Millennials and their Interpretation of the Concept of Hacking

Name	Aniek van den Brandt
Student ID #	6230906
E-mail address	a.vandenbrandt@student.maastrichtuniversity.nl
Course code	DCU4000
Group number	01
Supervisor/tutor	Prof. Karin Wenz
Assignment name	Final paper
Assignment #	00
Attempt	REGULAR
Academic year	20192020
Date	24-10-2019
Words	3298
Filename	20192020-DCU4000-00-REGULAR-6230906.pdf

Introduction

New digital practices appear frequently in today's media landscape. The way they are perceived by the public, are important for the impact they have on society. An example of this, is hacking. Since people are almost constantly online nowadays, it is inevitable that we hear about hacking practices frequently. Hacking, in this way, is an example of techno-moral change. Its development has impacted and is still impacting our society's value frameworks (Kudina and Verbeek, 2019).

Especially Millennials (people born between 1980 and 2000), who have grown up with computers and internet and as a result are able to adapt to new technologies very fast (Sweeney, 2006), are expected to have knowledge about hacking practices. They are digital natives. They read about hacktivist groups like Anonymous, that hack from political motivations, on social media. They receive warnings on their digital devices about their personal data running the risk to get hacked. Maybe they even have been hacked in the past, for instance during the Cambridge Analytica Scandal in 2018, during which 50 million Facebook profiles were harvested in order to get user data to target American voters (Gadwalladr and Graham-Harrison, 2018) All these experiences shape their view and opinion on the concept of hacking.

However, hacking is more than the hacktivists of Anonymous and the Cambridge Analytica scandal. Hacking does not always have to be a criminal practice. Using Richterich's (2016) definition of hacking, the practice is mostly about creativity and innovation and the term traditionally refers to "the process of solving an issue in a smart, possibly unexpected way" (p. 22). When understanding the term in this way, hacking can be seen as a socially acceptable practice. However, there are other voices as well, those who label hacking practices as destructive and illegal. Those voices tend to focus more on hackers in the form of cyber-attackers, generalizing all hackers as people who are victimizing other people with their actions.

Millennials are expected to have some general knowledge about digital practices like hacking. The question, however, is if they look at hacking practices as socially acceptable or as generally destructive and illegal. Therefore, in this paper I am going to investigate how Millennials interpret the concept of hacking. To answer this question, a theoretical framework on hacking and its interpretation is built in the literature review. Also, a qualitative interview with a Millennial is conducted, in an attempt to get more insights in how this generation looks at hacking. During this interview, topics such as 'the definition of hacking', 'sources of knowledge' and 'experiences with

hacking' are discussed. The insights gained during the interview are analyzed using theoretical frameworks presented in the literature review.

Literature review

Hacking is thus an example of a practice that causes techno-moral change. It softly impacts society, by changing user practices and value frameworks and causes. Especially malicious forms of hacking cause this kind of subtle shifts in society (Kudina and Verbeek, 2019). One form of hacking is for instance cybercrime, which attempts the revelation of digital data and information that was not meant to be public. Sullins (2012) states that hackers who perform this type of hacking work from their ideology and a 'hacker ethic', which is about "the idea that computers should be freely accessible and decentralized in order to facilitate "world improvement" and further social justice" (Sullins, 2012: n.p.). This is contradictory to an ideology in which privacy is the greatest good. This form of hacking has thus created a moral debate with values of data security and privacy on the one hand and openness on the other (Sullins, 2012). One's position in the debate influences one's value frameworks and user practices, which means we can speak of techno-moral change.

However, hacking is not purely about crimes and privacy issues. Jordan (2017) proves this in his genealogy of hacking, in which he distinguishes four phases in the development of hacking. The first phase is the 'pre-history of hacking'. This phase is about the emergence of hacking, in which four threads played a role: "conceptions of cyberspace as a place; techniques for manipulating materialized information; communities in virtual environments; and, the rise of programming as a profession involving both free software programmers and the programming proletariat" (2017: p. 10). They have formed a basis for the further development of hacking.

The second phase is the 'golden age of cracking'. Cracking is defined by him as "illicitly breaking into someone else's computer through a range of techniques" (Jordan, 2017: p. 14). In the golden age, the distinction between cracking and hacking almost disappeared. Often, the intentions of the hackers were not criminal, but in many cases, their practices did cause damages. However cracking was not the only hacking activity present in the golden age, it was the most general association with the concept of hacking.

