Stefanie Plank

Master's thesis

University of Lapland

Faculty of Education, Media Education

Spring 2022

Perception of privacy of young users on social media

- Analysis of the privacy paradox on the application TikTok

University of Lapland, Faculty of Education

The title of the thesis: Perception of privacy of young users on TikTok -Application of the privacy paradox on TikTok

Author: Stefanie Plank

Degree programme / subject: Media education

The type of the work: Pro gradu thesis_X_Laudatur thesis__Licenciate thesis__

Number of pages: 86

Year: 2022

Summary:

Privacy is challenged online and especially on social media. Nevertheless, people use social media platforms and post their private information, besides their privacy concerns. This phenomenon is called the privacy paradox. In this study, the goal is to understand how teenagers perceive their privacy online and how the privacy paradox can be applied. The focus of this research was the platform TikTok, owned by ByteDance with billions of especially young users. On the platform TikTok you can watch short videos from various genres and produce content yourself. I conducted three focus groups, with in total of fifteen teenagers living in Luxembourg, in which the participants were asked to reflect on their usage and privacy management on TikTok. The focus groups were recorded, transcribed and the data was examined following the thematic analysis method. The results show that knowledge, risk awareness, and the importance of social media in the lives of teenagers influence their privacy management. Depending on how they assess the risks to be relevant to them, they adjust their behaviour online. They receive several benefits when using TikTok which they weigh against their fears. Moreover, the teenagers emphasize the peer pressure they experience to download the application. To be part of the trend and benefit from the positive aspects they associate with the platform, the adolescents find it difficult to resist using TikTok.

Keywords: privacy, social media, privacy paradox, risk awareness, privacy calculus, peer pressure

Further information:

I give permission the pro gradu thesis to be read in the library _X_

I give permission the pro gradu thesis to be read in the Provincial Library of Lapland _X

Contents

1. Introduction

Privacy affects everyone. It concerns our daily lives at home, on the street and our interactions with other people. To decide which information, we keep confidential and which one we want to reveal is a challenging and individual process in which people need to fix rules and negotiate between boundaries. Our privacy management is even more challenged when we are online and use social network sites (SNS). Yet, those applications are omnipresent in our lives – and especially in the lives of teenagers.

In the last years there has been a new application which got more and more attention: TikTok. TikTok is owned by ByteDance whose headquarters is located in China. In the year 2017 ByteDance bought the former application musical.ly and renamed it to TikTok. The rebranding helped the application to be known outside of Asia and increase the number of downloads especially among its young target audience (Spiegel, 2017). In 2021 there are already 1 billion users worldwide (TikTok, 2021a). "TikTok is the leading destination for short-form mobile video. Our mission is to inspire creativity and bring joy" (TikTok, 2022a), as the company presents itself. On TikTok you find short videos picturing various genres: dance videos, lip-sync videos, pranks, vlogs, cooking recipes, hauls etc. You cannot only watch the contents of other users, but you can also produce videos on your own with the integrated video editing tool. The format of TikTok with its fresh, innovative, endless and, moreover, fast-moving content seems to be especially attractive for its young users (Leander & Burriss, 2020).

However, even if the application is appreciated by many people, there are several concerns regarding TikTok. TikTok is accused of various ethical violations. This is mainly caused by its algorithm. The "For you"-Page is made in a way that you spend as much time as possible on the application as it shows you videos according to your preferences. The New York Times (Smith, 2021) analysed the paper called "TikTok Algo 101" in which ByteDance explains how the algorithm works. It tracks how much time you spend on a video and your interactions with different contents in order to show you only certain kind of videos to avoid boredom and instead increase your engagement with the platform. This algorithm can, however, also have negative consequences such as it can "sometimes lead young viewers down dangerous rabbit holes, in particular toward content that promotes suicide or self-harm" (Smith, 2021, n.p.). Additionally, there are more critics discussed in the media such as the risk of addiction (Meral, 2021); propaganda and radicalisation (Cox, 2018a; Cook, 2019), extremism (Weimann & Masri, 2020),

nudity of underaged children (Cox, 2018b) and misinformation (Tardáguila et al., 2019). Moreover, there have been scandals about suppressing videos of disabled users (Kelion, 2019) and banning LGBTQ + content (Hern, 2019). To offer a personalized experience a big amount of data from the users is needed which increases the concerns of a misuse of data privacy (BBC, 2021). The Citizen Lab (Lin, 2021) published a comparative analysis of security, privacy, and censorship issues regarding the application TikTok and Douyin (the TikTok version for the Chinese market) which found that similar to other social media networks like Facebook there is a lot of data collected about its users which are either stored directly in the TikTok servers and/or sent to third parties. In India, TikTok is banned for these reasons (Slater, 2020) and in the US the military was advised to delete it (Vidgor, 2020).

Even if there is a lot of criticism, there are still many users downloading the application. This phenomenon is called the privacy paradox. It describes the paradoxical behaviour that people - besides their concerns about their privacy - download and use applications and web services (Barnes, 2006). In this thesis I want to investigate this phenomenon further regarding the application TikTok while focusing on young users. The goal is to understand how teenagers perceive privacy on TikTok and if the privacy paradox in this case is applicable. To answer these questions, I conducted three focus groups in Luxembourg with teenagers aged 12 to 18 years. I want to understand which privacy risks young users are aware of and more importantly how they perceive them. Additionally, I want to know which measures the teenagers take to protect their privacy on TikTok. To better understand how people approach privacy and decide how they manage it, I first give a theoretical overview of what privacy is and how people decide which information can be disclosed. To round up the theoretical chapter, I will explain the privacy paradox by focusing mainly on previous research which tries to find reasons for the paradoxical behaviour of users. This will set the base for the data analysis in which I want to reflect on what privacy means for the teenagers on TikTok, how they protect it, which online risks they are aware of and lastly make the link to the privacy paradox and its effect on the TikTok usage of young users.

2. Theoretical framework

Privacy starts by locking the bathroom door within the own apartment but also includes being surveyed on the streets by cameras. It is the opportunity to keep personal information hidden and protects a person from being traced (Gellman & Dixon, 2011). To decide which information, we want to disclose is not easy, especially when taking the online environment of social network sites (SNS) into account. By taking a look at the theory and previous research on the privacy paradox, we will see that there are many new challenges to our privacy. In this chapter, I will present the importance of privacy and explain what influences our decision making concerning our privacy management online.

2.1 Privacy

Privacy is important at various stages in our lives. It concerns one's physical abilities, information, relationships, communications, status and wealth (Gellman & Dixon, 2011). Furthermore, Westin (1967), a prominent scholar researching privacy, explained that privacy helps us to gain personal autonomy with which people control their own lives. Privacy gives emotional release. When people are out of sight you can reflect on yourself, because it offers time and space for self-evaluation to process the experiences. Lastly, privacy also in a way supports building trust and intimacy because people can limit and protect their communication with others at the speed they feel comfortable with (Rosen, 2000). In general, privacy is important for one's dignity and self-determination. Having private space and being able to behave freely without being observed, matters on a psychological and sociological level (Clark, 2012). Taking Maslow's "Hierarchy of Needs" into account, Clark (2012) says that "privacy is about the integrity of the individual. It therefore encompasses all aspects of the individual's social needs" (p. 2) such as privacy of the person which refers to decisions about the own body and health; privacy of personal behaviour which concerns any sensitive personal matters; privacy of personal communication which gives people the opportunity to communicate without being intercepted; and lastly, privacy of personal data means to be able to control which personal information is available to whom.

Since privacy plays an important role in everyone's life, Gellman & Dixon (2011) highlight that "[p]rivacy is a right, a human right, a legal right, a moral right, a property right, a positive right, a negative right, a value, an economic interest, a personal interest, a societal interest, and other things"

(Gellman & Dixon, 2011, p. 1). It is a right which is protected under the "EU Charter of Fundamental Rights" under Article 8 which points out that "everyone has the right to the protection of personal data" (Official Journal of the European Communities, 2000, p. 10). Moreover, it explains that personal information can only be processed after giving consent, as well as every person can have access to the collected data (Official Journal of the European Communities, 2000).

Furthermore, privacy is "a state in which an individual is apart from others either in a bodily or psychological sense or by reference to the inaccessibility of certain intimate adjuncts to their individuality, such as personal information" (Graeme, 2002, p.6). Privacy can be therefore, described as a "limitation of others' access to an individual" (Gavison, 1980, p. 428). Gavison (1980) says, in addition, that there are three elements which play an essential role: "secrecy, anonymity, and solitude" (p. 428) which are independent and yet interrelated to each other. Especially the idea of 'secrecy' can be found in other works. Posner (1981) for example explains privacy by referring to *the interest in being left alone* and the *concealment of information* (p. 272-273). The idea of 'the right of being left alone' already comes from Warren and Brandeis in their famous article "The Right to Privacy" (1890).

The latter privacy interest of Posner (1981), the "concealment of information," includes secrecy which means having the right to keep certain facts about oneself private. However, equating privacy with secrecy, caused criticism which is why Amitai Etzioni (1999) for example emphasizes the selective secrecy which explains that an 'actor' (e.g., a person, a group or a couple) can disclose some information to someone and yet conceal the same information in another situation or with another person. Similar to this, is the idea of Livingstone (2008) states that it is less about the disclosure of information, but more about having control over the own private information. This means that people want to decide what information should be kept private and which information should be shared with someone. Also, Westin (1967) says that: "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). Therefore, as Lutz et al. (2020) point out their privacy is all about "the notion of control" (p.3). However, Julie Inness (1992) challenges this idea and points out that especially when it concerns intimate information, people feel a loss of their privacy when the information is disclosed.

Arthur Miller (1971), Alan Westin (1967) or William M. Beaney (1966) admit that it is difficult to find a comprehensive definition of privacy. Also, Solove (2002) compared various conceptions of privacy by looking at different research areas such as philosophy, psychology, sociology and law and he says that "[l]ooking broadly at the discourse, almost all of the criticisms boil down to claims that the theories are either too narrow or too broad" (p. 1092). Having one complete definition of privacy has so far been challenging for many researchers. To better understand how people perceive privacy, I will give more explanation on how people control their privacy and decide which information to disclose to whom. This helps to understand how people manage their privacy and how they protect it.

2.2 Privacy Management

Even if everyone is confronted with the question of privacy every day, people have different standards about what is acceptable and what is not (Gellman & Dixon, 2011). To decide which information, we keep confidential and which we want to reveal is a complicated question. People try to find the balance between the demands of the situation, the personal needs and the needs of the people involved. Privacy gives the feeling of being separate from others and of protecting oneself from the risk of feeling embarrassed, uncomfortable, or exposed when a private information is revealed in front of the wrong person. To understand how people decide which information they want to keep private and which not, people need to manage their privacy (Petronio, 2002). "Privacy management is not about setting rules and enforcing them; rather, it is the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres" (Palen & Dourish, 2003, p. 3).

Sandra Petronio (2002) developed a concept called 'Communication Privacy Management' to explain how people control their privacy. Her concept has been used to describe how privacy is managed within a family (Petronio, 2010) but also for computer-mediated communication (Child & Petronio, 2011) and social media use (Child et al., 2012) which is why it is relevant and useful for this thesis.

Petronio's concept (2002) works with the metaphor of personal and collective boundaries which are depicted as a demarcation between private and public information. Personal boundaries are there to protect private information about oneself; collective boundaries, in addition, take private information

into account which is shared between more people because it concerns all of them. The boundaries can be permeable or impermeable; can change with time and age, and they are often linked with each other. “Boundaries function to identify ownership of information leading to subsequent control over who knows about private matters” (Petronio, 2002, p. 7). The ownership over the information can be ambiguous or strict. Being the owner of the information, however, is relevant according to the Communication Privacy Management theory, as it means having control over the information. This allows to decide to either reveal or conceal the information, which is important in order to manage the risks (Petronio, 2002).

Furthermore, according to the Communication Privacy Management theory by Petronio (2002) rules help to regulate and coordinate the privacy boundaries with other people. Rules are based on five criteria which are connected to culture, gender, motivations, context, and risk-benefit ratio. Therefore, when thinking about disclosing private data these are the main factors which influence the decision. This means that people make decisions based on what their culture taught them to do and how they were socialized. Depending on their gender, they might come to different conclusions. For example, men and women have different expectations, therefore, set different rules. Moreover, depending on the needs, characteristics and the expected outcome, people have certain guidelines they like to follow. In addition, looking at the circumstances helps to understand why and how people determine rules. Finally, people compare the risk in relation to the expected benefit. Depending on how we evaluate the risks, people adjust the privacy rules. Those factors set the structural base for how privacy boundaries are formed (Petronio, 2002).

2.3 Difference of privacy on SNS

As this thesis wants to answer how teenagers perceive their privacy on TikTok, I want to give an overview of the difference between privacy in the offline world and privacy on the internet with the focus on social media networks (SNS). However, online and offline privacy cannot be separated fully because what you do and reveal online can affect the offline world and vice versa (Gellman & Dixon, 2011). Yet, online privacy has a different dynamic. When we take technology into account, there are new “privacy issues that appear to fall outside the bounds of our traditional analysis” (Austin, 2003, p. 164). These different privacy issues are going to be explained to highlight the challenges social media users have to face.

2.3.1 Less control over information

The danger of SNS is, as Gellman and Dixon (2011) paraphrase, that a person walking down a street usually knows that other people are watching and observing him/her; however, on social media a user might not be aware that his/her data is collected and used. In addition, Boyd (2010) points out the difference that "a conversation you might have in the hallway is private by default, public through effort" (n.p.). However, when you post something on a SNS it is the opposite: "the conversation is public by default, private through effort" (Boyd, 2010, n.p.). Boyd (2010) defines four specific features of SNS: persistence, replicability, scalability, and searchability. Therefore, the data is stored for a long time and reaches a big audience. Additionally, contents can be duplicated and reuploaded easily. The information is visible and there is the potential that it is seen by many users. Lastly, the information can be accessible also via other sources not only the SNS platform. Moreover, privacy is challenged because "information on social media sites may not only be searched without permission or knowledge but may be permanently stored, meaning some material intended to be private may never enjoy a cloak of privacy" (Lee, 2013, p. 147).

The online environment challenges the borders of privacy rules which mainly concerned the offline world. "As a result, online privacy is expanding in its definition to include things that traditionally were never recorded at all and that may not have been thought of as having an online component" (Gellman & Dixon, 2011, p.7). So have Palen and Dourish (2003) for example tried to expand Altman's conceptualization of privacy in order to adapt it to the online environment in SNS. A new challenge is, therefore, the new spatial boundaries since you cannot longer understand who watches the content online compared to the overview you had when you were in one room together. Moreover, there are threats to the temporal boundaries because the data is stored and recorded and is more persistent. Lastly, there are the "intersections of multiple physical and virtual spaces, each with potentially differing behavioral requirements" (Palen & Dourish, 2003, p. 130) which means that there is no selective control over who is accessing the information. The same content can now be seen by different people like your friends and your employer, to whom you would usually present yourself in different ways, however, in the online world this is difficult to control.

2.3.2 More information is collected

The information that is stored online does not only include information people share online, like posts on the profile and the messages people send in the chat. There is more data which is collected for example the places people go by tracking the location of the phone or the metadata of the photos which were taken at different places, the websites people click on, search terms we use on search engines online, and the products we buy online by using Internet cookies (Kirwan, 2016). Nowadays it is possible to create personal records of a person with all the information gathered from various sources like online shops, social networking sites, government agencies and other online businesses (Gellman & Dixon, 2011).

