Philosophy and Ethics C&IS assignment 2

Menno Bartels
s1007797

Lucas van der Laan
s1047485

Marco Post
s1046670

Elwin Tamminga
s1013846

Ernst Hamer
s1047547

December 2021

1 Grey hat hacking should be legalized

The proposal is made, that the definition of criminality in gray hat hacking has to change. A grey hat hacker is someone, who has no permission to break into a computer system or online services, but does so anyway. His intentions are good, which basically means that the hacker will tell the hacked target that they have a vulnerability and not use the gathered information any further. The text states “Perhaps the litmus test for criminality should not be the accessing of information but what is done with that information and how the intruder acted”. This is in our opinion a very precise alteration to make because it shifts the border of criminality and gives more responsibility to the gray hat hacker himself. From a computer scientists point of view, one can argue that there are many more uses to tools like port scanning. In the field of networking, these so-called penetration tools, make the life of a computer scientist a lot easier. The advantages that one gets from such tools, should also come with responsibility for the grey hat hacker. When using these tools, it is the responsibility of the user to not wrongly used the information that is gained. This is a neutral instrumentalists approach; the tools in itself are not good or bad. The good or bad lies with the user of the tool.

Lets look at an example. Say Bob is setting up his fancy network at home. Bob is a computer scientist who has a hobby in networking and has a lot of knowledge of using penetration tools (like port scanning). His intent is to use these tools to be able to set up networks, and have a good time in doing so. Lets say he uses port scanning to find a port he himself set up, but with that he also finds open ports that belong to his neighbour, which make his neighbour vulnerable. He will not use the information he found himself, but instead notify his neighbour that there is some wrong setting within his network. Bob is not a criminal for setting up a home network, that is very much a legal practice. With such examples as an argument, we think that the shift that is proposed in the text is a good decision. However, what will happen if Bobs neighbour will take the case to court that Bob hacked his network?

Of course, not everyone will go the length of notifying the target that they have a leak. Even in that case, we think that the grey hat hacker is not in the wrong here. As long as his intentions, or rather actions, do not negatively influence the target, he is all right. Measuring someone intentions is not an easy thing to do, so we think measuring based upon his actions is a better practice. But then again, we can’t consider draw a line on where the legal practices stop, and the illegal ones begin. We think that such decisions should still be made from case to case.

2 Web scrapers and Robot denial files

The text proposes the following: “Should web scraping which ignores robots.txt instructions be considered hacking?” We think this depends on what the web scraping is exactly doing and how it affects the website that is being scraped. It cannot be fully put under one umbrella as it is completely dependant on how the scraping is being done and what is done with the data that comes form the scraping.

There are websites like archive.org that archive the internet as best as they can by scraping and storing webpages. This used to be done according to the robots.txt, but in 2017 they announced that they would stop doing so. [3] Archive.org decided that the robots.txt should not apply to them because “We see the future of web archiving relying less on robots.txt file declarations geared toward search engines, and more on representing the web as it really was, and is, from a user’s perspective.” and the fact that a lot of defunct websites would get removed as the “parked” domain would block all search engines using robots.txt, thus also blocking the archiver. Before the internet we also preserved history because we think that it is valuable to know what happened and to learn from it. Now that everything is digitized the internet is part of us and society (mediation theory), so we should also preserve the history of important events that happens on the internet, like we did with books or scrolls in the past.

We also think that price comparison websites (e.g. Tweakers) that use web scrapers to retrieve the current prices of products from different stores should be legal, even if they ignore the robots.txt instructions. Most stores will likely have a robots.txt to prevent this, because they have to compete with each other. So a price comparison website cannot exist without ignoring the robots.txt instructions. We think this should be legal because it can be seen as a tool (instrumentalism). As a consumer it is not forbidden to go to the website of each store to compare the prices themselves, so a comparison website just makes it easier for the consumer to compare those prices. The benefits that comes from the existence of these tools also outweigh the problems described in the text (special offers, unrepresentative or out-of-date information), which can be solved by the stores themselves by making it easier for scrapers to take into account these changes so they can adjust the price accordingly.

We conclude that in general, it should not be illegal in nature, but instead be illegal if it negatively impacts society. This because there are use cases where it should be legal for a web-scraper to ignore the robots.txt like described above.

3 An immune system for the internet

The article states that we should create “ethical” viruses and worms that update computers of owners that either knowingly or unknowingly refuse to keep their systems up to date. It’s basically an enforced updating of operating systems for owners that either don’t know about updates or don’t want to update their systems.

An argument for this method of updating operating systems can be made by recognizing that we all benefit from an healthy internet. To keep this clean and healthy internet we have to take away some personal agency of users and force them to update their systems. They will benefit from this method of updating without knowing about it.

The opposite argument can also be made: as the owner of machine I should be able to do with it what I want. No one should be able to force me to do anything, even if it’s worse for the system as a whole or I don’t know what I’m doing.

Both arguments have merit. The argument for taking control away from the end users can be defended by arguing that the internet should be a equitable place where every one gets equal treatment, and thus we must level the field such that everyone has a safe system to work and play on. The argument against can be defended by arguing that we don’t know what the results will be of forcing users to update their systems and taking away agency could be slippery slope that should be tread with caution. One such a worm is loose, it cannot be stopped.

No matter which opinion one chooses as their own we must admit that such problems as these will have a greater presence as technology influences our daily lives in an ever growing capacity. Not only that, as technology influences us more and more we will also steer the direction technology will take in the future. Some institutions have been created to give direction to technology such that it will be beneficial to society as a whole. An example of this is the IEEE which has the goal ”to foster technological innovation and excellence for the benefit of humanity” [2]. Rather than just releasing a worm that enforces updates on machines with unknown consequences, better protocols can be created in cooperation with other institutions such as software companies or governments. One successful example of this is the creation of the GDPR, which now ensures that consumers have ownership of their data. [1]

We think that rather than just forcing consumers to behave a certain way, better technologies can be created that ensure that the internet is a safe and productive technology. By creating institutions that democratically decide on how to solve certain issues we can come to solutions that maximizes the benefits societies enjoy from technologies and create technologies that are easy to use and do exactly what we want them to do.

References

[1] Data protection under gdpr. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm. Accessed: 2021-12-29.

[2] Mission vision. https://www.ieee.org/about/vision-mission.html. Accessed: 2021-12-29.

[3] Mark Graham. Robots.txt meant for search engines don't work well for web archives. https://blog.archive.org/2017/04/17/robots-txt-meant-for-search-engines-dont-work-well-for-web-archives/, 2017.