Policy Analysis Paper 2
Arrington Goode
CYSE 425

The Political Implications of Popular Web Browsers and How they are Harmful

Cybersecurity as it relates to law and politics is a very nuanced topic. Elected officials have had some difficulty creating and upholding certain laws and procedures when it comes to cybersecurity and the broader cyber world in general. Specifically, popular web browsers such as Google, Bing, and even Safari have dominated our online usage. They are the main way that we look for and receive information. However, the corporations that run these companies often do not have the compassion for the everyday person. They will usually cut corners. They are just like the elected officials and policymakers in that regard. People who have no true intention of helping those who really need it. Laws, policy, and government are a pillar that holds us together. If we do not want society collapsing we must examine the implications of not creating helpful laws, the attempts to make helpful laws, and finally what was the outcome of different laws that have already been established.

First we have to establish what are the potential dangers of technology before we can discuss the implications of not creating new laws to sustain it. In a book titled “CyberWar, CyberTerror, CyberCrime and CyberActivism an in-depth guide to the role of standards in the cybersecurity environment,” the authors explain how deadly technology can be. It has fundamentally changed the ways in which we interact with the world. The book explains how dangerous in particular web browsers can be. Web browsers control the flow of information. If the flow of information is not regulated then multiple dangers could occur. Misinformation can spread like wildfire or viruses and malware can dig their way into people’s computers. Due to this, it is vital that the government establishes certain laws that protect citizens from not only

these web browsers but also the internet as a whole. However, investigating web browsers will give us the basis to assess the political aspect of the whole internet since web browsers are the first step in investigating this larger world. When no laws or policy is made to combat the rapidly changing world, companies are left to interpret existing laws in whatever way they see fit. This usually means that they stop providing their best service and instead settle for a mediocre service.

The next step in discussing the political implications of web browsers and the internet in general, is to look at an attempt in which the government tried to create a law. In an article titled, "Cybersecurity Legislation: Preparing for Increased Reporting and Transparency," the authors discuss recent laws that have gone into effect and how they have transformed the cyberworld. One example of this is the Cyber Incident Reporting for Critical Infrastructure Act. (CIRCIA) This act says that any company has to now report any cyber attack to the Cybersecurity and Infrastructure Security Agency. (CISA) This is an excellent example of the political climate changing to keep up with the cybersecurity world. Due to this law, companies are now forced to report anything that goes wrong within their company. Then the agency can look deeper into and assess what happened. Now that this law is in place businesses, such as the ones that own Safari, Google, and Bing, are now required to act in the best interest of the consumer. They know now that they are under the law and so they must follow it. Which, in turn, means that more people are protected.

Finally, we must look at the outcome of different laws being enacted. When a law is put into place, it takes a while for it to really change the way society does things. Every aspect of our lives is a direct result of some law. When we examine the changes in the cyberworld due to these different laws being enacted, we can see some prevalent changes. The article titled,

“Cybersecurity Developments and Legal Issues,” gives us some insight into the changing world of cybersecurity. The authors explain how different the online world looks now and how different laws are put into place to help inspire change. In today’s time, we now can see how these laws are impacting us. Our internet browsers are heavily regulated and are working in our best interest. Different websites now have to report their cyberattacks. These are just of the very small changes that make a huge difference. While we do have a long way to go, we can still appreciate how much the online community has changed for the better. The political landscape is rapidly changing to keep up with the cyberworld and each day we get closer to a truly safe internet.

Works Cited

Bailey, Tucker, et al. “Cybersecurity Legislation: Preparing for Increased Reporting and Transparency.” *McKinsey & Company*, McKinsey & Company, 17 June 2022, www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency.

Ivory, Ian, et al. “Cybersecurity Developments and Legal Issues: White & Case LLP.” *Cybersecurity Developments and Legal Issues | White & Case LLP*, 22 Mar. 2023, www.whitecase.com/insight-alert/cybersecurity-developments-and-legal-issues.

Mehan, J. (2014). CyberWar, CyberTerror, CyberCrime and CyberActivism an In-depth Guide to the Role of Standards in Cybersecurity Environment.