Especially considering that the life of many people and mainly teenagers is partially happening online, it becomes evident that by spending more time online, a more comprehensive record of a person can be created (Gellman & Dixon, 2011). It becomes comprehensive because the information from different sources can be linked through a variety of means (Kirwan, 2016). Considering the quantity of data collected, especially SNS "create a central repository of personal information" (Barnes, 2006). Yet, we need to take into account that online users want the best possible experience which can be done when the usage is personalized, which for a 'strong user model' needs to be created. "Strong models also require information about the user: demographic information, behavioural information, information about the user's social context, etc." (Zheleva et al., 2013, p.1). Therefore, the collected data ultimately provides a better and more personalized online experience for the user.

2.3.3 Interconnectedness

Another factor why privacy on SNS is challenged, is because of the interconnectedness with other users and third parties. Gellman and Dixon (2011) note five key areas where they see challenges for privacy on SNS:

> "(1) the definition of what constitutes public versus private information, (2) the role of users' consent and rights to their own information, (3) secondary uses of the data made available on social networking sites, (4) adequacy of notice, and (5) ease of exercising privacy choices" (p. 41-42).

Often the application and service can only be used if the user agrees to the data distribution to third parties. Therefore, the users do not have the choice if they want to use this platform. They have to their consent when they want to be part of this online community. Moreover, there is another question of consent on SNS. Often posting something on SNS publicly is seen as passive consent which allows for example potential employers to view the post. Even if there is sometimes the option to limit the access of this information to certain people, there is still the possibility that the information reaches a wider audience than planned for example if friends repost your contents (Gellman & Dixon, 2011). This problem is also addressed in the Communication Privacy Management theory by Petronio (2002) where she talks about the co-ownership of information. When information is shared with more people, they all have the responsibility to protect it. Therefore, when people post something on SNS other users become co-owners of the information. If their responsibility, however, is not followed, there might occur privacy turbulences and violations.

This becomes also relevant when thinking about privacy as a "networked privacy" as Marwick and Boyd (2014) suggest. They mention the fact that through simply being in a network, like on social media, other people within this network can publish information about a person – even information the person did not approve. In addition, on SNS there is an invisible audience which means that one does not know who the other users are reading the post, especially when taking the context collapse into account which means that different groups merge together (Machackova et al., 2015). "In result, because of the audience's invisibility and context collapse, SNS users cannot always sufficiently assess the social context of their disclosures, foresee their consequences, and overall adequately manage privacy boundaries" (Machackova et al., 2015, p. 97).

2.3.4 Privacy violations

On social media there are not only 'benevolent' users who want to enjoy communication on these platforms, but there are also 'malevolent' users. "Malevolent users include scammers, stalkers, and identity thieves" (Zheleva, Terzi & Getoor, 2013, p.2) or as Zheleva et al. (2013) continue there are users who mine and sell data for targeted advertising or other data misuse.

Considering the interconnectedness of users online, different possible privacy breaches can occur. Especially via links and connections to other users, one's privacy management is challenged (Marwick

& Boyd, 2014). Privacy breaches as Zheleva et al. (2013) list can be: Identity disclosure, attribute disclosure, social link disclosure and affiliation link disclosure. Through identity disclosure, one's identity can be revealed by matching the profile with the real person. Attribute disclosure is when certain attributes found on SNS correlate with the real attributes of the person. Social link disclosure reveals relationships via connections online and lastly, affiliation link disclosure comes along with a group membership which can be of sensitive nature (Zheleva et al., 2013).

In general, when thinking about privacy you can distinguish between institutional and social privacy threats. Social privacy threats mean that users are concerned that other users are able to access their information. Institutional privacy threats, on the other hand, mean that people are concerned about how third parties are using the collected personal information (Raynes-Goldie, 2010). Similar results have Krasnova et al. (2009) found in their focus groups, yet they refer to them as organizational and social threats. Social threats refer to threats like uncontrollable actions, bullying, and stalking and organizational threats refer to the data collection and distribution of the provider and third parties.

Since especially on SNS there is the danger that our privacy is violated, users need to have more strategies on how to act when unwanted information is shared. This is what the Communication Privacy Management theory describes by enacting but also negotiating privacy rules, in order to control the private information (Petronio, 2002). Moreover, Trepte (2015) points out that there is the need for metacommunication, to be able to reflect on how people want to handle private information. This includes checking privacy settings on SNS. Since whatever we post or communicate on SNS belongs to the web server and is sold to third parties, it becomes evident that being online challenges our privacy routines. Challenges or privacy breaches can be solved easily when they are taking place offline like communicating with that person or adjusting the induvial rules. However, when those turbulences occur on SNS, it is more complex which is why metacommunication is needed. Users are required to reflect about their actions and possible consequences and adjust their privacy settings. Negotiating privacy influences the way of communication, since it determines what we communicate and how we do that (Trepte, 2015).

Last but not least, it is important to mention that the user's rights are protected by the European law under the name EU General Data Protection Regulation (or GDPR). These rights apply to companies that are located in the EU or offer their services in the EU. This includes for example social media

platforms when they request personal information of people living in the EU. It allows the companies and organizations to collect data when users give their consent which they can reject at any time. Moreover, the user needs to get access to the data whenever wanted and needs to get the possibility to correct the information. In addition, there is the 'right to be forgotten' which gives the users the chance that all their data can be deleted if the data is no longer needed or is used unlawfully. Whenever there is a data breach, it needs to be reported to the nation's data protection authority (European Union, 2020).

2.4 Privacy paradox

Privacy is a complex construct that is relevant for many of our daily decisions. However, especially when thinking about our behaviour online on social media networks, privacy is at a higher risk of being violated. We have less control over our information as we share it with numerous other users who have access to a lot more information than in an offline setting. Moreover, companies and providers store our data and use it for their purposes. Now the question arises why people voluntarily use SNS nevertheless.

To look for an explanation for this behaviour, Barnes (2006) coined the term "privacy paradox". In her essay, she highlights the problem that many users -especially teenagers- are eager to share their intimate stories on SNS which causes many privacy issues. She says: "teenagers will freely give up personal information to join social networks on the Internet. Afterwards, they are surprised when their parents read their journals" (n.p.). The contradiction between wanting to keep a dairy safe in order to take care of the privacy, but at the same time posting similar personal stories and details online which are accessible to many people, is described in Barnes' paper as the phenomenon of the privacy paradox. This means that even if people express that they are concerned about their privacy, they nevertheless, reveal their personal information online and use services which collect their data. Barnes (2006) explains this by saying that the "teens are not aware of the public nature of the Internet" (n.p.) and that "private versus public boundaries of social media spaces are unclear" (n.p.). Therefore, even if people - and according to Barnes mainly teenagers - want to keep their information private, they still post them online because they do not realize or understand that SNS is a public space through which other users can access this information.

Norberg et al. (2007) established the term further and describe the phenomenon followingly. On the one side, there is the development of technology which make it easier to collect, distribute, store and manipulate information about users; and on the other hand, there are users who are concerned about their rights and privacy because of this development. Yet, the same people who are complaining and expressing their concerns are the ones who freely give away their personal information online. This dichotomy between being concerned about privacy online, but yet sharing personal information describes the privacy paradox. In other words: "on the one hand, users express concerns about the handling of their personal data and report a desire to protect their data, whereas at the same time, they not only voluntarily give away these personal data […] but also rarely make an effort to protect their data actively" (Gerber et al., 2018, p. 227).

2.5 Research on the privacy paradox

In general, there has been a lot of interest in the topic of the privacy paradox in research. Especially in the early 2000s when SNS like Friendster and MySpace emerged and made communicative practices like posting photos or sharing thoughts online more popular, the topic of privacy in the online world and the paradoxical behaviour became interesting for research (Boyd & Ellison, 2007). Therefore, the focus of the research on the privacy paradox was mainly connected to social media and digital technologies (Acquisti & Gross, 2006; Quinn, 2016; Tufekci, 2008). Additionally, there has also been similar research connected to online shopping (Brown, 2001) or e-commerce (Spiekermann et al., 2001). Acquisti & Grossklags (2003) already looked at this problem and tried to understand why there is the dichotomy between the stated attitudes and actual behaviour without using the term 'privacy paradox' on SNS. In addition, they continued with their research and made a study on Facebook to prove that there is this paradoxical behaviour. Their result was that the privacy concerns of an individual are only a weak predictor of saying if the person is going to sign up and use this platform or not (Acquisti & Gross, 2006). Furthermore, there have been studies that looked into the different perceptions people have about privacy. So found Humphrey (2003), in cooperation with Dr. Alan Westin who has done many years of research about privacy, three different groups of people. There are privacy fundamentalists who are very concerned about privacy matters; there are privacy unconcerned who are not worried about privacy; and lastly, privacy pragmatists who do have strong feelings concerning privacy and, therefore, want to protect it, however, this group of people is also likely to disclose information whenever they see a valid reason for it. The last group is in particular interesting for this study in the context of the privacy paradox to understand why and when people are willing to trade personal information.

Current research on the phenomenon of the privacy paradox tries to find explanations for the paradoxical behaviour of users. I grouped different approaches into five categories: the importance of SNS in the lives of especially teenagers, the theory of the privacy calculus, the lack of risk awareness which comes along with the lack of knowledge about privacy issues and skills to protect oneself, self-efficacy, and lastly, privacy cynicism. These will be discussed in the next chapter.

2.5.1 Importance of SNS

Using social media turned into a daily routine. Many people check their profiles, their feed and messages regularly. It became a tool for entertainment, diversion and communication. Moreover, SNS serve the needs of the people. They help to connect to friends and build relationships. On SNS you can benefit from the social capital of various people you can be connected to. For example, you could get support, help or ideas from your online friends when you disclose certain information about yourself to which they can react (Ellison et al., 2011).

Moreover, it plays an important part especially in the life of a teenager because SNS can influence the construction of the identity (Debatin et al., 2009). By seeing the posts of others and, moreover, getting feedback on their own posts, especially young users go through a process of self-clarification and validation, as well as social control and representation (Lee et al., 2013). In this learning process, the teenagers reflect on who they want to become and how others see them. Presenting themselves online, therefore, is a mean of expressing their ideas and values. In return, they are waiting for feedback to validate themselves and their personality (Erikson, 1968). Therefore, the negotiating process of looking at others and being looked at is not anymore only taking place in real life like in schools or sport clubs. It is extended to the online world because “by looking at others’ profiles, teens get a sense of what types of presentations are socially appropriate” (Boyd, 2007, p. 10).

SNS is not only a place to communicate but also for social negotiation processes. To miss out on social media means missing out on all the social processes which are happening in the online world. Not being part of social media comes along with social isolation and exclusion (West, 2019; Zuboff, 2019). Lutz et al. (2020) even states that “individuals can no longer meaningfully participate in society without paying with their personal data as a kind of entrance fee” (p. 1169). SNS became engrained

in the lives of especially teenagers nowadays (Blank, Bolsover & Dubois, 2014). “Cyber abstinence” (Adorjan & Ricciardelli, 2019, p. 10) is, therefore, mostly not an option for teenagers.

Furthermore, a certain level of self-disclosure is needed to contribute to the community, just like the other users do as well (Ellison et al., 2007). Therefore, “active participation in the networked world requires disclosure of information simply to be a part of it” (Palen & Dourish, 2003, p.4). This brings us to a big challenge for users’ agency. The study from Tufekci (2008) shows that, the participants of her research feel that a certain level of self-presentation and disclosure is required when having a profile on a SNS.

Disclosing personal information can be needed to create social connections on SNS (Boyd, 2007). SNS can act like socialization venues, which make it difficult, especially for teenagers who try to develop their identity, to give up on actively participating on such platforms (Blank, Bolsover, & Dubois, 2014). SNS can be seen as social collectives which hold their member together by internalizing emotional ties and implicit rules. Especially the emotional attraction and rewards towards and from SNS are more attractive and important to its users than the risks like data misuse (Lutz & Strathoff, 2014). This is why participating on SNS which often comes along with disclosing information which is more important to the young users than protecting themselves and their privacy online. However, it is not necessarily the wish of people to hide all information about themselves. There is in instead, according to Altman’s (1975) privacy model, an optimal degree of how much one person reveals about oneself and in addition how much input one wants from others.

2.5.2 Privacy calculus

Similar to the ideas of the first paragraph, the privacy calculus has emerged to be the most prominent model to explain the privacy paradox (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). It postulates that users expect certain benefits which outweigh the perceived risks. Users perform, therefore, a calculus between the potential gain and benefits and the expected losses. The user decides according to the resulting outcome of the privacy trade-off (Dinev & Hart, 2006).

A study found as an explanation for the privacy paradox that "as teenagers perceived more benefits from information disclosure, they were more willing to provide information" (Youn, 2005, p. 86). Therefore, the perceived benefits such as entertainment, communication, information, and socializing are traded in return for providing information (Youn, 2005). The satisfaction users get from self-presentation and maintaining friendships outweighs the risks when personal information is disclosed (Kokolakis, 2017). This is in particular applicable to the institutional privacy threats (Raynes-Goldie, 2010; Young & Quan-Haase, 2013).

Especially when a SNS platform is seen as socially relevant, users are more likely to disclose personal information – even when they are concerned about their privacy (Taddicken, 2014). Interestingly, the idea of the privacy calculus also applies to users who have already experienced privacy invasion (Debatin et al., 2009). Also, according to Petronio's Communication Privacy Management theory privacy is seen as a dynamic process where users negotiate the privacy rules to control their boundaries. This means that the expected benefits when a user discloses information like the satisfaction of socialization and self-expression, have a considerable influence on how people are managing their privacy (Petronio, 2002).

However, critics say that the privacy calculus assumes that there are rational users who base their decision on economic choices with full agency, which is often not realistic (Kokolakis, 2017). Instead, research shows that the decision-making process is influenced by incomplete information, bounded rationality and psychological biases, such as confirmation bias, hyperbolic discounting and others (Acquisti & Grossklags, 2007). So leads the affect heuristic for example to a quick decision that is based only on impressions. In this case, people often on the one hand overestimate the risks when it comes to things they do not like and, on the other hand, underestimate the risks when the decision is about things they like (Slovic et al., 2002). This applies for disclosing personal information when for example the interface of SNS suggests getting positive resonance (Kehr et al., 2015). Moreover, the problem is that people tend to value immediate gratification higher than future ones, and, therefore, prefer to receive the benefits of information disclosure which outweighs the long-term risk of data misuse (Acquisti, 2004).

2.5.3 Lack of risk awareness

The lack of risk awareness has been identified as an additional reason why users do not show protective behaviour which can be connected to the lack of privacy literacy and internet skills (Bartsch & Dienlin, 2016; Dienlin & Trepte, 2015). Since users sometimes do not understand the risks which come along when their information is disclosed, they accordingly do not show any protective behaviour (Hargittai & Marwick, 2016). Acquisti & Gross (2006) and Tufekci (2008) discovered as well that one of the reasons why young people disclose information, is that they do not understand which risks and dangers might come along with the disclosure. The lack of knowledge about privacy risks and one's rights influences how people protect themselves online. The less they know about privacy and related topics, the less they are engaged in their privacy management (Debatin et al., 2009; Park, 2013).

In the study from Youn (2009), she also proposed the explanation that young users might misjudge their online safety because they assume that they are in control of their data and, therefore, do not change their online behaviour. She raises the question whether young adolescents are already capable of fully understanding the privacy risk, since their scientific understanding of the Internet use is not fully developed and "their perception of privacy self-efficacy could be optimistically biased" (Youn, 2009, p.20). In addition, Dienlin & Trepte (2015) argue that users lack first-hand experiences of privacy invasions and other negative consequences. This is why they underestimate the privacy risks and do not take preventive measures.

