark Zuckerberg:
Mark Zuckerberg is the co-founder, chairman, and chief executive officer of Facebook Inc. Facebook is a social media platform in which individual users can create content and post pictures to connect with other people that they may know. With more than 2.3 billion users, Facebook has access to an immense

amount of user data. Zuckerberg has admitted to using this personal information and charging advertisers for details on advertisement interactions, as well as trading information with Amazon, Yahoo, and Huawei in order to obtain contact lists. The social media company must also deal with censoring and online policing regarding the content allowed on the platform. Facebook is based in Menlo Park, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Kim Hyun Suk/Koh Dong-Jin/Kim Ki Nam:
From March of 2018, the chief executive officers of the South Korean multinational electronics company Samsung Electronics have been Kim Hyun Suk, Koh Dong-Jin, and Kim Ki Nam. The company is well known for its sale in hardware and software devices such as cell phones, watches, appliances, and other devices. Samsung is also known as a leader in the development of artificial intelligence in software. For Samsung cellphone users, user data is sold to third parties and may be used for future product designs or development. Although Samsung does allow users to opt out of having their data sold, the company has also revealed that user data may have already been sold. Samsung is based in Seoul, meaning that the company is under the jurisdiction of South Korea and has to operate under restrictions imposed by the South Korean government.

Jack Dorsey:
Jack Dorsey is the co-founder and chief executive officer of Twitter as well as the founder and chief executive officer of Square, a mobile payments company. Twitter is a social media platform launched in 2006 in which individual users and creators can develop short passages called "Tweets." Jack Dorsey has condemned other social media platforms for selling user data, however, in a similar fashion as Facebook, Twitter also collects user information and sells it in a series of commercial data feeds, also known as social media data mining. Twitter as a platform must also address what content should be prohibited from the platform and censored. Twitter is based in

San Francisco, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Zhang Yiming:
Since 2012, Zhang Yiming has been the founder and chief executive officer of ByteDance, which is the parent company of the popular social media platform TikTok. ByteDance is also the owner of other companies such as Douyin, BaBe, Vigo Video, Helo, and Huoshan. TikTok has grown to be incredibly popular over the past couple of years, raising suspicion among many regarding data collection and management. Recently, the country of India has banned TikTok as a platform from use by its citizens, raising censorship arguments as well as data collection arguments. Additionally, censorship and policing must be dealt with by the company as multiple creators have come forward regarding "shadowbanning." Although TikTok headquarters are located in Los Angeles and are under management of a different CEO, the CEO of TikTok answers directly to Zhang Yiming, CEO of ByteDance. ByteDance's headquarters are located in Beijing, meaning that the company is under the jurisdiction of China and has to operate under restrictions imposed by the Chinese government.

Evan Spiegel:
Evan Spiegel is the co-founder and chief executive officer of Snap Inc. and its development Snapchat. Snapchat is a popular social media platform that allows users to interact with others through pictures and snapshots that disappear after a certain period of time. The appeal of the platform is the impermanence of the photos and chats, which raises concerns about the company supposedly retaining these images for use even after they disappear for the users. Not only may the platform use data to personalize what gets recommended and advertised, it was also accused of selling the data to other third parties. That being said, Snapchat is notorious for not policing content and generally has very relaxed censorship. Snachat's headquarters are located in Santa Monica, meaning that the company is under the jurisdiction of the United States and has to operate

under restrictions imposed by the United States' government.

Hans Vestberg:
From August 2018 onward, Hans Vestberg has been the chief executive officer of Verizon. Verizon is primarily an internet service provider, but it offers a multitude of services beyond just that including communication and various entertainment. Verizon has also acquired other companies as subsidiaries, including Yahoo in 2017. Due to this, Verizon has a lot of user information, including the location of many people, making security and privacy concerns prominent for the company. Additionally, Verizon has come under fire for slowing Internet speeds, which has become even more prominent after net neutrality was repealed. This may come into play when talking about policing or regulation of the Internet, especially since Verizon now owns Yahoo. Verizon's headquarters are in New York, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Sundar Pichai:
From December 3rd, 2019, Sundar Pichai has been the chief executive officer of Alphabet Inc. and its subsidiary Google LLC. Sundar Pichai himself has made claims that privacy should never be a luxury good and that Google as a company would never sell user data, however; Google has a bidding system that allows the company to still make money off of user data and use that data to personalize advertisements. Although Sundar Pichai has rarely talked about Internet policing, he does prioritize Youtube (a subsidiary of Google), and recognizes that Youtube needs better policing. Google is based in California, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Satya Nadella:
Since February 4, 2014, Satya Nadella has been the chief executive officer of the technology company, Microsoft. Currently, Satya Nadella views data privacy as a "human right" which he has said in interviews. He has also praised the GDPR for their work in establishing privacy regulations

overseas in Europe. However, the Microsoft company does collect user data and uses it to sell targeted advertisements. Satya Nadella is also in favor of regulation of the Internet and AI technology. In addition to this, Microsoft also owns Xbox as a subsidiary, making the policing of certain online interactions an issue of theirs. Microsoft is based in Washington, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Ren Zhengfei:
Ren Zhengfei is the founder and chief executive officer of the Chinese multinational telecommunications equipment company Huawei. Huawei is also the leading cell phone maker in China, owning 27 percent of the market share and having growing bases in Asia and Europe. Ren Zhengfei has made it clear through interviews that he would refuse to sell data and is committed to customer privacy. That being said, in the US, some government officials have raised concerns over Zhengfei's affiliation with China's government fearing that he would sell user information to government officials. He has not currently spoken on internet policing or censorship. Huawei is based in Shenzhen, meaning that the company is under the jurisdiction of China and has to operate under restrictions imposed by the Chinese government.

