Social Implications of the Cybersecurity Enhancement Acts

Introduction

In legislation, laws of all types have the chance to generate social issues based on what it aims to achieve when made legitimate by Congress. These issues can be glaring at times with violations of certain civil and public rights outlined by existing documents for individuals and groups of people, including organizations and companies. As is the case with ethical issues that can arise from certain acts and laws, the social implications are just as subjective. What may be a social issue for one party or group, may not actually be one for another and thus a discussion is had to sort out these issues. For the cybersecurity enhancement act of 2014, many of these issues came in the form of a violation of basic human rights and having to report activity and dealings between companies all over the United States, which can be seen as an invasion of company privacy by some.

Social Implications of the Cybersecurity Enhancement Act of 2014

As mentioned above, the Cybersecurity Enhancement Act of 2014 was not met with a lot of controversy when it was first adopted and made into a legitimate law. However, after more cybersecurity laws were made, groups of people became aware of the possible implications and threats that each one had on rights of individuals and groups. According to an article from Public Knowledge, many cybersecurity policies and laws are overly broad and ill-defined and lack clear checks and balances. This can definitely lead to issues with basic human rights for individuals and cause innovation and law creation to stall completely. Some of the main things that are defined as social issues within cyber policies and laws are monitoring all communications

(invasion of privacy), censorship (right to free speech), and possibly wrongful criminalization if a user was to voice their opinions and views on the internet.

Social Factors That Influenced the Creation of the Cybersecurity Enhancement Acts

In the world we live in now, cyber threats were the biggest social factor that led to the creation of these acts and laws. People began to think differently about how to gain secrets and information from the use of a computer. The world had to come up with a way to defend against that and quick. These laws were made in hopes of defending and securing information of all kinds and worked for the most part, however, we have learned that nothing is going to stay 100% secure. These acts are the best thing that can help secure and defend information from being leaked or stolen for someone else's gain. Every year, several new cyber policies and laws are introduced and made into law to shore up defenses in our foundations. Encryption is a massive part of this security and defense system. As for the cybersecurity enhancement act, part of what made it effective was the mandatory reporting of cyber threats and attacks for everyone. DHS became a centralized command center for all incoming or existing threats that were happening across the country. This move created a need for the public, private, and government sectors to come together and achieve a system in which they could all benefit and ensure that they would have help if they were to need it. However, some groups saw it as an invasion of privacy and did not want to comply with the rule as they believed that they could handle their cyber related issues themselves.

Works Cited

Appazov, Artur. “Legal Aspects of Cybersecurity - Justitsministeriet.” *Www.justitsministeriet.dk*, 2014, https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.

K, P. “Cybersecurity and Human Rights.” *Public Knowledge*, Dec. 2014, https://publicknowledge.org/cybersecurity-and-human-rights/.

McCaul, Michael. “H.R.756 - 113th Congress (2013-2014 ... - Library of Congress.” *Www.congress.gov*, 2013, https://www.congress.gov/bill/113th-congress/house-bill/756.