On the other hand, the more users know about data collection and risks, Boyd & Hargittai (2010) found an increase in the privacy management of users on the example of Facebook. This applies to adult consumers. When they are aware and conscious of threats like scams or identity theft, they feel more vulnerable and, therefore, are also more concerned about their privacy (LaRose & Rifon, 2007; Dinev & Hart, 2004). Therefore, it seems to be a crucial point since it proves that the more people are aware and know about the risks, the more they show protective behaviour and, therefore, neglect the privacy paradox. Studies prove that the level of privacy concerns is a strong predictor which leads its users to protect themselves for example to fabricate personal information, to adopt privacy-enhancing technologies, or also to stop interacting with certain websites (Lwin et al., 2007).

In addition, Hargittai & Marwick (2016) have identified, besides the lack of understanding of the risks, that users lack skills to protect their privacy and act as an explanation of the privacy paradox. Even if the users express privacy concerns, they do not know how to protect themselves online and, therefore, do not do it. In contrary, the people who have good skills are more likely to for example change their privacy settings (Boyd & Hargittai, 2010). This applies especially to the younger generation (Blank et al., 2014). Even if these skills are important, internet skills vary among people (Hargittai & Litt, 2013; Litt, 2013; Park, 2013). Moreover, since some of the SNS change their privacy settings frequently, it makes it difficult for the users to manage one privacy settings (Boyd & Hargittai, 2010; Stutzman et al., 2013).

2.5.4 Self-efficacy

Self-efficacy is another crucial factor for understanding why users apply or do not apply any protective measures. Rogers (1975) has identified three factors which have been adapted by another three factors from Maddux and Rogers (1983). In the end, they found six factors which influence the motivation to show protective behaviour: 1) if the perceived risk is likely to occur 2) if the risk is perceived as severe 3) if the protective behaviour is seen as effective 4) self-efficacy 5) the costs of the protective behaviour 6) and the expected benefits of it. Youn (2009) who took these factors as the base of her survey of adolescent consumers in connection with the privacy paradox sums up that "the vulnerability to the risk, the severity of the risk, response efficacy, and self-efficacy" (p. 393) are the crucial factors to show protective behaviour.

Self-efficacy is relevant because it helps that users are more motivated to protect themselves, if they perceive that their behaviour is effective (Floyd et al., 2000, LaRose & Rifon, 2007; Yao & Linz, 2008). Rifon et al. (2005) for example prove that users with more self-efficacy provide less personal information online. Youn (2009) concludes that "consumers who are more confident in their privacy protection would be better able to understand the negative consequences associated with privacy invasion, thus leading to greater concerns for privacy" (p. 398). However, self-efficacy can be misperceived as "optimism bias, overconfidence, affect bias, fuzzy boundary and benefit heuristics, and hyperbolic discounting" (Kokolakis, 2017, p.129). Cho et al. (2010) for example found that the optimism bias, which means that individuals assume that they are less likely at risk of being affected by the negative effects, is related to the privacy protective behaviour.

2.5.4 Privacy Cynicism

Privacy cynicism can be another explanation of the privacy paradox since it describes how the attitude of users influences which protective behaviour they show. Privacy cynicism can be understood as the feeling of powerlessness, uncertainty or mistrust against media institutions which leads people to think that protecting their privacy is useless (Hoffmann et al., 2016). Users feel like they lose control over their personal data which emerges in the feeling of powerlessness, as the study of Lutz et al. (2020) showed. Draper & Turow (2019) explain it as a feeling of digital resignation. Especially when users are facing institutional privacy threats, other researchers address this idea and these feelings as privacy apathy (Hargittai & Marwick, 2016), or surveillance realism (Dencik & Cable, 2017). Moreover, Choi et al. (2018) use the term privacy fatigue in the context of psychological literature by which he means "the sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet" (p. 42).

Lutz et al. (2020) argue that privacy cynicism acts as a coping mechanism especially against institutional threats. This coping mechanism helps "disempowered users to participate in online platforms without cognitive dissonance since they rationalize privacy protection as useless" (p. 1174). Therefore, Choi et al. (2018) point out that this is a negative coping mechanism which leads to disengaged users who stop protecting their personal data.

A big challenge for the users online is to understand the online world which is getting more and more complex. To take accordingly good decisions about their privacy, is, therefore, difficult for many users (Hoffmann et al., 2016; Choi et al., 2018; Dencik & Cable, 2017; Hargittai & Marwick, 2016). One reason for the complexity of the online world is the networked privacy (Marwick & Boyd, 2014). "Privacy is not an individual process, but rather a collective effort that requires the cooperation of those with whom we connect on social media, as well as the technological affordances of the social media sites themselves" (Hargittai & Marwick, 2016, p. 3752). This is why for example to control the spread of the disclosed data becomes more and more difficult, the bigger the network on SNS is. Because of this, both technological and social violations of privacy can occur (Marwick & Boyd, 2014). Especially when the users try to protect themselves, but still suffer from privacy violations, it can lead to the feeling of resignation and users stop protecting themselves in the future (Hargittai & Marwick, 2016).

However, it needs to be stated that the feeling of resignation can vary. Privacy needs to be understood as contextual (Nissenbaum, 2004) and situational (Masur, 2018). Users are exposed to many different risks, both vertical threats, which are mainly institution-based and horizontal threats which are peer-generated (Sujon, 2018; Young & Quan-Haase, 2013). Users can perceive those differently, give them different values and perceive their protective behaviour as less or more effective depending on the threat. Therefore, users "may not perceive the same level of resignation in all settings and situations" (Lutz et al., 2020, p. 1182-1183), yet in a "digital domain, vertical and horizontal pressures interact: mistrust toward a platform may impede social interactions, and conversely, social concerns may lead to adjustments in platform use" (Lutz et al., 2020, p. 1183).

3. Methodology

Based on the presented theoretical and empirical explanations, the goal of this study is to understand how young users perceive their privacy online and followingly how the privacy paradox can be applied to the usage of teenagers on TikTok. To answer these questions, and to get more insights on the usage and protective behaviour on TikTok, I conducted three focus groups in Luxembourg with teenagers aged 12 to 18 years. In the following paragraphs, I will present the four research questions and give more information about the application TikTok which was the object of this study. In addition, I will explain how the focus groups were planned and implemented, how the data was analysed, and lastly which ethical concerns were considered.

3.1 Research questions

The privacy paradox is a wide-ranging phenomenon which tries to explain different online behaviours. In this study, I want to use this theory as a starting point to understand the behaviour of teenagers on the platform TikTok. Looking at the download numbers of TikTok and the frequency of usage (Ceci, 2022), it becomes evident that TikTok as an SNS platform has become a part of the lives of numerous users. But considering how difficult it is to manage one's privacy in general and especially in the online world of TikTok, where your data is exposed to various risks, the question arises why there are so many users downloading and using this application nevertheless. In this study, I want to use this theory as a starting point to understand the behaviour of teenagers on the platform TikTok. The goal of this research is to look into the theory of the privacy paradox and the various attempts for explanations of this phenomenon and see how this can explain how the usage of teenagers on TikTok. I want to know if the teenagers show paradoxical behaviour when downloading and using the application and if yes, what are their reasons for it. To answer these questions, I developed four research questions which are based on the presented theory in the previous chapters:

RQ1: How do the participants perceive their privacy on TikTok?

RQ2: How do the participants protect their privacy on TikTok?

RQ3: How do the participants perceive the risks on TikTok?

RQ4: How does the privacy paradox apply to young users of TikTok?

Firstly, after comparing various definitions of the concept of privacy, it matters in this context how the interviewees perceive their privacy online. I want to understand which information is important and considered to be private. Subsequently, it is of interest how they protect it and which strategies they use to manage their private information. In addition, I want to examine which risks they are aware of and how they perceive them to be relevant to them. As the research on the privacy paradox shows there are different factors influencing the privacy management like the importance of being part of SNS, the calculus between gratification and threats, the risk awareness, self-efficacy, as well as the attitude toward privacy and the protection against privacy breaches (see chapter 2.5). I want to understand which of these factors are relevant when explaining the online behaviour and, therefore, be able to answer how the privacy paradox applies to young users of TikTok. In the following paragraph, I will explain which approach has been used to collect data and how it was analysed.

3.2 Object of study

TikTok has gained over the last years more and more attention and billion users all over the world (TikTok, 2021a). Compared to other audio-visual media platforms, TikTok convinces with its fast-moving and fresh contents which especially attracts young users (Leander & Burriss, 2020). You can use TikTok passively as a consumer and swipe through your “For me”-page where you find videos of people you follow. Additionally, there is the endless “For you”-page which shows you random videos that fit your interest. The algorithm behind this is what makes the platform special. It tracks which kind of contents you are engaging with or producing yourself, and accordingly shows you similar videos on your feed. This user-centred contents help to avoid boredom and instead increase the engagement rate and time spent on TikTok of each user (Smith, 2021).

On TikTok, there is also a video making tool with several effects and editing options to produce contents on your own. As these tools are easy to use, practically anyone interested can become a content producer on this platform. The simplicity of using the app and the easy entry, makes TikTok appealing especially to many young users (Weimann & Masri, 2020). Furthermore, the speciality of TikTok is that due to its algorithm, creativity is encouraged and the access to popularity is more reachable, as it is easier that videos go viral and can, therefore, be seen by various users of the platform (Leander & Burriss, 2020). Thanks to these features TikTok has become the fastest growing social media platform in the world (Weimann & Masri, 2020).

To generate a personalized experience, ByteDance, the company that owns TikTok, collects numerous data. This challenges the privacy management of its users. As privacy and privacy issues are the focus of this thesis, I am going to have a closer look at the privacy policies of TikTok and link them to the previous chapters. ByteDance (TikTok, 2020a) is explaining on its website how they are collecting data when using their services via the website and via the application. Depending on your residence there are different privacy rules. The one presented here concerns people living in the European Economic Area (EEA) or the United Kingdom, or Switzerland. The following rules refer to the time when the focus groups were conducted (February and March 2021). In the meantime, TikTok changed the privacy rules in October 2021. In the changes they adapted the layout of the website to make it easier for the users to read and find the information, according to Fox, Head of Privacy on TikTok (2021). Furthermore, they increase the transparency by adding details about which data is collected, used and shared as well as more detail about user privacy rights (Fox, 2021). In the United States they changed the settings indicating that the application is allowed to store biometric data (TikTok, 2022b). This, however, is not the case for the EU, as the data protection regulations are stronger here. Yet, ByteDance collects non-biometric data to identify objects in videos or records the audio text (TikTok, 2022b). In the following paragraphs, I will discuss the privacy policies as they were presented in spring 2021 for the EEA and explain how I implemented this in the focus groups.

3.2.1 Types of personal data collected on TikTok

In general, every interaction on the platform TikTok is surveyed. They process the content you upload, but also you watch including the preferences and settings, as well as any interactions with other videos such as comments or likes. In addition, they save how you engage with the platform and how often you use it. Moreover, they collect information about the profile which means when a user registers to the platform, the username, date of birth, email address and/or telephone number and the information one writes in the profile including the profile picture/video (TikTok, 2020a).

Regarding the technical information, ByteDance collects the IP address of the users and information about the device which accesses their platform. Moreover, the location from where one accesses the application is collected in order to provide the user with matching content. In addition, while creating

your profile there is the possibility to sign in with the account from Facebook, Instagram, Google, Twitter or Apple. If the user does so, ByteDance is allowed to share and collect information with and from them. Furthermore, there are also information from third parties, information about the friends, in-app purchases, information through surveys, and information through cookies which are collected about the users (TikTok, 2020a).

The stored information is kept for 'as long as it is necessary' to provide users with adequate service. If the users decide to delete the account, the profile will be first deactivated for 30 days and then the data will be deleted. ByteDance tries to keep the personal data safe by encrypting the data. However, they admit that no transmission via the internet is completely secure (TikTok, 2020a).

When considering where and how TikTok is collecting data, organizational privacy threats are at risk (see chapter 2.3.4). Looking at the various types of personal data, which is collected on TikTok, it becomes evident that there is a lot of information stored about the users. Every action, every klick, every post made on TikTok is saved. Therefore, the amount of data which is stored and used is relatively high. The comprehensive data collection challenges the privacy management of the users as explained in the previous chapters. It is difficult for the users to have an overview of which information is collected about them. In the focus groups, therefore, I want to understand if the young users are aware of the amount and type of data collected about them and how they perceive this to challenge their privacy.

3.2.2 How ByteDance uses personal data

ByteDance uses personal information to create a "personalized" experience for its users which means that the content is adapted to the collected interests of the user and presented in a way which is suitable for the device on which TikTok is used. TikTok is promoting different topics and uses the collected data to optimize and measure advertising. All companies which put their advertisements on TikTok can access analytics tools to measure the effectiveness of their strategies. Moreover, TikTok uses the data to communicate changes and provide support, as well as it is using the data and other surveys as feedback to improve and develop their platform. Furthermore, the data is used to make sure that the terms and conditions are followed, and that the safety of the users is guaranteed (TikTok, 2020a).

By highlighting the benefits of data collection, TikTok points out the advantages for its users to have a better experience online thanks to data collection. This refers to the 'strong user model' (Zheleva et al., 2013). Therefore, to create a memorable online experience, the application catches its users with content specialized for the individual. However, I want to understand in the focus groups, how the teenagers perceive their privacy to be treated on TikTok. The questions, therefore, rise if they only see the advantages as they are presented by ByteDance or if they are aware of the risks which come along.

3.2.4 Users' rights

Whenever users want, they can access, delete, change or correct the personal information and object or restrict that ByteDance uses their data by withdrawing the consent every user has to give in the beginning. If there are changes within the privacy policy, the users are informed (TikTok, 2020a). Not only that the users have the chance to be informed about the privacy policies on TikTok, but the users are also encouraged to take action to protect their privacy. TikTok tells its users to go to the privacy settings to reduce the risks for them online. They for example suggest that users can decide whether they want to see personalized advertisements or if they want to deactivate this function (TikTok, 2020a).

TikTok warns not only about data collection from third companies but also informs its users about possible privacy violations caused by other users. They warn that anyone on the platform can access information when it is posted publicly. In this context, they refer again to the privacy settings and highlight the option to have a public or private profile on TikTok which helps to regulate who can see the contents (TikTok, 2020a). This becomes especially helpful when taking the TikTok algorithm into account. On the "For-you" Page you can see any publicly posted videos, even of accounts you do not follow. Even if these videos are based on the individual interest of the user, as explained before, any publicly posted video can potentially reach a huge number of various viewers (TikTok, 2020b). Therefore, if you post something on your public profile, you cannot control who will see this video. This is why the invisible audience and the context collapse (Machackova et al., 2015) as explained earlier is a challenge especially for the users of the application TikTok.

TikTok states in the Terms of Service that "[t]he Services and the Platform are only for people 13 years old and over" (TikTok, 2019, n.p.). To protect the young users who are under 18 years old, there are pre-settings on the accounts to reduce the risk of making negative experiences online. For young users from 13-15 years, the profile is automatically set to private. In addition, the option "Suggest your account to others" is by default off. They also cannot receive direct messages, or host live streams and the option to download a video is removed. For users between 16 and 17 years the default settings are a bit less strict, however, it is still not possible for them to interact with everybody on the platform. So are certain functions for example "Duet and Stich" are set to "Friends". Moreover, to buy, send or receive a virtual gift is limited to users over 18 years old. TikTok also improved the "Family Pairing" which makes it possible for adults to change and fix settings for their children (Han, 2021).