In the third phase, Jordan sees the identification of hacking with cracking coming to an end. Hacking could now be divided in four phenomena: "rise of cybercrime, emergence of hacktivism, new prominence of free software and emergence of open source; and, the idea that hacking is an ethic of creativity" (2017: p. 18). These four divisions contributed to a process in which the term

'hacking' was pulled away from the connotation of hacking to cracking, and returned to a connotation to the broader idea of hacking as clever ways of using information technology.

The fourth and final phase, Jordan (2017: p. 22) sees as a dichotomy between triumphant and lost. He recognizes triumph in institutions and governments that hire hackers to help them secure their computer systems. At the same time, he also still sees that hacking is sometimes interpreted as a purely criminal activity. The latter is also the form that is mostly present in the news.

From all of this, Jordan argues that hacking "should be understood as practices that express the rationality of information techno-cultures" (2017: p. 3), in which he thus keeps the definition of hacking very broad, without focusing on specific practices within the concept of hacking. That aligns with the definition given in the introduction, in which hacking is explained as "the process of solving an issue in a smart, possibly unexpected way" (Richterich, 2016: p. 22). This definition is broad as well, however Richterich focuses mainly on the creative and innovative sides involved in hacking. She ignores the criminal activities, while Jordan does include them in his explanation of the term, without focusing on this side only.

Thus, in academia, there is acknowledgement for the broader definition of hacking. However, when using the word 'hacking' or 'hacker' in everyday life, the focus is often only on the malicious side of the practice. The widespread definition of hacking generally refers to "unauthorized intrusion into a computer or a network" (Techopedia, n.d.: n.p.). A similar definition is used by Google (see Figure 1).

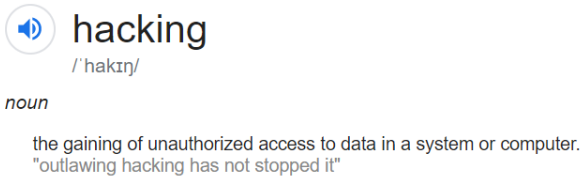

Figure 1: the definition of hacking according to Google

Thomas (2005) states that even though the amount of criminal hacking events have decreased in the last decades, the discourse on hacking in the fields of media and politics is still negative. He speaks of a "demonization of hackers being out of proportion to the threat" (Thomas, 2005: 600), not only in the golden age of cracking, but also today. Wall (2012) underlines this argument, by stating that the stereotypes on hackers are often negative, not only in the regular media, but also in popular cultures like science-fiction movies. Hackers are presented as

cybercriminals there as well and according to Wall, that has been "very influential in shaping our understandings" (2012: n.p.).

Thus, there is a certain indistinctness on the definition of hacking, with on the one hand hacking as an activity of cybercrime and on the other hand as a creative, innovative activity, raises the question which definition of hacking is the most common in society. If Jordan (2017) is right, we are now in the fourth phase, which means there is a dichotomy between the right and the wrong sides of hacking, also known as 'black hat hacking' and 'white hat hacking' (Wall, 2012: n.p.), but that at least both forms of hacking get a stage. However, if the most used definition is the one in which the focus is on cybercrime, as Thomas (2005) and Wall (2012) state, the general interpretation of the word hacking might lean more towards the back hat hacking, which would mean there is an incomplete image of hacking.

Methodology

For this paper, the qualitative interview is chosen as a research method. I conducted one in-depth interview with a Millennial, in which the selection of the interviewee was based on a few factors. Firstly, the Millennial was not supposed to have a background in hacking him- or herself. Secondly, he or she was supposed to follow the news on a frequent base, since media are expected to be of large influence on the interpretation of hacking.

The conducted interview is semi-structured, which means that prior to the interview, I prepared several questions. The follow-up questions depended on the answers given during the interview. The questions prepared, I divided into several categories, namely 'associations with the word hacking', 'sources of knowledge', 'experiences with hacking', 'hacking in the news' and 'personal definition of hacking'.

Results

The interviewee is a 24-years-old female Millennial, born in 1995, from The Netherlands. She does not have a background in hacking except from what she describes as general knowledge herself, and she follows the news on a frequent basis via news platforms on social media.
The interviewee had mainly negative associations with hacking. She stated that the word has a negative connotation and she came up with a few examples of hacking, in which the malicious side of it was clearly present. She mentioned Russian hackers that tried to manipulate the American voting systems. She also mentioned WikiLeaks and other big data leaks that were in the news

recently. Furthermore, she pointed out some small-scale cases of students hacking school systems and a recent case in which a man hacked the ticket system of a theme park and started blackmailing the park after that.

