Political Committee: The Right to Privacy in the Digital Age

Members of the Dais: Verónica Alonso and Conrad Hamilton

CPNMUN 2019: September 20th and 21st, 2019

---

1. Historical Context

Since the 1960's the world has been seeing the advances of the internet and its adjacents, from computers, to smartphones to talking sound systems; the world has evolved into a new technological era. This new era comes with many uncertainties that the whole world faces. One of these major uncertainties is the security of the information these companies hold and who has access to it. Some countries around the world have begun using the information found on the internet, to control, manipulate and surveillance their population. This chaos has caused constant turmoil in the world-wide population. People feel the world is unsafe because confidential data is exposed to companies and for others to see. A worldwide demand for more security in the technological field has been imposed. The current 40% of the world population feel they lack control over their personal data, according to a survey by McAfee, and one-third of parents don't know how to explain online security risks to their children. Last year, major corporations such as Facebook, Panera Bread, and the Sacramento Bee experienced data breaches that put tens of millions of personal records into the hands of criminals. These information breaches caused awareness to form in the midst of the public; who now demand accessible security measures. It could be said that these breaches are the "tip of the iceberg" when it comes to hacked accounts and stolen data. Consumers are beginning to take notice. Terms such as crypto-ransomware, crypto-mining, and banking Trojans make their way into the mainstream vocabulary. Data privacy concerns among people in the U.S are hitting an all-time high. This has caused conflicts in the government on how it should protect its information and what is considered public and

private information. Now more than ever there is a need for online security and there been more awareness on the topic.

2. Recent Issues

Equifax Data Breach Settlement

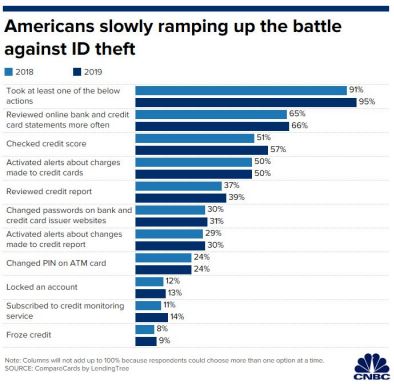
In September of 2017 Equifax, a credit reporting agency that maintains information on over 800 million consumers and more than 88 million businesses worldwide, was breached by hackers. Over 147 million people had there credit card, social security numbers, addresses and credit scores exposed to online hackers. The effects of this massive breach are still seen today because millions of users are still exposed to credit card and identity fraud. Equifax is one of the three main credit scoring companies; this is why it affected so many people. The Federal Trade Commission ruled that Equifax will have to pay up to $700 million in individual compensation and civil penalties because of the hack. People are still falling short in their efforts to make sure they aren't the victims of fraud, according to a new survey by CompareCards.com. This comes despite thousands of other breaches since then, including more than 1,200 in 2018 alone, according to data from Statista.com. "I think consumers are just desensitized to it because they live in a world where breaches are a reality," said credit expert John Ulzheimer, president of The Ulzheimer Group in Atlanta. This massive breach shed light on the lack of security that companies have on consumers information. This caused massive concern and uproar by the population whose information got leaked. Equifax has taken steps to correct the massive undoyings this breach caused but many are still affected.

Capital One Breach

For the past couple of years, the private sector has gone against regulation on cybersecurity, saying that the market will do a better job of making companies change and invest in cyber defense. Their logic goes as this customers will flee companies that do not protect their data and investors will rebel and hold companies accountable for the damage to their brand.

Nonetheless, the steady stream of major breaches in the last few years have exposed

Data breaches have little to no long-term impact on companies' business



This is exactly what happened to Capital One, on July 19, 2019. Capital One, is a forty five billion dollar bank who is the tenth largest banks in the United States. This breach affected one of three people in the United States. The hack originated when a Paige Thompson obtained access to the cloud. This caused credit card numbers, social security customers and individuals who had applied for credit card products to have their information exposed. Capital One immediately apologized but didn't really take massive action to fix this problem for the future. They gave empty promises saying they'll work with federal law enforcement but this does not mean reinforcing their security systems and anti-hack defense. This massive breach in security was a wake up call for millions of Americans. People realised they couldn't trust the big corporations with their information.

These massive breaches have caused awareness in the worldwide community since they show a lack of security for the information we store in these companies. The world has shown massive steps into wanting to improve these security measures. It is essential to come up with viable solutions for the lack of privacy consumers have over there information.

3. Guide questions

a. What is your delegations position on cybersecurity and what is it actively doing to enforce it?

b. Has your delegation done anything in order to evoke or help cybersecurity?

c. Has the breaches mentioned previously or other security breaches affected your delegation? If so how?

d. How can your delegation help improve cybersecurity and privacy laws worldwide?

e. What is your delegation actively doing to improve privacy in the digital era; what are its future plans?

4. **Message of the dias**

Delegates, The Right to Privacy in the Digital Age is one of the most broad, current and complex problems in the world. Therefore, we urge you all to look further into all the topics discussed in this document, and to develop creative solutions to the matter at hand. It is of utmost importance to provide plans that are not only effective, but plausible. Having said this, we urge delegates to not only look into the issues our world faces regarding cybersecurity, but also to evaluate how their respective delegations have been affected by it. We are very excited to see the plans you create and how to make our technological world into a safer and better place.

Position papers are due on wednesday, September 18 by 11:59 PM. These should be written in **Times New Roman font, size 12, double spaced.** The document must be at **least 2 pages** long but **no longer than 3 pages**. We would prefer the format of the documents to be **PDF**, but we will also accept **Microsoft Word files** and **Google Docs**. If this is your first time ever in a Model UN competition you must state in your position paper (in the heading) that you are a **Novice** but if you have been in a competition or are working with someone who has been in a competition before then you must state that you are a **Veteran** next to your delegation on your position paper. Please be punctual because we need time to correct your papers and look into the plausibility of your solutions. If these requirements are not followed points will be deducted off the position paper rubric. It is also worth highlighting that the committee will be set in **present day**.

We are very excited to see what you guys bring to committee! Please email your position papers to both of us as soon as they are ready! Feel free to reach out to any of us if you have any questions or concerns about the committee and we are very excited to start the year with you guys.

Thank You

Conrad Hamilton
conradgreat@gmail.com

Vero Alonso
verodelc21@gmail.com

Works Cited

David Gorodyansky, AnchorFree. “Privacy and Security in the Internet Age.” *W* Conde Nast, 7 Aug. 2015, https://www.wired.com/insights/2015/01/privacy-and-security-in-the-internet-age/.

“David Oragui.” *The Manifest - Small Business News, Data, and How-To Guides*, https://themanifest.com/app-development/4-reasons-your-app-needs-privacy-policy.

“Equifax Data Breach Settlement.” *Federal Trade Commission*, 1 Aug. 2019, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

“How to Check If You're Affected by the Equifax Data Breach.” *LifeLock Official Site*, https://www.lifelock.com/learn-data-breaches-how-to-check-if-youre-affected-by-the-equifax-data-breach.html.

“Perspectives: Companies Get off Too Easy with Data Breaches. Bigger Fines Are a Good Place to Start.” *CNN*, Cable News Network, 31 July 2019, https://edition.cnn.com/2019/07/31/perspectives/capital-one-data-breach/index.html.

Staff, Techworld. “The Most Infamous Data Breaches.” *Techworld*, 16 Apr. 2019, https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/.