To sum it up, TikTok informs its users, gives suggestions on how to improve one's privacy management and offers special protection for young users. They highlight especially the option to regulate one's safety by adjusting the privacy settings. This is supporting the idea of the Communication Privacy Management theory that privacy rules need to be controlled and negotiated (Petronio, 2002). Yet, this can only work if the young users are aware of these possibilities and if they consider them to be helpful. To understand if the young users make use of these tools to protect themselves and what they think about the measurements taken by ByteDance, it was part of the questions in the focus groups. This will help to find out how young users are approaching privacy on TikTok and how they protect themselves.

3.2 Method

The overall approach for this study is phenomenological. The term 'phenomenology' derives from the Greek words 'phenomenon' and 'logos'. 'Logos' means 'the science of', therefore, phenomenology means 'the science of phenomena' (Heidegger 1962, p. 50). Husserl (1983), the acknowledged founder of this approach, suggested that phenomenology is a philosophic approach which tries to examine the meaning of unconscious experiences by trying to transform them into something explicit. Husserl assumed that people live naturally and act sometimes subconsciously (Todres & Holloway 2004). By using the phenomenological approach, you try to understand the goals of the act and the nature of the intention behind the actions (Smith et al., 2009). This means that the researcher attempts to understand the thoughts behind our everyday knowledge and actions and asks for the perceptions of

certain subgroups (Lindgren & Kehoe, 1981). This is why I decided to use the phenomenological approach for my research. The goal for me is to understand and give meaning to the thoughts and actions of the interviewees by reflecting on their intentions. Therefore, I want to investigate the potentially unconscious reasons and thoughts why and how teenagers use the platform and especially how young users perceive and protect their privacy on TikTok.

To reach this goal and to understand the reasons for the behaviour of the teenagers, I chose to conduct focus groups. A focus group is "a carefully planned discussion designed to obtain perceptions on a defined area of interest in a permissive, non-threatening environment" (Krueger, 1994, p.6). Focus groups can be put in place between participant observation and in-depth interviews (Morgan, 1997). There three main components of focus groups are: 1) the method for data collection; 2) the interaction between the participants as the base for the analysed data; 3) the active role of the researcher during the group discussions (Morgan, 1996). Moreover, this qualitative research methodology is especially effective when investigating a shared phenomenon that several individuals have experienced (Creswell, 2009, Creswell, 2013).

The reason I chose this methodology for this study is to collect the different opinions and motives of the participants on how they protect their privacy. Especially getting to know more background information about the various actions and thoughts the teenagers have concerning the application TikTok was of great interest in the study. Focus groups seem to be a suitable approach, as the interviewers can benefit from the discussion between the participants and can learn insights about the individuals (Morgan, 1997). "They are set up in order to explore specific topics, and individuals' views and experiences, through group interaction" (Litosseliti, 2003, p. 1). Group dynamics are the distinct feature of focus groups through which valuable data can be extracted. The social interactions between the interviewees offer deeper and richer data, compared to a single interview (Thomas et al., 1995). This is why it is important to make the participants comfortable sharing their thoughts and feel that their points of view are valuated (Byers & Wilcox, 1988). Followingly, the responses from the participants can be candid and reflective (Hillebrandt, 1979).

The benefits of focus groups are that they can "provide information about a range of ideas and feelings that individuals have about certain issues, as well as [they are] illuminating the differences in perspective between groups of individuals" (Rabiee, 2004, p. 656). Similar to other qualitative

approaches the strengths of focus groups are: "(1) exploration and discovery, (2) context and depth, and (3) interpretation" (Morgan, 1997, p. 12). Also, Bauman and Adair (1992) suggest that focus groups help to understand various types of data: responses to different stimuli and issues; details about reactions and answers to specific topics; a rich understanding of cognitive and affective processes; and personal context and background information which influences the responses of the interviewees.

When trying to understand trends and issues in the field of education and psychology where research wants to gain insights into the people, it is especially valuable when the interviewer is in direct contact with the individuals (Vaughn et al., 1996). The relationship between the interviewer and the participants in focus groups can be seen as a "dyadic and even clinical relationship" (Kamberelis & Dimitriadis, 2013, p. 7). In general, the role of the interviewer is rather complex. Not only the preparation for the discussion is essential, but also during the interview, the interviewer has an important role. S/he needs to listen actively to the participants and needs to channel the conversation between the interviewees. However, s/he has also the opportunity to add more depth to the conversation or influence it by adding more dimensions to the discussion (Vaughn et al., 1996).

3.3 Sample

I conducted three focus groups which were held in Luxembourg. The first group was in a children's home in the north of the country. The second one was a youth house in the southeast of Luxembourg and the last one was a youth house in the southwest of the country. It was important to have the focus groups in different parts of the country as the social context differs among the chosen areas.

In total there were 15 participants aged between 12 and 18 years. In the children's home there were four participants - two girls and two boys aged 12 to 14 years. In the Youth house in the southeast there were as well four participants with one girl and three boys aged 13 to 18 years. Lastly, the youth house in the southwest was the biggest group with seven participants; among them were two girls and five boys between 13 and 16 years. The first two focus groups were rather small. Yet, the recommendations for the number of participants vary among different researchers. MacIntosh (1993) says between six to ten participants; Goss & Leinbach (1996) did studies with up to fifteen people; or Kitzinger (1995) only up to four participants. The bigger the groups, the more discussion there was,

however, I could go more into deep for each topic when there have been only four participants. Therefore, the mix of the group sizes helps to cover both strengths of focus groups.

I chose to conduct the focus group in youth centres and children's homes because it should be a group where the participants get along and feel at ease to share their opinions. Moreover, they should feel respected and understood when talking about their experiences (Morgan, 1997). Krueger (1994) suggests using homogenous groups which are similar for example by their gender, age and social background. In focus groups it is recommended to find "members based on predetermined characteristics" (Vaughn, 1996, p. 58). This is called purposive sampling and means that participants are selected based on a specific criterion to which all the participants can relate to (Vaughn, 1996). Therefore, all participants should have similar socio-characteristics and have something to say concerning the chosen topic (Richardson & Rabiee, 2001). When contacting the organization, it was explained that for this survey we need teenagers who use TikTok. However, in the end there has been in each of the focus groups one person who did not use TikTok. This person could barely participate in the conversation, yet the interviewer tried to make references to the platforms s/he used.

However, there are also com critics concerning the sampling of focus groups. Vaughn (1996) says for example that this way of selecting participants makes the generalizability difficult (Vaughn, 1996). Moreover, there are also critics which suggest to better have a heterogenic group. In groups in which the participants do not know each other before, they may be more honest and show more spontaneous behaviour. When the participants know each other the responses and behaviours are mostly based on their pre-existing relationships and group dynamics (Thomas et al., 1995). Yet, in heterogeneous groups there is trust missing especially when it comes to sensitive topics (Kitzinger, 1994). In general, the idea behind the focus group is that there is a discussion, so the participants do not need to have the same point of view, instead, there should be a group dynamic so different arguments and opinions are produced (Kitzinger, 1994). Nevertheless, for this study I decided to use homogenous groups. Like this, I expected that they feel more comfortable sharing personal experiences and opinions.

3.4 Planning

The initial process of contacting various organisations was led by a colleague who works for a safer internet centre in Luxembourg called BEE SECURE. Through this institution it was easier to get an appointment since it is a trusted organisation in Luxembourg. The results of this survey are also used in the frame of the "Youth Panels" for BEE SECURE which are shared among other safer internet centres in Europe. Therefore, in my role as the interviewer, I also represented BEE SECURE which was helpful since most of the participants were familiar with this institution and, therefore, felt at ease sharing opinions and experiences.

Moreover, to make the teenagers feel comfortable all the focus groups were held in the places of the different organizations which is usually what is recommended (Gibbs, 1997). The focus groups were planned during the regular opening hours of the youth houses and children's homes and lasted one hour for the two smaller groups and one hour and thirty minutes in the youth house with seven participants. As the discussions were recorded with an audio recorder, the teenagers had to hand in a consent form with the signature of their caretaker.

Additionally, in the preparation phase I got familiar with the application TikTok myself. It is important in focus groups that the researcher has some initial knowledge and tries to understand the topic more in-depth and understand the implicit motives or clarify conflicting points from previous studies (Vaughn et al., 1996). Calder (1997) points out that "the value of phenomenological focus groups is in the experiencing of consumers. What they should yield is the experiencing of the experience of consumers" (p. 360). This is why it is important, according to Husserl (1983) that researchers need to be aware of their prejudices and stay open during the process. Therefore, it was essential not to have a bias when talking to the teenagers. It was important to keep in mind that each experience with the application can be different and all their answers are valuable. Moreover, since the focus group was organized together with the safer internet centre in Luxembourg, there was a risk that the interviewees might not tell their own experiences but say what is supposedly a correct and safe online behaviour. Usually a training from a safer internet centre, like BEE SECURE talks mainly about the dangers of the internet and reasons they should be careful what to do online, it was essential in the beginning to say that all opinions are valued and that the interviewer is open to hear about the positive and negative aspects about TikTok equally.

3.5 Implementation

The interview started with an introduction which was followed by questions concerning their usage of TikTok. They were for example asked if they also produce contents or if they are mainly consumers of the contents from others. Since the strength of focus groups is the flow of the communication, the focus was to create a discussion by stimulating the controversy by doing an exercise called “bad cop / good cop”. For this exercise, the teenagers were split into two groups. One group had the task to write down all the positive aspects they could think of about TikTok. The other group should note all the negative aspects. After collecting the aspects in the groups, they should present their arguments in front of the others, which was followed by a general discussion of the two aspects. However, not in all the focus groups it could be done like this, as there were not enough participants to engage them in an activity like this. This is why in the two smaller groups the collection of positive and negative arguments was done in the whole group.

After collecting the arguments of the teenagers, together in the group we tried to extend the list especially of the potential risks. The goal was to get more background information on their behaviour, thoughts and knowledge. Therefore, choosing focus groups as a method gave the freedom to explore many insights into the participants’ behaviours. The arguments the teenagers found for and against TikTok and especially the discussions afterwards helped to get to know the points of view and experiences of the participants and I could, therefore, learn by listening to the teenagers.

Later on, the conversation was led towards the topic “data collection”. At this point the goal was to understand how much the teenagers know about this topic, get an insight into their opinions, and lastly get to know how they protect themselves against it. Therefore, the teenagers were asked to go on the privacy settings on TikTok. We went through the different settings and clarified their meaning. This was followed by a discussion if they think that TikTok is doing enough to protect their privacy or not. To end the interview, we took a look at the future and the teenagers could state how they would like TikTok to change to be a safer and better place.

3.3 Analysis

The base of analysis were the transcripts of the recorded audio. For the two smaller groups in which the focus group lasted one hour, both of the transcripts were 14 pages and the third focus group with a duration of one hour and thirty minutes was 23 pages long. I coded and grouped the data sets manually. As the focus groups were done in German and Luxemburgish, the text was translated into English for the quotes in the thesis.

In this study, the 'thematic analysis' was used. This analysis is often recommended since it helps to understand both implicit and explicit meanings and ideas as it goes beyond for example counting phrases in a data set (Namey et al., 2008). It is, therefore, applied when the research seeks to understand and interpret the data, because it allows to compare and relate the concepts with the gathered data (Alhojailan, 2012). It can be described as "a method for systematically identifying, organizing, and offering insight into patterns of meaning (themes) across a data set" (Braun & Clarke, 2012, p. 57). Braun & Clarke (2012) who are often associated with this analysis explain further that by looking at similarities across different data sets, the researcher can generate meanings shared among different groups and experiences. It helps to identify what there is in common and, therefore, extract the patterns which are the most relevant concerning the research questions. This approach is flexible and allows to apply a combination of an inductive or bottom-up approach, as well as the deductive or top-down approach. The first approach generates the codes according to what is in the data. The second approach, in contrary, starts by applying a concept or idea to interpret the data" (Braun & Clarke, 2012).

Krueger & Casey (2000) point out that the analysis should be on the one hand systematic, and sequential, and on the other hand verifiable, and continuous. To be able to group and code the data set, eight steps according to Braun & Clarke (2012) are needed. First, it is about the familiarization with the data set. Second, you generate the initial code by working through the data sets and writing codes which are descriptive and/or interpretative. Third, you search for themes which group some codes in relation to the research question which then need to be reviewed in the fourth step to make sure that it captures the most relevant elements of the dataset. Later on, the themes need to be defined and given a name. Lastly, there is the production of the report. This, however, can be done throughout the process. The report needs to tell a story which goes beyond describing the data. It

generates arguments to answer your research questions (Braun & Clarke, 2012). However, as the goal is to give meaning to the data, there is a certain extent of subjectivity needed (Rabiee, 2004). As I have done the focus groups and the interpretations alone, it was important to look through the transcripts often to see similarities and differences between the participants. Therefore, coding, mapping and interpreting the data was an important step while analysing the data.

The eight-step process described by Braun and Clarke (2012) was followed in this thesis. After transcribing the three audio recordings, the data was coded and categorized which resulted in the themes “privacy”, “usage”, “protection online”, and “risk awareness”. While working on the data, I could learn new insights and create links which were not foreseen in the first codes. Finally, I created new codes which I matched to the themes. For example, in the general use of TikTok I summarized how the participants consume TikTok, their reason for downloading and using the application and the positive aspects of TikTok. The next category was “risk awareness”. Here I focused on which threats the teenagers know of and are the most concerned about. As in the coding process it became clear that there is a significant distinction for the interviewed teenagers between social – and organizational threats, they were again divided by the risks addressed during the focus groups like cyberbullying and inappropriate content and on the other side hackers and data collection. The next category looked into the protective behaviour. Here the teenagers mentioned more measures to protect themselves than anticipated, which is why there are subcategories explaining how they adapt their privacy settings on TikTok, as well as other ways of protection which the teenagers mentioned. In connection to that, there is a reflection on how the teenagers want their online privacy to be better protected, what the teenagers criticized about TikTok and their ideas about improvements in their privacy policy. Lastly, to answer the fourth research question concerning the privacy paradox, I combined the results from the different themes mentioned earlier and compared them with the presented theoretical explanations in the second chapter of this thesis.

3.4 Ethical considerations

In focus groups the participants are encouraged to share information about themselves. However, this raises ethical concerns regarding their privacy. It needs to be considered who can have access to the identities of the participants (Vaugh, 1996). There are three key factors which need to be assured which are first of all consent, as well as confidentiality and anonymity (Sim & Waterfield, 2019).

Consent is important as the participants need to be able to make an autonomous decision whether they want to be part of the study or not (Beauchamp, 2009). There are four elements to ensure autonomy in the decision: disclosure, comprehension, competence, and voluntariness (Sim, 2010). This means that the interviewees need to have adequate information about the research and it needs to be assured that the participants understand the rules and goals of the study and are able to make a decision by having the freedom to decline at any moment (Sim, 2010).

Especially when conducting focus groups with teenagers, these ethical considerations need to be taken into account. It is important to explain to the teenagers that they can voluntarily give their consent in participating in this research. Therefore, it is crucial that the participants understand what is going to happen in the focus groups and what will happen with their data. It needs to be highlighted that they are not forced to participate but voluntarily can share their opinion with the interviewer (Vaughn, 1996). Therefore, before starting the interview and the recording, I explained the procedure to the teenagers and that the participation is voluntary. As most of the participants in the conducted focus group were underaged, I asked additionally for a signed consent from their caretaker which ensures that the collected information and data is treated anonymously. Only the teenagers who handed in the consent form, were recorded, and participated in the focus groups.