The question whether the interviewee could come up with examples of positive forms of hacking has been asked explicitly, but she had no examples of real events that recently happened. The only example of positive hacking she mentioned was an imaginary one: "You can have these organizations or maybe in some countries the government who are really closed and not transparent at all. And some information should be out in the open in order for people to make informed decisions about for example voting. So then I can imagine it could be positive." (Personal communication, October 2017, 2019)

The negative examples above, the interviewee learned about in the news, which she mentioned as her main source of knowledge about hacking. Besides what she learned from the news about hacking, she mentioned that she had also experienced hacking in her home environment once and that she had a training on prevention at her work, but she said those experiences had not been of big influence for her opinion on hacking: "When I hear about it in a personal environment, those are incidents that are very small-scale and don't usually have a big impact. But, when you hear it in the news, then it usually has a big impact. At least on society, so that's what comes top of mind for me." (Personal communication, October 17, 2019)

It turned out the interviewee also linked privacy issues with hacking, not on a personal, but on a societal level. That was something she was concerned about as well: "It does make me feel kind of worried about society and how or privacy of things. How you can guarantee privacy when hacking is possible, for example for bank accounts. That's more of a concern to me than the personal things on my laptop or telephone, because I don't think that's interesting to people." (Personal communication, October 17, 2019)

Elaborating on the privacy issues that can be linked to hacking, the interviewee believed that hacking often has to do with accessing data and sensitive information and revealing it to the world. That was something she stood very negative against: "It's about the bigger picture of privacy. (…) And I think in 99 percent of the cases privacy is more important than getting the information out in the open. (…) Maybe 1 percent could be positive, but I think usually it's negative." (Personal communication, October 17, 2019)

Besides this, the interviewee could not think of any positive intentions hackers might have. In her reasoning, she mainly focused on the harm hacking can do to society. That influenced her

general image of hackers: "I honestly don't know why you would want to do it. (…) I wouldn't want to do it. I wouldn't want to get information that I'm not supposed to get. So that makes my image of hackers not very positive." (Personal communication, October 17, 2019)

According to the interviewee, the word hacking has a very negative connotation. However, she was also provided with the idea that the definition hacking does not always have to be negative. The word 'lifehack', which means a creative strategy of using a certain technique, in order to manage daily life activities more efficiently, was used by the interviewer to illustrate this. In a reaction to this, the interviewee underlined the truth that the term can be interpreted differently, but after that, she stated that she thinks a more negative association was, according to her, more logical: "If you say hacking, then you don't think about lifehacks. Then you think negatively. I think most people would think negatively." (Personal communication, October 17, 2019)

After talking about hacking and associations for a while, the question if the interviewee could come up with a definition of the practice was asked as well. The definition for hacking she came up with was: "Getting into a system, and that could be anything digital, and getting information out of that that you're not allowed to get out of it." (Personal communication, October 17, 2019)

Discussion

Before starting on the discussion of the results, it is important to point out some limitations of this research. Firstly, only one Millennial was interviewed. To gain information about the whole group and to be able to generalize, more Millennials should be interviewed. The gathered data is not representative for the whole group. Nevertheless, the outcomes are interesting and can be linked to what was discussed in the Literature review.

Firstly, there seems to be a big consensus between the definition of the interviewee ("Getting into a system, and that could be anything digital, and getting information out of that that you're not allowed to get out of it") and the definition of Google search ("The gaining of unauthorized access to data in a system or computer", see Figure 1). The definition of the interviewee, and also the examples given during the interview, are not even close to definitions of Jordan (2017) or Richterich (2016), in which the focus is more on the creative side of hacking.

The definitions given by the interviewee and Google search are very similar, but as discussed in the Literature review, also one-sided, with a focus on the malicious type of hacking. They are even very similar to what Jordan (2017) defined as cracking. Interpreting the term hacking in this way, for

the interviewee meant that she worried about hacking as well. She stated that she was not that worried about her personal computer or laptop, but she was worried about the bigger picture of the privacy of society. In this way, techno-moral change is happening: the interviewees view on hacking has changed her value framework on privacy. Also, in the trainings the interviewee had in her work environment, she learned about hacking as a criminal practice as well. These trainings were about prevention mostly, and after those, she changed some of her user practices. An example she mentioned was how she learned to recognize phishing mails and that she had to instantly delete them.