Michael S. Dell:
Michael S. Dell is the founder, chairman, and chief executive officer of the American multinational computer software company Dell Technologies, a company well known for its computer and monitor sales and development. Dell has been incredibly successful in the United States so far, owning 16.8 percent of the market share. Dell Technologies is based in Texas, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Arvind Krishna:
Since April 6, 2020, Arvind Krishna has been the chief executive officer of International Business Machines Corporation, or IBM. IBM is an information technology company

and it is known for its sale in computer hardware and software. It also is a large research organization and is expanding its operations in other areas regarding technology. IBM deals highly in artificial intelligence, making privacy a large concern. As of 2020, IBM has announced that it will no longer offer or develop facial recognition software out of concern of privacy. IBM is based in New York, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' Government.

Kenichiro Yoshida:
From April 1, 2018, Kenichiro Yoshida has been the chief executive officer of the Japanese multinational conglomerate company Sony Corporation. Sony is a consumer electronics company, and also produces online content such as media and music. As Kenichiro Yoshida took over as Sony's CEO, he looked to expand the content side of the company while maintaining production of electronics. In Sony Corporation's privacy policy regarding California law, the company outlined that data may be collected and sold using some of their devices to third parties. However, the consumer is allowed to request that the company does not sell their data. In the past, Sony has also given Playstation data to the FBI, making headlines in some cases to help make arrests. Sony Corporation is based in Tokyo, meaning that the company is under the jurisdiction of Japan and has to operate under restrictions imposed by the Japanese government.

Daniel Ek:
From 2006, Daniel Ek has been the chief executive officer of Spotify, a Swedish recognized online music provider. Spotify currently has around 286 million active listeners, giving the company a plethora of user information due to the popularity of the platform. The company does provide this information to third parties for advertisement specialization and personalization, but claimed it was unaware of the spread of user data. Additionally, with songs of all kinds on the platform, Spotify also must deal with Internet policing and regulation. Spotify's headquarters are based in Stockholm, meaning that the company is under the jurisdiction of Sweden and has to

operate under restrictions imposed by the Swedish government.

Randall Stephenson:
Randall Stephenson is the chief executive officer of the multinational conglomerate AT&T. AT&T, like Verizon, is viewed primarily as an internet service provider due to its subsidiary AT&T Communications. However, the company has largely expanded and bought extensions of the company such as Crunchyroll, DIRECTV, and all companies owned by Time Warner after a merger. AT&T does collect user data, but they do allow the user to opt out of this process and request that their data is not sold. Additionally, since AT&T has come to own so many companies, censorship and Internet policing is an active problem that the company must face. AT&T's headquarters are based in Dallas, meaning that the company is under the jurisdiction of the United States and has to operate under restrictions imposed by the United States' government.

Ma Huateng:
Ma Huateng is the founder and the chief executive officer of the multinational conglomerate Tencent. The subsidiaries that Tencent holds include entertainment, technology, artificial
intelligence, and many Internet-related services. One of the most famous of which is its gaming subsidiaries as it owns Riot Games (League of Legends) and has stakes in Epic Games, Ubisoft, and Activision Blizzard. Tencent also provides Internet, online advertising, and e-commerce transactions. Although they operate worldwide, they have a massive market share in Asia and specifically China. Currently they expected to expand more heavily into the United States. Tencent has headquarters in Shenzhen, meaning that the company is under the jurisdiction of China and has to operate under restrictions imposed by the Chinese government.

Questions to Consider:

How will data privacy restrictions and changes in internet policing affect your company?

Has your company sold user data or made attempts to more heavily

police the internet in the past? How will your companies' past actions affect what bills you are in support of?

How does the country that your company operates in affect what privacy regulations and policing you have to abide by?

How will you ensure accountability from advertisers and users that violate your terms of service?

What bills would your company have an interest in passing and what effects may those bills have on the future of Internet freedom? How much power does your company have based on its past interests and actions?

Based on how your role acts normally, would you be in favor of Internet policing? If so, to what extent is the policing of Internet content okay until it is considered censoring?

References:

1. https://svisummit.com/
2. https://onlinecensorship.org/
3. https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-ho
4. w-company-shares-monetizes-and
5. https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/
6. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
7. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
8. https://www.uhi.ac.uk/en/about-uhi/governance/policies-and-regulations/data-protection/
9. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
10. https://www.dataprotectionreport.com/2019/02/gdpr-ccpa-and-beyond-changes-in-data-privacy-laws-and-enforcement-risks-to-monitor-in-2019/
11. https://www.bloomberg.com/news/articles/2019-06-24/u-s-sees-russia-china-iran-trying-to-influence-2020-elections

12. https://en.wikipedia.org/wiki/Russian_interference_in_the_2020_United_States_elections#cite_note-3
13. https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cantdo-about-online-harassment/382638/
14. https://www.nytimes.com/2019/04/21/technology/facebook-zuckerberg-harmful-speech.html
15. https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clashwhere-us-views-about-censorship-often-were-overridden-by-chinese-bosses/