Confidentiality and anonymity are as important as giving consent. Confidentiality defines what is happening with the given information and to whom it will be disclosed. Anonymity describes if the person can be identified by the information given in the study (Sim & Waterfield, 2019). In the consent form which the parents or respectively the educators signed, it was also explained that the data will only be used for this thesis and for the report of BEE SECURE in which possibly identifying data is anonymized. To ensure their anonymity, I changed the names of the interviewees. The quotes in the next chapters of the teenagers only indicate the correct age. The names, however, are fictional. Therefore, there are no direct conclusions as to who the teenagers are possible.

4. Results

In the following paragraph I will present the results of the three focus groups, according to the analysis explained earlier: how teenagers perceive privacy, the usage of TikTok, the risk awareness and their protection online. Hereby I want to give an overview of the opinions and experiences of the teenagers. This will set the base for the discussion in the next chapter, where I will analyse the data and reflect on it.

4.1 Privacy

> "Privacy is when there are a few things you don't want to tell the public; they are only meant for you, and you should be the only one who sees them - not anyone else" (Tom, 16)

What the boy easily summarized, however, turns out to be difficult for some of the other teenagers. They have similar opinions on what should stay private and what not. Listening to their partially well thought through decisions on what to post, it becomes clear that this is a topic they are confronted with on a regular base. Privacy in general means for the interviewed teenagers to have their private space where they can be by themselves without any influence from neither the family nor other distractions. They like to follow their own interest and have their private moments. Svenja (14) for example explains: "Privacy means to put your phone away and enjoy the day. […] I want to do my sport and have my privacy without anything distracting me."

However, not only privacy in a more physical sense but also privacy online seems to be a topic the teenagers care about. Online privacy is for them mainly connected to limiting who can see their contents: "Privacy means you post things, only the people you know can access" (Jessica, 15). They like to share videos and information about themselves, but only with their friends not with the public. There are certain aspects about them like their relationship status which they do not want to be public. This is for example a topic they like to share with their friends and some also with their family but not online where anyone can access this information. They seem to know their boundaries and have an idea of what to tell whom: "You can only tell people you trust your private information" (Andreas, 16). They remembered seeing TikTok videos of couples talking about their relationship. Sophie (15) reacted to this: "not the whole world needs to know our private life". The teenagers also talked about a person who smokes, strips, drinks etc. in live videos on TikTok. Moritz (15) said followingly: "this is not

supposed to be shared with other people. That's stupid." The interviewees instead select very careful which information to disclose and which not:

> "I'm very careful to only tell certain things about myself. I don't care if others will know the information I show as there will be no consequences for me. I would not post a photo with a gun in my hand; but saying that I live in Luxembourg is fine for me" (Michael, 18).

Another boy (Tom, 16) says that he would be fine with sharing his creativity. However, he does not post it because he - as well as the other teenagers - is afraid of negative reactions to their videos: „I think that everyone is afraid that your video can be a failure and that you can embarrass yourself" (Tom, 16). In general, they barely produce any content on TikTok because they do not want to expose themselves to the risk of cyberbullying. Why the teenagers enjoy being on TikTok nevertheless, and how the teenagers use TikTok in general will be explained in the next paragraphs.

4.2 Usage of TikTok among the participants

All of the participants are familiar with the platform TikTok and yet have different ways of using it. 12 out of 15 participants use the application TikTok. There was one participant who recently deleted the application and the other two watch TikTok videos and compilations videos on YouTube. None of them use the web version of TikTok. They have been using the applications for many years already, mainly starting when they first got their smartphones.

8.2.1 General use of TikTok

All of the 12 participants are "huge fans of TikTok", as they called themselves. They enjoy watching funny videos, memes, and dance videos. Moreover, they like it "because it inspires your creativity" (Tom, 16), "it is interesting to see what other people do in their lives" (Bernd, 14) and because "there you find something for everyone" (Peter, 16), a boy adds. The interests of the participants vary and, therefore, also the videos they watch. All in all, they like funny videos, videos they can learn from, get news about famous people, lifestyles and trends, as well as videos they can get inspiration from regarding their hobbies, sports or fashion.

Most of the participants are passive users of the application TikTok. They mainly watch videos on their "For you - Page" and only sometimes consume the contents on the "For Me - Page". In general, they do not engage that much with the platform such as commenting or following except for a few more active participants. One girl for example follows more than 1300 people and comments especially under videos of her favourite TikTok Star hoping that he will react to the comment. Moreover, there was a girl (13) who posted a video with a friend which got 600 Likes: "We were so happy and then we got more and more followers, so that I reached 1000 Follower. That was great!" (Julia, 13). Others repost videos of famous people like comedians or influencers on their private profiles or posted privately slideshows of photos they took with friends and added background music.

Even if communicating and staying in touch with their peers plays a big role for them, none of them use TikTok for communication. Most of the participants are also on Snapchat, WhatsApp and/or Instagram which they mainly use for communicating with friends and family. They consider those apps to be their favourite apps instead of TikTok. "Usually, I do not spend so much time on TikTok. I mainly use Instagram and Snapchat, because I can chat there with my friends", as Robert (14) explains. The only way of communication they use on TikTok is that they send each other funny videos or tag them under the video in the comments. Some did not know about the possibility to send messages on the application.

They, instead, mainly use TikTok as a diversion. They like to spend some time on the application and watch videos, mostly "to distract myself from waiting […] because it seems like the time passes by faster when I watch TikTok videos" (Andreas, 16). Also, others like to "waste some time" (Franz, 15) with the application. According to the participants, they use TikTok in average for two to three hours a day. Some of the other participants themselves or their parents set a time limit to control the time they spent online.

All of them know the newest trending songs and dances on TikTok. When asking the participants about the newest trends, in each group they started imitating the dances or remembering the latest memes. Yet, besides a few exemptions, they barely produce contents on their own. Some participants produce videos, but only save them in their drafts, because "I am afraid that other people watch my videos like the people from my class. This is embarrassing" (Sophie, 15). Another boy does not do any videos because "I do not have anything to show or offer. Videos which should entertain people? I don't

manage to do that; this is why I don't post anything." (Michael, 18). Their friends, however, produce few videos.

8.2.2 Reasons for downloading and using TikTok

There were two main reasons which in some cases go hand in hand with why the participants downloaded TikTok. The first and main reason why they installed TikTok is that their friends downloaded TikTok as well: "All my friends have it and then I thought I do not want to be the only one who does not have it" (Svenja, 14). Therefore, she did not think about any possible risks of that platform. Being part of the social network - like all her friends - was more important to her. Also, the other participants of the other groups confirmed that: "I think it is also a kind of obligation, because if everyone has it then you want to belong to it, so you want to download TikTok as well" (Jessica, 15). Another boy highlights the peer pressure there is to have TikTok by making a comparison to the pressure some youngsters feel about smoking: "Why do I post a video on TikTok? Because I want others to see it. Why do you smoke cigarettes? Because others do the same. It's the same thing." (Andreas, 16)

The second reason why they are using TikTok is that most of them have already used musical.ly and then switched directly to TikTok, as all their peers did. Most of them made positive experiences with musical.ly which is why they liked it and they wanted to continue to be part of that experience. They highlight that they liked the dance and lip-sync videos and more importantly that they felt that the user experience was more positive and polite: "On musical.ly you still had a lot of fun. There was way less hate" (Julia, 13).

Nevertheless, three boys do not have TikTok installed. One boy (Mark, 16) who deleted TikTok is in general rather critical about new media and was concerned about how much time he spends online which is why, he decided to stop using the application. Also, the other teenagers agreed that TikTok is a "time-waster" because "you can easily forget how much time you spend there" (Bernd, 14), yet they are still using it. The reasons why the other two participants do not have TikTok installed, are that one (Max) of them is 12 years old, and, therefore, his parents do not allow him to download the application, as the age restriction is 13 years. The other boy (Daniel) prefers online games instead of spending time on social media.

8.2.3 Positive aspects of TikTok

The positive and negative aspects were collected by the participants and completed together with the moderator. Starting with the positive aspects, there are a few things which the participants in each of the groups had in common: entertainment, inspiration and creativity. They enjoy the easy entertainment they can get from this application, since the algorithm shows you random videos which fit very well their interest. This can be dance videos or funny videos like memes etc. In connection with this, they pointed out the different emotions you feel when you scroll through your feed:

"When you watch videos on TikTok, entertainment is the main point. You can watch some videos which make you cry. Then you can watch memes and you laugh again. This is why I like TikTok" (Peter, 16).

Another point is that they are getting inspired by the contents. For some teenagers this means reading interesting quotes about life and friendships, for others it means that they collect ideas about fashion, lifestyle, hobbies or cooking. This is also sometimes a way for them to be up to date to understand what happens in the world. Moreover, some of them appreciate that they can show their hobbies, even only among the chosen friends they accepted on their private profile.

Furthermore, they are looking for role models they can identify with. They are looking for confirmation and appreciate that there you find people with the same interest, worries and thoughts. Especially as they are teenagers this serves an important need and makes the application attractive for the youngsters as the content is so diverse and easily adapts to their own interests:

"You see many bodybuilders or sporty people in general. They do sport every day. They are my motivation" (Tom, 16)

„Sometimes I see videos in which they talk about something, which makes me realize that I think exactly the same way. Also, in the comments so many people say the same and share their opinions with each other. Then I tell myself, you are not the only one who feels that way. This makes me feel less lonely"(Jessica, 15).

4.3 Risk awareness

The participants were also asked to collect negative aspects of TikTok and note them. Even if these lists were shorter than the positive aspects, the risks influence their usage of TikTok significantly. They all mentioned cyberbullying and hate online. Moreover, all of them saw inappropriate contents, yet all define them slightly different which will be explained in the following paragraphs. Besides the social threats, the interviewees also mentioned identity theft and data collection as organisation threats. The two different types of threats will be explained further in the following chapters.

4.3.1 Social threats

Social threats are the main concerns for the teenagers. They see risks which are immediately affecting their social life or influencing their online experience. There is especially one concern which was the main topic in every interview: the hate online. According to the teenagers there are many unreflected users of the internet who either post inappropriate content and/or spread hate in videos and comments. Those two sides are going to be described in the next paragraphs.

8.3.1.1 Inappropriate content

Most of the participants did not encounter bad experiences on TikTok themselves except seeing inappropriate content. This is something they have all been in contact with. There are diverse contents that they claimed to be inappropriate: nudity, dangerous challenges, bodies/suicide, fake news, and unrealistic self-representation.

Especially when asking about the newest trends, they mentioned one of the first two categories of the list above. “What I mainly see on my For you-Page are woman/girls, who are half-naked. It just appears on my feed a lot!” (Franz, 15). However, the other groups did not mention nudity as a problem. They were mainly focusing on other challenges which encourage people to do dangerous things. The risk they were the most concerned about was that others - and especially younger children - will imitate those videos without thinking about it:

"There are also so many young children, who are like 10 years old. They could follow those bad examples" (Svenja, 14).

"People are so manipulative. When they see a video of people driving with 200 km/h on a highway, they start thinking about it. They see it as a motivation to do the same" (Mark, 16).

Moreover, two groups talked about suicide they saw on TikTok. "These videos are often just hidden between normal videos, and this obviously shocks you. Before you know it, you see a corps. The moment somebody reports it, somebody else already reposted it" (Peter, 16). When they see videos like this they immediately swipe to the next video. They said, moreover, that they have encountered those videos also on other platforms where other people sent it to them.

Furthermore, they identified lies and fakes on TikTok. Some teenagers already saw fake news on their feed for example concerning the elections in the States. The risk they see about fake news is that "sometimes the videos and messages are so unrealistic, yet sometimes they are very convincing, and you might share them" (Bernd, 14). Fake News, however, did not seem to be a relevant risk for the rest of the groups.

The lies on the internet they identified were mainly concerning the way people present themselves. They expressed the fear that people might get depressive "because they see the life of the famous people, see all the things they achieved, and the way they look like. These are all things you usually don't get" (Mark, 16). He continues: "you can also get easily jealous when you see a boy or a girl who is more beautiful than you. Then they get comments about how pretty they are. They get what they want, but you can get depressive because of that and start hating yourself" (Mark, 16). Therefore, self-representation on SNS has a bad connotation for the teenagers. They are aware that the way people present themselves online does not depict the reality. They fear that this unrealistic picture people show their audience can affect followers of such accounts negatively as it makes them question themselves and their bodies which can lead to psychological issues.

8.3.1.2 Cyberbullying

The fear of having a depression or feeling down does not only concern the effect of unrealistic self-presentation. The other participants mainly referred to the possible mean interactions with other users on the platform which can affect you negatively. They name mainly hate in comments and mean videos which they are afraid of.

The first reaction I received when asking them why they do not post any videos was “when you post something others do not like, you might receive hate comments or you could be bullied online and in school” (Svenja, 14). I could observe this constant fear and concerns in all three focus groups. The fear of being bullied and receiving negative feedback or comments, is constantly influencing their way of using the applications and influencing their decisions on what or if to post something:

“I don’t want to post anything, not because my educators tell me so, but I don’t want that anybody could say: ‘Iiiih, look that girl made such a video.” (Elisa, 14)

“People, who post videos which don’t meet the standards are being bullied, rejected and destroyed.” (Michael, 18)

None of them has ever experienced cyberbullying themselves, yet they either know someone personally who was affected by that or saw comments and reactions to other videos on their feed. This is why they blame in general the impact TikTok and other SNS have on our society and the way people behave online. Yet, because of the negative examples they see, they change their perspective and behaviour. They saw for example videos in which a woman with a handicap is bullied. “Many simply don’t understand that. Then they repost her videos and make fun of her” (Elisa, 14). This is why Elisa checks, whenever she gets a follower request, the profile. She does not accept people who share videos showing harassment and/or bullying and stops following those who start sharing this kind of content. In the other groups they also observed similar bullying because of someone’s handicap, sickness or body weight. Some of them even heard stories in which there was a person who killed themselves because of all the hate they received. This is why they are strictly against hate comments, and therefore also changed their usage: “I never put a negative comment. You always have to consider how the person might feel. If you don’t like what they are doing, well then don’t watch the video” (Andreas, 16).

Moreover, because of these experiences, they are very careful about what to reveal online: “If I post something, I am very careful about that; therefore, I adjust my posts in a way that they cannot cause any problems or prejudices” (Moritz, 15). They are also aware that when they post something online, they do not have control anymore over their own content. They know that the moment something is posted online, it is impossible to remove it completely from the internet. “Nobody can stop you for example from reposting my video“ (Mark, 16). Because of this uncertainty of the reactions of the users in the online world, the participants stopped posting videos on TikTok.

They are not only concerned about the consequences online, but they are also afraid of the being bullied in school and in general in their social life. This is especially relevant as Luxembourg is a rather small country where the chances are higher that you either know the person already, or you will see them around. “It can happen that one day I see someone on TikTok and the next day I see him in the city” (Bernd, 14). Moreover, they already received messages from strangers because they posted something. “So many people wanted to add me and also found me on other platforms like Snapchat. But how? This is crazy” (Julia, 13).

4.3.2 Organizational threats

Besides the dominant fear of social threats and especially of the hate online, they, in comparison, barely mentioned any organisational threats. As data collection is mainly related to online privacy, the conversation was led toward this topic. In the following chapters the opinions of the teenagers about hackers and data collection will be presented.

4.3.2.1 Hackers

When starting to talk about organisational threats, the teenagers mainly mentioned the fear of being hacked. They referred hereby to three different risks: phishing, virus and identify theft.

