Maria Vargas Dominguez
ITS343: Cyber Law and Ethics
Paul Nevill
April 11th, 2023

Week 11-12: Chapter 6 - Securing the Electronic Frontier

The word hacktivism already seems to be used as the fact of hacking in a moral way. Hacktivism can be defined as the action of hacking with the intention of promoting a political or social agenda. In the case study of "The Lulz Sec Hackers" provided in the book "Cyberethics: Morality and law in Cyberspace", it is considered that The Lulz Secc Hackers hacked in a moral way since their supposed intentions can be justified by the meaning given to the word hacktivism, "hacking with the intention of promoting a political or social agenda". Among their most notorious cases of hacking, we can find the hacking of the Central Intelligence Agency's website, Sony Pictures, or the hacking of 2000,000 user accounts of the video game Brink, a product from Bethesda Software (Spinello, 2021). In spite of these actions, The LulzSec Hackers defended that they performed these activities with the purpose of finding security holes among large companies, and demonstrating how "the solid security guarantees proclaimed by companies and public bodies are nothing more than a passing illusion" (Spinello, 2021). Therefore, they portrayed themselves under the term of ethical hackers, thus what they were doing was good for society since they found the weaknesses and vulnerabilities of the security system of the companies. Their actions only demonstrated the lack of security and the need to work on a stronger security system.

In "Cyberethics: Morality and law in Cyberspace", it is explained that hacktivism can be justified on different and special occasions. In the case study, it is pointed out that hacktivism is a valid form of online protest and civil disobedience. What this principle seems to advocate is that hacktivism is seen as morally permissible if it is a proportionate response to an unjust situation.
As already indicated above, another situation in which hacktivism seems to be justified is to expose security deficiencies. It is therefore seen as a good thing since the purpose of hacktivism in this situation is to make a certain company aware of its security holes and can reinforce them to prevent hackers from breaching its security wall in the future.

Although this circumstance is not quoted in the case study, I imagine that hacktivism would also be morally justified if it is done for the purpose of hacking into systems or websites that are involved in unethical or illegal activities. For example, in government corruption, or human trafficking, among others. Moreover, hacktivism would also be seen as morally permissible if they want to hack into the systems of other hacker groups because what these other groups are doing is not morally justified. In this case, the hacktivist aims to expose the wrongdoing or raise public awareness of different issues and therefore should be considered morally acceptable.

It can be concluded that hacktivism can be morally permissible under certain circumstances and conditions. Not every act of hacktivism is suitable and accepted since some of its practices can cause infiltration of data and private information that can harm companies, individuals, and families. I believe that the practice of hacktivism should be tightly controlled and only be accepted if it meets the moral rules accepted.

Work Cited

Spinello, R. A. (2021). Chapter 5: Privacy Rights in the Age of Surveillance. In *Cyberethics: Morality and law in Cyberspace*. essay, Jones et Bartlett Learning.