If more Millennials interpret hacking in this negative way and adapt to that, the question is whether we are in the fourth phase right now, in which both morally right and wrong forms of hacking are present and are 'fighting' against one another, or if we are back in the golden age of cracking (the second phase), in which hacking has become a synonym for cracking. It is a fact that there are many types of white hat hacking as well, but if people are not able to make a clear distinction between the right and the wrong side, or more precisely, do not know about the types of hacking that are morally right, it seems like the dichotomy between the white hats and the black hats has been won by the latter.

Furthermore, the interviewee stated that the media were her primary source for knowledge about hacking. What she read in the media was more important than for instance the experiences in her home environment and at work. Also, the news is where she learned about the negative examples of hacking, and even though it was explicitly asked, she could not come up with a real-life example of a case of positive hacking. From this, it can be concluded that she has not seen, or at least not consciously, any positive examples of hacking in the media lately, even though she followed several different newspapers and platforms. That raises the question whether the image of hacking that is drawn by the media in general is complete, or if it is framed into the direction of the malicious side of hacking. The mass communication 'framing theory' states that "the way in which the news is presented, creates a frame for that information" (Mass Communication Theory, n.d.: n.p.). This influences the opinions of the public on a certain topic and can thus change their value frameworks. Following this theory, it would be interesting to do a content analysis, to research if it is true that the frame on hacking that is used by mass media, is a negative one, that focuses on black hat hacking.

As stated in the beginning of the Discussion, the data is limited because of the small number of interviewees. Nevertheless, the gathered data confirms that the interpretation of the term hacking

is very one-sided, with a focus on malicious forms of hacking, as was expected from the information presented in the literature review as well. That is interesting, and one suggestion for future research therefore would be to increase the amount of interviewees, to see if this one-sided view is something that is characteristic for all Millennials.

Conclusion

After discussing the results, it can be stated that this research paper is limited in its ability to generalize, but that it offers several suggestions for further research on hacking. The research question 'What interpretation do Millennials have on the practice of hacking?' is difficult to answer based on only the data of only one interviewee. However, based on the data and the literature review, an estimation can be made, which is that the interpretation of Millennials is quite negative, because there is an incomplete image of the practice of hacking. In this image, the focus is on black hat hacking. A possible cause for this incompleteness could be the way hacking is framed by the media, where the focus is probably too much on the big incidents of data leaks and data security when it is about hacking. To confirm this estimation, there is a need for further research, for which in the Discussion a few suggestions were given.

References

Gadwalladr, C. & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election on 2019, October 21.

Jordan, T. (2017). A genealogy of hacking. Convergence: *The International Journal of Research into New Media Technologies, 23*(5), 528-544.

Kudina, O. & Verbeek, P.-P. (2019). Ethics from within. Google Glass, the Collingridge dilemma, and the mediated value of privacy. *Science, Technology, & Human Values, 44*(2), 1-24.

Mass Communication Theory. (n.d.). Framing Theory. Retrieved from: https://masscommtheory.com/theory-overviews/framing-theory/ on 2019, October 22.

Richterich, A. (2016). 'Do not hack'. Rules, values, and communal practices in hacker- and makerspaces. *Selected Papers of AoIR 2016* (The 17th Annual Conference of the Association of Internet Researchers, Berlin, Germany, 5-8 October 2016).

Sullins, J. (2012). Information technology and moral values. *Stanford Encyclopedia of Philosophy*. Retrieved from: https://plato.stanford.edu/entries/it-moral-values/#MorValComAccInf on 2019, October 23.

Sweeney, R. (2006). Millennial behaviors and demographics. *Newark: New Jersey Institute of Technology*, *12*(3), 10.

Techopedia. (n.d.) Hacking. Retrieved from https://www.techopedia.com/definition/26361/hacking on 2019, October 21.

Thomas, J. (2005). The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age'of hacking. *New Media & Society, 7*(5), 599-624.

Wall, D.S. (2012). The devil drives a Lada: The social construction of hackers as cybercriminals. *Constructing Crime*, 4-18. Palgrave Macmillan, London. Retrieved from https://link.springer.com/chapter/10.1057/9780230392083_2 on 2019, October 23.