One boy (16) received a phishing message. He points out that: “You don’t expect something bad to happen when you receive a message from a friend. But then the misery starts when you are hacked“ (Andreas, 16). In addition, a girl talks about a fake SMS she received which contained a virus: “I was really scared, because I thought my parents take my phone away for one year when I tell them” (Svenja, 14). Moreover, another boy remembered that something similar happened to one of their educators and followed “it could easily happen to us as well that people hack into our account” (Max, 12). Max, moreover, fears that someone logs into your account and pretends to be you as this already happened to him - yet not on TikTok but on Microsoft Teams which they used for home schooling.

These fears are, therefore, still related to social threats as their main concern regarding this topic was that the “hackers” could post something embarrassing about them which leads again to their concerns mentioned in the chapter before. With this example, we see that they are constantly worried about being bullied, even for something they did not post voluntarily. This is also connected to the risk that

people can reuse or repost contents: “There might be contents, where you can see myself. They can be reused or photoshopped and shared, even without my knowledge” (Michael, 18).

4.3.2.2 Data Collection

As the focus of this thesis is privacy online, the risk of data collection plays a significant role. However, only in one group one participant was concerned about this. He said: “You know the quote ‘if you don’t buy the product, you are the product’ which means that all your data is being collected. I’m very sure that in a few years there is going to be a scandal about TikTok” (Mark, 16). The boy got the knowledge mainly from documentaries. He then makes the connection that “in the documentaries they were showing this on the example of Instagram, but I am sure that for TikTok it is the same. They want you to spend as much time possible on the application by using several tricks… and they manage” (Mark, 16).

When asking the other participants if they have ever thought about big data as a risk, they said no. The participants never thought about if or which data is collected of them. This is why I asked them follow-up questions and gave them more explanations about this topic. My approach was to make them reflect on how TikTok is earning money. Their guesses were that TikTok earns money via the downloads, likes or videos. Even if some then understood that advertisements are the main source of money, they did not make the connection that this platform is attractive for the companies because they are selling the data of its users. When the question was asked to whom they sell these data, they answered for example: “I don’t know, maybe TikTok is like a sub company and the “upper” company which bought TikTok can now access the computer and the data” (Elisa, 14). It was clear that they never thought about this topic before and lack knowledge.

Continuing the conversation and the questions with the different groups, I asked if they know which data is collected. In summary, they answered with age, gender, date of birth, phone number, contacts / friends, IP address, uploads, likes, channels you follow and search results. The list is relatively long, which means when giving them the input to think about this topic, they realize themselves which dimensions this can take on and understand how TikTok, and its algorithm works. However, they all said that they were not aware of this before and have never questioned this.

When asking the teenagers if they are worried now about this issue, they all said no. They also do not have the feeling that they are being surveyed, nor that they are at risk:

„It's not that it doesn't matter, but I'm not worried about it, because I think nobody who shouldn't have my data will not get it." (Bernd, 14)

„There is no harm for me. I don't have anything to hide. Plus, I think that this is also kind of my advantage. Now they only show me videos I like. This is why I don't question it too much" (Jessica, 15).

Only Mark (16) who was critical from the beginning and, therefore, deleted the applications summarized:

"Isn't it too good to be true?! If you think about how much you get from this platform and you don't have to pay anything? There has to be something odd about it. But many people don't think that far. But I know that, in retrospective when there is going to be a scandal, they will all realize that this was a scam" (Mark, 16).

4.4 Protection online

Looking at the methods they use to protect themselves, I will start with the privacy settings they choose to make their account safer against certain online risks. As the teenagers, however, do not use this as their primary measure to protect themselves, this will be followed by explaining their other preventive behaviours. Moreover, I collected their wishes on what TikTok or other factors could improve which would make them feel safer.

4.4.1 Setting

When asking the question in general if they know what they can do to reduce the amount of data which is collected about them, they could not give me any answer. They all said that they either have never checked their settings or it was a long time ago. Therefore, I asked them to open them on the application and check them together. Some of them found them very easily, some others, however, had troubles finding the setting.

Half of the participants still had the pre-settings from TikTok which they could not change. Therefore, they all had a private account. All the other settings which you find under security like “comments”, “mentions and tags”, “following list”, “duet”, “stitch”, “liked videos”, “direct messages” were set to “only me” or “followers”. Mainly they could not change the settings, because the option was blocked. The option to stop “Ads personalization” was also mainly not given. They could only download their data which they have never done.

Yet, the settings varied between the groups. One reason can be that the participants selected a different date of birth, as they mainly started using TikTok before they were 13. When asking, they admit that their age on TikTok is more than 18 years which means that they are not affected by the special pre-settings for young users explained earlier. Nevertheless, besides few exemptions they had a private account and also the rest of the settings were mainly set to the safest option.

After checking their settings, I asked about their opinions about them. The main feedback was that these settings do not change their opinion on whether they are safe on the platform or not: “I really don’t care, but I think it’s a good thing that they at least give this option. Like this people can adapt the settings who don’t want to be public and still have the chance to use TikTok” (Franz, 15).

They believe in general that their behaviour on the platform is what makes you feel safer on TikTok - not the settings. On the one hand, they highlight that the settings give you a certain frame in which they feel freer to post anything: “When you have a private profile, you can post anything you want. Only when you have a public profile, you should be very careful with what you post” (Julia, 13). Therefore, having a private account gives them some kind of security. On the other hand, they discussed that you can never be safe on the internet.

Another aspect which plays a significant role, is that they believe that their data is anyways already collected by Google and Facebook etc. Therefore, data collection is in their opinion nothing you can avoid or stop by adapting the settings. Even deleting TikTok does not seem to be an option they consider, because they think that this will not protect them anymore because „they have anyways access to my data, therefore, there is no big difference if I delete the application or not” (Sophie, 15).

4.4.2. Other protective behavior they use

The teenagers also mentioned other ideas they use to make their online experiences safer. They suggest to only post something on a private account and if something is public, to turn off the comments. However, it is best according to them to have as less interactions with the platform as possible which means that you should not follow people or write comments, as well as to reduce the time you spend on TikTok in general. Lastly, they suggest using a VPN or having an anti-virus program on the device to be also protected against hacker attacks.

Additionally, some thought about the option to delete TikTok to be safer online. However, as explained earlier they do not believe fully in those measures and the positive aspects of TikTok exceed the negative ones. They instead adapt their behaviour online in order not to offer any weak points to the potential haters. Therefore, they do not post any videos on their accounts. „Just because there are many negative things on TikTok, it doesn't mean that you have to delete the application, because it's still fun. You better be careful if you want to post or write something" (Robert, 14).

4.4.3 Wish for better protection

The participants were lastly asked what TikTok can improve so that the users feel safer online. One group mentioned that TikTok should stop storing all the data. Moreover, they request more security so that it gets more difficult for example to hack your profile. They ask for more encryption and authentication and to make the access to an account more difficult. One more suggestion was that they can verify the person and their age by sending a photo of your ID to TikTok. Yet, they do not feel comfortable giving this information to TikTok:

"If you want to book holidays, it makes sense that you have to send a photo of the ID. I'd trust them more than TikTok. TikTok is used in the whole world, and everyone who knows something about technology could potentially access and hack it" (Moritz, 15)

In addition, they point out that social media is influencing our lives negatively. They feel that there is more hate instead of kindness and support among the people. They criticise how other users behave on the platform and subsequently hope that other users change. Other users should realize that „you only lose energy and time when you spread hate. You don't achieve anything positive only that the person feels hurt. So, keep it to yourself, if it's nothing positive" (Mark, 16). They fear that this attitude has an impact on the real lives where "people look only for having great contents, instead of helping

others” (Julia, 13).

However, by moderating the content, limiting the possible interactions and reactions to videos the teenagers hope that TikTok becomes a nicer and safer place. They think that there should be more warnings on videos with potentially scary, unhealthy or dangerous content. Like this they hope that there will be less inappropriate contents. Moreover, TikTok should completely delete functions like the option to download your video or the possibility to comment. Then there should be also less hate according to the teenagers because „if everybody can post what they want and nobody can comment, nobody needs to be afraid anymore” (Tom, 16).

5. Discussion

In this analysis I want to answer the research questions by reflecting on and discussing the statements of the teenagers regarding the theory. I want to explain what privacy means for the teenagers, how they protect themselves and how they perceive the risks on TikTok to be relevant for them. In the end, I want to point out the relevance of the findings for applying the privacy paradox to young users of TikTok.

5.1 What privacy means for the teenagers on TikTok

Privacy is an important topic for the teenagers offline as well as online. If they post something, they are very careful about which information to disclose. The online environment, however, challenges the young users. They become insecure about what to post or if they want to post something. In the following paragraphs it is explained what is important for the teenagers regarding their privacy and how the application TikTok specifically challenges them.

5.1.1 Fear of (cyber)bullying

Even if a boy (Tom, 16) said during the focus groups he would like to show others his creative videos, there is a constant fear which keeps him from doing that. The reason for this is not necessarily his concern about his data when something is published online. Instead, the teenagers see their privacy in danger concerning the social threats. When they think about posting a video on TikTok showing their hobbies, creativity or dances, they feel exposed. They do not want this personal information to be online, because they fear that others make fun of them or bully them. They, therefore, see cyberbullying and hate as the predominant risk on TikTok and the internet overall. Privacy, therefore, means for the teenagers to be able to keep certain information hidden in order to protect themselves against social threats.

They are aware that numerous people can watch their content – including friends they trust, people they know but are not friends with, and strangers with good and bad intentions. Taking the Communication Privacy Management theory from Petronio (2002) into account which talks about

managing different boundaries, it is obvious that different groups require different sets of boundaries. However, this is difficult to manage on SNS since there is no selective control over the information - if the information is posted publicly. Especially that any video can go potentially viral on TikTok and can be, therefore, seen by various people, makes this platform even less secure for the participants.

Their whole online experience circles around being afraid of receiving hate in any form. They do not distinguish how it would affect them online and offline. They instead see a direct link from the hate they could receive online to their social life in the real world. They anticipate that when you are bullied online, it continues in school and other parts of their lives. The fact that the teenagers live in the rather small country Luxembourg in which they can be easily recognized, increases the pressure on the teenagers. This also includes that other people, who usually do not have access to the things the teenagers post on the internet, like their parents or grandparents, would get to know this information. As they value the opinions especially of their family this is something they are afraid of as well.

Looking at other studies, Livingstone (2008) for example points out something similar. She said that "unlike privacy advocates and more politically conscious adults, teens aren't typically concerned with governments and corporations. Instead, they're trying to avoid surveillance from parents, teachers, and other immediate authority figures in their lives" (p.58). These are also the findings of the survey of Adorjan & Ricciardelli (2019) which realized as well that the concerns of the teenagers are mainly about their peers and other users and less about the organisational issues like the authorities or institutions.

Data collection, next to this dominant fear of getting bullied, seemed indeed to not be as relevant for the teenagers. Nevertheless, they see their privacy in danger on TikTok. However, it needs to be distinguished between social and organisational threats which is fundamental for the following analysis. When just looking at the opinions about data collection, it seems that the teenagers do not care what happens with their information. However, they are so occupied with protecting their privacy from social threats that big data and related risks stay in the shadow. The reasons that the teenagers do not see data collection as a dangerous threat have different explanations which are going to be discussed in the next chapters. However, first I want to question which role TikTok plays for the teenagers regarding their privacy and, therefore, understand why this is the predominant threat they perceive.

5.1.2 TikTok as a platform with high standards

To understand the role of TikTok regarding the perception of privacy, I want to first take a look at other SNS they use. Even if they like being on TikTok, they use it for different purposes than other applications. On other applications they like to communicate with their friends and present themselves. Everybody enjoys using TikTok, and yet some teenagers said that their favourite application is Snapchat or Instagram. Interestingly, the interviewees adapt a different privacy management depending on the SNS they use. On TikTok they barely share any information. If they do, mainly only on their private profile. However, on other SNS they seem to be more open and set different standards regarding their privacy.

„Yes, on Instagram I post photos, but you can't recognize me" (Elisa, 14)

"On Snapchat and TikTok I have a private profile, which means you have to add me first to see my content. But on Instagram my profile is public" (Julia, 13)

"Twitter, I see almost like a diary. There I write things about my parents for example, they should better not read it" (Michael, 18)

The concerns the teenagers expressed like hate and cyberbullying can be applied the same way to the other platforms they are using, and yet the teenagers are more open when posting something on Instagram or Twitter. Some of the teenagers expressed that they feel that there is some kind of self-disclosure needed in order to be part of these online communities. Ellison et al. (2007) and Palen & Dourish (2003) also pointed out this fact. However, not only that self-disclosure helps to be part of a community, but it is also an important aspect in the process of self-identity which is especially in the lives of the teenagers a crucial development task. This process is no longer only taking place in the real world but "SNS provide people ample opportunities to satisfy their need for self-identity" (Wu, 2019). According to Min & Kim (2015) this starts from creating a profile and displaying personal interests, over getting feedback from other users how they perceive myself, to understanding how others perceive and show themselves.

Developing their own identity is essential and nowadays also partially happening on the internet. It seems that this is more applicable to the teenagers on other platforms than TikTok. This can be explained by the different natures of the platforms. One boy (Michael, 18) for example explains it by saying that you have to post videos according to the 'standards' of TikTok, if you do not want to be

bullied. He adds: „I usually don't do videos, because I don't have anything to offer. On Instagram I like to do photos. That is something easier" (Michael, 18). Here he is referring not to his media competence of doing videos but to his way of expressing his hobbies and his identity. He feels on TikTok mainly the pressure that the content needs to be done a certain way so that it can be liked by many other people instead of feeling free to express himself. In addition, on Twitter he posts his thoughts and feelings and cares less about the consequences. TikTok is, therefore, mainly connected with the fear of receiving hate for him. Also, other participants were saying they were not dancing good enough to dare to post a video on TikTok, yet like dancing in general. However, TikTok, or better its community, makes them feel vulnerable which is why they prefer to keep their videos to themselves instead of sharing it with other users.

Most of the teenagers used musical.ly before. They point out that back then, the feeling and experience they had was different - more positive and polite. They enjoyed sharing mainly dance videos without having the fear of receiving hate. This points out the shift of the application, the teenagers perceive. TikTok changed "from a video platform with funny dance videos, to a place where you're criticised if you don't meet the standards", as Sophie (15) summarized. This new user experience is influencing the interviewees. Even if they are "big fans" of the platform, the echo which goes through the conversations is that there are many inappropriate things happening on the TikTok: starting from hate in comments, over contents which show violence, to reposts of embarrassing videos. These risks seem to be predominant on TikTok for the teenagers.

5.1.3 Control over private information

Remembering the words of Lutz et al. (2020) which highlight that privacy is all about "the notion of control" (p.3), it explains why this seems to be an important aspect for them. They want to decide which information is seen by whom to be able to better predict the consequences. They are afraid that their information is getting in the wrong hands and is, therefore, out of control. They want to be the ones who select what to disclose, at what time, which way and to whom.

Especially on TikTok there is the fear that any publicly posted video can potentially be seen by numerous users. Considering the special algorithm on TikTok, which want to help users to get easy access to popularity (Leander & Burriss, 2020), can also cause a video to be seen by thousands of users not because they appreciate the content but because they make fun of it. Since you cannot know how

big your reach with your video can be, TikTok challenges the desired control the interviewed teenagers ask for.

Moreover, the teenagers pointed out that they are concerned that their information can be reposted even without their knowledge. They talked about other videos which were downloaded and reuploaded within a very short time. This is something they want to avoid about their own videos on TikTok. This reminds of the four specific features of SNS Boyd (2010) defined which challenge privacy: persistence, replicability, scalability and searchability. The knowledge of the teenagers that "nothing can be deleted" (Sophie, 15) from the internet is scaring the teenagers. This is what Petronio (2002) describes under the co-ownership of information. As a user of SNS anyone becomes a co-owner of the information, who can do anything with this information. The problem the teenagers mainly associate with this is that it is not possible to prevent someone from reposting a video. The interviewees themselves have never been affected by this yet saw already many videos where somebody made fun of other people. The problem is that these videos are not only circulating on TikTok. Somebody downloads them and the teenagers are sharing these videos on the other platforms and applications as well. This means that the power which comes along with the co-ownership becomes even bigger and, therefore, the experienced control over the information is decreasing.

Furthermore, TikTok implemented a function which takes the co-ownership another step further. On TikTok there is the possibility to duet or stitch a video. TikTok (2020c) explains these functions like: "Stitch allows users the ability to clip and integrate scenes from another user's video into their own. Like Duet, Stitch is a way to reinterpret and add to another user's content, building on their stories, tutorials, recipes, math lessons, and more" (n.p.). This means, if the user activates the possibility to stitch or duet a video, anybody can use this content and integrate it into their own video. This can generate very creative videos on the one hand, and yet makes cyberbullying on the other hand easier. Like this there can be many reposts of the video which gives even more visibility to your content. This is another factor why especially TikTok challenges the online privacy of its users.

In addition, if the boundaries of the users are not respected, privacy violations can occur. As Trepte (2015) describes it, it is more difficult on SNS to deal with privacy breaches, because users do not have enough control of the information. Especially as they are not only afraid of the social threats online but also of the consequences which also affect them in the offline world, makes it even more difficult for the participants to deal with privacy breaches. They understand that hate – no matter if online or

offline – cannot be controlled or stopped easily. Due to their lack of measures to fight against these violations, they see their privacy in danger.

To have better control over their information, most of them created a private account on TikTok. This gives them more control over who sees which videos. It offers them some kind of security, as they reported. Moreover, they believe that on a private account you can post anything without any risk. This is why some of the participants did upload some videos with this privacy setting, as they made them feel safe enough to disclose information. In the experiments of Brandimarte et al. (2013) similar results were found. When users were given more control over the shared information, they tended to disclose more information – even though that there are still risks which remain. In fact, their followers can still react negatively to their videos or repost the videos. However, it was important for the teenagers to better determine who can access this information. They want to decide who sees the content as they only want people who they trust to see their selected videos.

Even if the teenagers are grateful for the settings like the option for a private account, they do not perceive that TikTok has enough control over its content. On TikTok the teenagers saw many reposts of videos which TikTok is not able to take down on time. Moreover, not only that they feel that TikTok cannot control the video uploads, but they also think that the platform cannot limit the interactions between the users sufficiently. The teenagers feel that everybody is allowed to do anything they want on TikTok including spreading hate because it is not regulated enough. They want to have stricter rules and consequences when a user violates the community guidelines. Like this they hope that other users are changing their behaviour online and TikTok becomes a safer and nicer place. They know that there are "content moderators" which try to keep the platform clean, but they feel that their work is not enough.

TikTok (2021b) provides on its website an overview of the videos taken down by its content moderators and innovative technology. It shows the 'proactive removal rate' – when a video was deleted before it was reported by users- and the percentage of 'removals within 24 hours' – when a video was removed within 24 hours after it was reported. Comparing the percentages when the focus groups took place (Jan- March 2021), there is the highest discrepancy between the numbers for harassment and bullying with a 66.20% proactive removal rate and 83.80% removal rate within 24 hours. Even if the second number is higher, within 24 hours such videos can be reposted, downloaded and reused numerous times. Therefore, the fear of cyberbullying and the perceived lack of control concerning privacy breaches of the teenagers is justified. Even if the teenagers think that it is not

TikTok that is causing the threats, they still see the platform in the responsibility to do something against it. The lack of control which they are perceiving, is something TikTok should be working on to make them feel safer.

5.2 Users are caught between inspirations and fears

When doing the activity "Good Cop – Bad Cop" with the teenagers, the two lists of positive and negative arguments varied considerably in the length. The teenagers perceive many positive aspects of TikTok which is why they also called themselves "big fans" of the applications. However, when talking more about this subject it became obvious that the teenagers also struggle with fears and insecurities related to the platform which mainly circle around inappropriate content and cyberbullying. And yet they are – besides one – still using and loving the platform. In the following chapters the confrontation between the two different sides such as inspiration and entertainment and on the other hand the perceived risk, is going to be compared. It is going to be discussed how the teenagers perceive the risks and how they react to and prevent the risks accordingly. I want to investigate why the teenagers still use the application even if they are aware of certain risks.

5.2.1 Outweighing risks

The interviewed teenagers consume contents to laugh, to learn but also to be inspired from. In general, they connect many positive emotions with this platform. They have the possibility to share their own opinion which gives them a way of expressing themselves. At the same time, they see other people sharing the same thoughts and fears. In general, TikTok serves as a platform for a very diverse public. Everybody finds their interest and way of using the platform with their individual preferences. This reminds of the social capital Ellison et al. (2011) pointed out. TikTok serves the need of the teenagers. They can get support, as well as ideas from friends but can also meet other people they share the same interests with or feel connected to. They are encouraged to be creative, and they are inspired by various role models. Therefore, TikTok can have an influence on the construction of identity as for example Debatin et al. (2009) found out already for Facebook. The teenagers were referring to some TikTok videos also as motivators to do sports for example or as inspiration for being creative. All in all, TikTok is a platform which serves several needs of the teenagers. TikTok inspires and entertains as it plays an important role in the community of the young people which offers them many opportunities for self-expression and identification with others.

All positive aspects about TikTok, however, also have a downside. That the teenagers see in some cases their privacy in danger on TikTok is already obvious. Yet, they perceive the threats differently. Lutz et al. (2020) observed the same phenomenon and conclude that depending on how the users perceive the risks, different threats (vertical and horizontal) are more or respectively less relevant in the decision making. Taking the privacy calculus idea into account it explains certain behaviour by comparing and outweighing benefits and perceived risks (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). Indeed, the teenagers applied different calculi depending on the risks and their results and, therefore, their behaviours differ.

To start, the organisational threats like hackers and data collection are not predominant for the interviewees. There is the influence of the immediate gratification which weighs higher than the gratification a person receives in the future (Acquisiti, 2004). Therefore, they enjoy more the positive emotions they receive when using the app which outweigh the benefits they receive in the future when they are now protecting their data. However, this is not completely relatable to the privacy calculus theory as this assumes that they take the actions rationally. This requires a full understanding what data collection is and which impact it has on the teenagers individually. Yet, besides one participant, the teenagers did not know about which data is collected by whom and for what reason. Therefore, their decision making is biased through incomplete information which Acquisti & Grossklags (2007) already warned about.

In contrary, the teenagers are more aware of the risk of phishing, virus and identity theft. Nevertheless, the benefits they receive from TikTok weigh more, considering the privacy calculus. They prefer to watch funny and inspirational videos, instead of quitting the application because there are dangers which can affect them anywhere on the internet. This calculus can be biased, however, because they are likely to underestimate the risk, as they have to question something they like and associate positive emotions with. With this bias, it is difficult again to take a rational decision, since both sides are not valued the same way (Slovic et al., 2002).

The other risk the teenagers mentioned is inappropriate content. This also seemed to be a risk they are confronted with very often. These contents seem to shock the teenagers and they find it outrageous that this can be found on TikTok. Yet, even if these contents seem to affect their user experience negatively, the participants did not do anything to protect themselves from seeing this

content. They do not take any measures and just swipe to the next video, because the risk for them is not perceived as very high. This is why they only seem to be bothered by this, but do not suffer from any further consequences. What should not be forgotten in this context is that SNS can not only act as a stressor, but it also helps the users to cope with various challenges they have to face in their lives (Wolfers & Utz, 2022). Watching the other plenty of positive videos where they can regain energy and which make them feel good as they transmit positive emotions or encouraging messages, is what the teenagers highlighted as well. These videos in which they are entertained and inspired weigh more than the inappropriate contents they involuntarily consume, therefore, they keep using TikTok as they are used to.

Last but not least, there is the risk of cyberbullying which the teenagers present as their greatest fear on TikTok. The teenagers are well aware of the other social threats and especially of the negative reactions any video could get. In contrary to the other mentioned risks above, they do not expect any immediate gratification when posting a video. In other studies, such as by Tufekci (2008) different results were found. He highlighted that "the need to be seen is greater than the fears students have about privacy intrusions" (p. 34). In this research instead, the fear of getting negative feedback is predominant. The urge in contrary 'to be seen' is not as attractive for the teenagers. On the one hand, they know that getting likes and followers, feels rewarding. On the other hand, they see this risk of cyberbullying likely to happen, which is why the importance of protecting themselves against this risk increases. Petronio (2002) describes in her Communication Privacy Management theory that privacy management is a dynamic process. Various inputs influence their decision making. Especially as they see and hear many examples of others being bullied or receiving hate, makes these risks seem more realistic and, therefore, it has more impact on the decision making and calculus to protect their privacy. Moreover, as explained in the previous chapter they feel the pressure to perform according to the 'standards' of TikTok. This insecurity influences the decision making and makes them adapt their online behaviour. The teenagers mainly see the negative consequences which outweigh, in contrary to the above-mentioned risks, the positive gratifications. Therefore, they decide not to post any videos.

5.2.2 TikTok, a “must have”

All these positive emotions, explained earlier, are increased by the fact that their peers think the same way. They all said that they downloaded TikTok or former musical.ly because of their friends. They see TikTok as a way to be connected to their peers. They send each other funny videos or sometimes also do TikTok’s together (and save them in their drafts). Moreover, TikTok became a topic in conversations. They talk about the newest trends and memes and imitate the dances of the platform. Two boys in the focus groups did not have TikTok installed, yet tried to be up to date by checking the newest TikTok trends on YouTube to be able to follow. Lutz et al. (2020) describe SNS as an entry ticket to society. If you want to be part of the group and to understand the jokes, it seems that the teenagers indeed felt the pressure to have TikTok.

Even if the boy who deleted TikTok tried to argue that “well, if that's the argument for TikTok ‘to be like the others, then you have to think that you don't always have to be the one who imitates everything, but you can also be the one who starts something or who is different” (Mark, 16). However, with this opinion he was the only one in the groups. They all agreed that TikTok is a “must have” in our society to understand what is happening around them. Considering that many of them use TikTok as a source for information about politics, fashion etc., it serves various needs of the teenagers to be part of the society and their peers.

Yet, this pressure caused that the teenagers downloaded TikTok without hesitation. They did not question the application and possible privacy violations. “Cyber abstinence” as Adorjan & Ricciardelli (2019, p. 10) called it, is not an option anymore for the teenagers. If they want to be part of their peer group, they feel forced to download the application. Besides the one critical interviewee (Mark, 16), they all said that that is kind of an obligation to have TikTok on the phone. They do not want to be left out which is why they did not think about the risks for example of data collection before downloading TikTok. They all agreed that they did not reflect critically before installing it. This is also what Bailey and Steeves (2015); Hargittai and Marwick (2016) and Livingstone (2008) found in their research. The way for the teenagers to protect their privacy is not to give up on using social media as it is immersed in our society. The need for being part of this trend and benefiting from the various positive aspects, outweighs the perceived risks. It even pressures the teenagers into installing the application without questioning the possible risks in advance.

However, that the peer pressure does not influence their posting behaviour is unusual. Authors like Palen & Dourish (2003) point out that it is a requirement to disclose private information to fully be part of the SNS community. A boy highlights the same idea by making a comparison to the peer pressure some youngsters feel about smoking. Yet, posting something has not been as tempting for the participants, even if all of them feel this peer pressure. All of them reported that their friends also post videos. For the interviewees, however, the social threats were higher than the wish to be seen on the platform. Nevertheless, there were a few participants who still wanted to share their videos at least on their private profiles. With this setting, they felt safer, and the anticipated risk felt lower. Only under those circumstances the teenagers, wanted to post a video.

All in all, we can say that the teenagers are caught in this double bind. TikTok offers them many possibilities to be entertained, inspired and, moreover, to be part of a community. Depending on the risk, the teenagers come to different results on how much they feel the need to protect themselves. However, mainly TikTok with its benefits wins over the threats which are pushed because of the peer pressure they receive. In contrary there is cyberbullying as a social threat which has a special impact on the teenagers which is why they decide to protect their privacy and adapt their behaviour online. In the next chapter I want to investigate this further by focusing on the different risk awareness' and subsequently their perception of the protective behaviour.

5.3 Anticipated risks and effectiveness of protection

An argument that is often mentioned is that users lack the knowledge and skills to protect themselves, which is why they show paradoxical behaviour as described in the theoretical part of this thesis. The lack of knowledge goes along with the awareness of the risks which influence the behaviour. However, if they put the protective measures into practice is not only depending on the skills of the users, but also related to the expected self-efficacy of their privacy management.

5.3.1 Knowledge and risk awareness

As we can already resume from the previous paragraphs, the risk awareness of social threats is higher among the students, compared to the risk of organisational threats. One reason for this is that the teenagers have a different level of knowledge concerning the two topics. So do other studies already explain that the knowledge about privacy and privacy breaches is important when explaining the privacy paradox (Acquisti & Gross, 2006; Tufekci, 2008).

During the focus groups it became clear that the teenagers know more about cyberbullying than data collection. Cyberbullying or hate online in general is dominant during their online experience. Even if they have never experienced cyberbullying themselves, they have seen and heard many examples of friends or other users on the internet who were affected. In addition, not only that they see these risks themselves, but it is also a topic in school for the Luxemburgish students. As a boy explained in Luxembourg there are different organisations going to schools to do sensibilisation about this topic. BEE SECURE (2022) for example, through which these focus groups were organised, goes regularly to schools to talk with the students about internet safety. Various topics are discussed in the trainings. However, when asking the students, the main topic they recall is cyberbullying. This means that they learn from various sources – in school and from their own experience – what cyberbullying is and which consequences it can have. Subsequently, their knowledge and their risk awareness are high. Accordingly, they adapt their online behaviour and privacy management in order to prevent them from these threats. They barely post anything on social media. If they do, they carefully select what and mainly also that they cannot be identified.

On the other side, big data is a topic the teenagers know less about. Even if it is also discussed in the BEE SECURE trainings (2022), the students usually do not recall as much from this part of the trainings. Their knowledge is in general not elaborated which I could see from the follow up questions concerning this topic in the focus groups. The teenagers do not understand the system behind TikTok but also have never questioned it. They barely had any knowledge about big data and are, moreover, not aware of the consequences it can have for them. Especially the fact that TikTok, instead of most of the other services they are using, does not belong to Meta or Google, makes it even more difficult for the teenagers to understand the system. As Hoffmann et al. (2016) already explained the more complex the online world gets, the more difficult it is for its users to understand the potential risks and mechanism behind it and, therefore, make adequate decisions. They have a vague idea how these big companies work and which applications they own, but their knowledge about ByteDance instead

is even smaller. As they do not understand the system of who is owning their data and what they do with it, it becomes difficult for them to estimate and understand the risks. Therefore, the teenagers' risk awareness is not as high as for cyberbullying.

Not only that the risk awareness is not as high, but the teenagers also do not perceive data collection as a problem. They do not see the information collected by ByteDance as a privacy violation as they do not know that much about it. They, on the one hand, do not understand how valuable this data is for the company, and, on the other hand, which impact it can have on their future lives. This described feeling of indifference or helplessness occurs especially regarding organisational threats, which also Hargittai & Marwick (2016) found in their research. The teenagers do not see any harm to themselves when thinking about big data and believe that they are in control of it when they limit what they post. They underestimate how much data is collected about them, because they are not aware that TikTok collects a lot of data even when you use the application passively by collecting what you like, what you watch etc. In addition, there is the feeling of indifference. They believe that their data is not useful for any company and cannot be used against them. The combination of a low level of knowledge and the feeling of indifference causes to not see data collection as a threat and, therefore, not to take any measures to protect any private information on TikTok.

On the contrary to the opinions above, I could also observe also the opposite during the focus groups. There was one participant who was very critical concerning media and, therefore, was well aware of the risk – both social threats and organisational threats. He questions how TikTok operates and became very suspicious. Furthermore, he anticipated that there is going to be a scandal like a data breach on TikTok soon which is why he decided to delete the application. Instead of feeling resigned like the other participants he felt insecure and took action. This example underlines the statement of Bartsch & Dienlin (2016) and Dienlin & Trepte (2015) described in the theoretical chapter that the lack of privacy literacy influences the risk awareness which in conclusion determines how or if the person shows protective behaviour. In this study we could see that the more the teenagers know about the topic, the more concerned they are and vice versa. Yet, when explaining to them in the interview how their data is collected and how TikTok treats it, they still expressed spontaneously that they would not adapt their behaviour and instead keep using the application as they are used to do it – being careful what to post but still be part of the TikTok community.

5.3.2 Perceived self-efficacy of protective behavior

Depending on how efficient the users see their protective behaviour to be, the more likely they are to put it into practice (Floyd et al., 2000; LaRose & Rifon 2007; Yao & Linz, 2008). This seems to be a crucial aspect for the teenagers. They do show certain protective behaviours when it comes to protecting their privacy. However, they are missing out on more opportunities to protect themselves better, because they do not see other measures working sufficiently.

Starting from the privacy settings they could use to protect themselves from social as well as organisational threats, there was no interviewee who uses this actively for privacy management. For the big majority of the teenagers this is not the case because they are lacking the skills to change them. Even if they had in the beginning some troubles finding it, they all managed as they know how to navigate on TikTok easily. They mainly appreciate the option to change the settings or already having the safer pre-settings when you are a young user, however, they are not entirely convinced of their effectiveness. They did not report any experiences or fears that strangers contact them, therefore, these settings did not seem to be relevant for the teenagers. They believe that privacy settings make it more difficult for hackers to get their information, but not impossible. Moreover, they understand that they already have so many digital footprints on the internet that a lot of information can be found.

Even if in general the teenagers are not entirely convinced about the privacy setting, there is one setting which all of the interviewees appreciate and trust: the option to have a private profile. Lutz et al. (2020) explains that the level of resignation can vary depending on the threat and which value users give to it. Most of them activated it, because like this they feel protected concerning the social threats as only chosen people can see their contents. Nevertheless, the most efficient method to protect themselves is according to the teenagers to not post anything. Besides a few exemptions, they all follow this instinct. They select - if they post something - very carefully what information they want to disclose. But in general, by stopping to produce content, they do not give others the possibility to harm them, and they are, therefore, protected for their greatest fear of cyberbullying. This is why other settings like limiting the possibility for others to for example ‘stitch’ their contents or to comment are not relevant as they do not produce contents.

Even after the teenagers understood that also ByteDance collects their data nevertheless, most of them were shocked but still not very concerned. This is because they feel powerless concerning the data collection. They feel that now it is already too late to change something, and they cannot protect their privacy anymore. There assume that there is already a lot of data collected as they already use TikTok for some years and, moreover, use also other SNS and the internet in general. In the theory this was presented as privacy cynicism. Lutz et al. (2020) described that this emotion of feeling disempowered makes the users believe that any measure they take now are not helpful anymore. The interviewed teenagers for this study believe the same. They resign and give up on their privacy in that sense. They already feel exposed to organisational threats and do not see a way out of this. Even deleting the application does not help, as ByteDance already has a lot of information. Therefore, they prefer to having the application as they are used to. They are confident enough by protecting themselves from social threats. The organisational threats which they see not as relevant anyways, do not motivate them to change their privacy management on TikTok.

5.4 Privacy paradox on TikTok

The distinction between social and organisational threats seems to make a big difference for how the teenagers perceive privacy on TikTok and, therefore, how they adapt their privacy management. This in return has an influence on how the privacy paradox can be adapted to the usage of TikTok of these teenagers. On the one hand, the teenagers present themselves as mature and well aware of the risks to which they show adaptive behaviour and, therefore, protect their privacy. On the other hand, however, the teenagers still use the application without questioning what is happening with their data. The different aspects mentioned in the previous paragraphs are now going to be summarized and reflected regarding the privacy paradox.

5.4.1 Relevance of social threats

First of all, I want to reflect on the social threats which the teenagers perceive as the most important. The privacy paradox states (Barnes, 2006) that the teenagers, even if they want to keep their privacy safe, they still post something on SNS, because they are not aware of the “public nature of the Internet” (n.p.). This indicates that the users upload videos without questioning who will see this content and what others can do with this. The results from this study, however, show that the

teenagers act according to their concerns and adapt their privacy management related to social threats. They do not want to expose themselves by trying to keep up with the 'standards' of the platform. Even if some of them like to dance or do handcrafting, they prefer to do this in a for them safe environment where they have more control over the information and, therefore, can protect their privacy better. Teenagers are aware that a public post can be potentially seen by everybody. Yet, they do not want to share their private information with many people. Therefore, they consciously decide not to post anything. They take preventive measures and do not want to expose themselves naively to this threat. They mainly adapt their posting behaviour but also use some privacy settings to limit the people who can see their contents. They feel that those measures keep them safe from potential privacy breaches and perceive their strategy as efficient. This realization puts the theory of the privacy paradox in a different light.

Moreover, it does not only contradict that the young users are aware of the reach a post can have especially on TikTok, but it also underlines that the teenagers do not show paradoxical behaviour. They know that their content can receive hate comments, can be reuploaded or even shared on other platforms. They developed a fear of cyberbullying. It is a topic their online experience circles around and they are confronted with from various sources. They are aware which impact cyberbullying could have on their lives which is why they would do anything to prevent this. Their risk awareness keeps them from posting any contents as they fear that potential privacy breaches are not controllable. They see this problem of negative reactions to their content and act accordingly. They found a strategy which makes them feel safer. In this point the privacy paradox theory underestimates the users. Instead of naively following the trend, the interviewed teenagers want to protect their privacy instead. The privacy paradox can, therefore, not be applied to the social threats of cyberbullying on the application TikTok for the interviewed teenagers.

5.4.2 Relevance of organizational threats

When we take data collection as a threat into account however, the findings go according to the theory of the privacy paradox (Barnes, 2006). The teenagers do not question downloading the application. They just do what all of their other friends are doing in order to be part of the (online) community. In this sense, they naively follow every trend, as it is more important for them to have this application installed and use it, than thinking about their privacy. Yet, there is one essential difference: we have to take into account that the teenagers do not express direct concerns regarding how their private information is treated on this platform. Therefore, they did not act contradictive to their opinions. As

they are careful what to post, they consider themselves being relatively safe on the platform. However, that their data is anyways collected, they do not fully understand. This is what Youn (2009) described by saying that the young users do not know enough to judge their online safety correctly. They overestimate their protective behaviour concerning the social threats and, therefore, falsely believe that they are safe.

However, even after explaining and discussing this problem with the teenagers in the focus groups, they express that they want to continue to be on TikTok as it is more important to them, than stopping ByteDance from collecting information about them even without actively posting videos. The explanations for this phenomenon described in the theoretical part of this thesis can, therefore, be applied to the interviewed teenagers. The findings of this research shows as well that the less knowledge they have, the less they are concerned about this issue and, consequently, do not take any preventive measures. Instead, they either do not care about what is happening with their data or see mainly the positive aspects which result for them. As they do not consider this problem to be changeable, they feel powerless because they feel that they cannot do anything to prevent ByteDance from collecting their data. The feeling of powerlessness, as well as the feeling of indifference concerning the data collection reduces the relevance for the teenagers to worry about their privacy and to prevent themselves from organisational threats.

Contrarily there was one boy (Mark, 16) who acts differently. He admits that he was not thinking when downloading TikTok, but after he got more information on how SNS are working, he decided to quit the application TikTok. He is a very critical user with a clear idea of what is important for him and what he wants to keep private. He does not want to be pushed to do something just because others are doing it. He was in general critical about too much SNS usage and pointed out the negative mental health issue which this can cause. Therefore, he is not as positively biased as the other teenagers who mainly see the benefits which outweigh the risks. He consumed documentaries to learn more about the "truth about the world of SNS" (Mark, 16). Thanks to the knowledge he gained about privacy breaches, he deletes the application TikTok. Moreover, the big difference compared to the others is, that he not only has more knowledge about big data, but he is also aware of the risk and the negative impact it can have. He is expecting privacy scandals which could also affect him. Hereby we see the importance of risk awareness which can influence the privacy management. Having knowledge is the first important step, but then what seems to matter is how they perceive the risk to be relevant for them. Even after explaining the dangers to the teenagers in general, they still did not see this as a threat for them. Therefore, focusing on the consequences for each user, could be more useful. Then

as we can see from the example of Mark, there is a chance that the teenagers do not show paradoxical behaviour anymore and instead protect themselves and their privacy.

5.4.3 Placed in a double bind

Not only the lack of knowledge and risk awareness seems to have an influence on their behaviour online, there are on the other side also many positive arguments that outweigh the negative aspects of TikTok and encourage the teenagers to keep using the application. West (2019) describes a feeling of being "placed in a double bind, caught between desires for privacy and the ability to form meaningful communities" (West, 2019, p. 37) which seems to be the main challenge for the teenagers.

They enjoy being on TikTok. They can learn something, get inspired, follow their hobbies and interests, and stay up to date. They connect many positive emotions with the usage of the application. It also gives them the possibility to be part of a community – with their friends and peers online. According to the teenagers, TikTok has as a positive influence on their social life. Receiving this gratification is more important for the teenagers, than protecting their privacy. These benefits, therefore, influence the privacy calculus considerably. They did for example not question, whether they should install the application or not. They do it because they want to be like the others; they want to be part of the trend. The risk of inappropriate content does not seem to be perceived as dangerous either which is why it does not influence their behaviour. Instead, they want to benefit from the other positive and entertaining videos, as their friends do as well. It seems that especially their thinking 'to be like the others' and the peer pressure they receive, is influencing their decision making. They pointed out that being on TikTok gives them the opportunity to be part of something bigger.

However, there has been a limit to the peer pressure for the interviewed teenagers. Even if some of the teenagers were tempted, they still did not post any videos, because the fear of being bullied and receiving hate is too big for them. This points out again how much the teenagers are afraid of the hate online. This has the greatest impact on the decision making. There are many concerns and insecurities involved which impact their whole online experience. They do not appreciate negative contents and the potential that it could also target them, and yet are still bound to this application because as some teenagers described it, it is a "must have" nowadays. Besides their existing concerns, they still would download the app or respectively would not delete it. Only one participant managed to break this

circle and decided against TikTok. Yet, the other participants are not willing to give up on TikTok because of the expected gratifications. They rather want to get inspired and enjoy the positive moments on this platform as all their peers do. This argument seems to be, besides the knowledge and awareness of the risks, the most relevant concerning the privacy paradox for the interviewees in this thesis. It explains why besides the concerns and perceived risks, they voluntarily spend time on the application TikTok.

6. Conclusion

To conclude, young users care especially about their privacy online when it concerns their private moments of expressing their hobbies and interests. They fear that this information could spread unwantedly among the online and offline community, and people bully them. As they care about their privacy on TikTok and fear that cyberbullying can affect them negatively, they take preventive measures. To protect themselves, they barely adapt their settings, but they instead control their posting behaviour. This contradicts the theory of the privacy paradox and underestimates the young users. The main impact, when taking a decision, has the risk awareness on their protective behaviour. However, when looking at organizational threats, there is another factor that influences especially the young users considerably: the peer pressure and the wish "to be like the others". TikTok has a big impact on society and attracts mainly young users. To be part of this trend and benefit from the positive aspects, makes it difficult to miss out on this opportunity for the teenagers. This combined with the lack of knowledge about big data leads the teenagers to keep using TikTok. Its special algorithm enforces the positive associations the teenagers have by providing them with personalized contents. The immediate gratifications they receive while swiping through their feeds outweigh the social as well as organisational threats.

All in all, to explain the privacy paradox for the usage of teenagers on TikTok the following three main aspects can be extracted from the results: lack of knowledge about data collection, risk awareness which gives values to the perceived risk; and last but not least the importance of SNS in the lives of young user with the resulting peer pressure which influences the decision making.

However, there are some limitations to the presented study. Firstly, the data could be richer when there have been more interactions between the teenagers. In two of the groups there have been four participants who seemed to be too small for the chosen activity, therefore, there have not been as many interactions and discussions between the participants as in the bigger group. The group activity was initially a good idea, as it helped in the group of seven participants to generate many different opinions. Nevertheless, through various targeted questions, I could still receive rich data from each individual and get an understanding of everyone's opinion thanks to the small groups. Moreover, the fact that there have been only 15 participants who all were passive users makes the generalization of the findings difficult. Even if the homogenous groups seemed to help them to open up and feel

comfortable sharing their thoughts, the teenagers showed, besides one participant, all rather similar online behaviour. A more diverse group could lead to more controversies and, therefore, enrich the data.

For future research I recommend using a mixed methods approach to first understand the online and posting behaviour in a questionnaire. According to the results, the participants can be divided to generate more heterogenous groups. Therefore, more discussions can occur, and the moderator has a better understanding of their previous online experience. Moreover, as we could see in the results of this study depending on which SNS the teenagers used, they show a different behaviour and deploy a different privacy management. Therefore, including different SNS in the discussions can be interesting. It can be investigated how they perceive the different platforms, which behaviours they show, and if they anticipate different risks. Like this, comparisons and links can be made, and these results could give further interesting insight on how young users perceive privacy online.

Lastly, following the main results of the presented study, there are two factors which make the online experience safer for young users. First of all, it seems to be useful that TikTok activated certain pre-setting for its young user. In addition, TikTok should give the users more possibilities to control which data is collected and inform its users better about this topic. ByteDance should, therefore, create informational contents which reach its young target group. Besides this, the main criticism about TikTok from the teenagers was concerning the online behaviour of other users and subsequently the standards of TikTok which the teenagers perceived as pressuring. This is why the community guidelines need to be better enforced and there should be more control over the contents on TikTok. ByteDance could use more content moderators to regulate the contents better and implement more filters and settings which prevent users from spreading hate and reuploading contents.

As this is relatively difficult for TikTok to ensure, education as a second player, needs to prepare the children for a safe and responsible internet usage. In Luxembourg there is a school subject called “digital science” in their seventh year of school starting from September 2021 (Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse, 2021). This can help to give the teenagers more knowledge about big data and the related issues. Education should focus on how big data can affect the teenagers and raise, therefore, concerns in combination with giving them tools how to protect themselves. The goal should be to make young users competent users with full agency who can make

decisions based on sufficient knowledge. In addition, there is BEE SECURE and other organisations in Luxembourg which do sensibilization about cyberbullying to talk about the social threats online as well. The results show how concerned and fearful the teenagers are because of the anticipated risks. Therefore, it seems useful to integrate the topic of “netiquette” in which teenagers could reflect about their online behaviour. Teenagers need to learn from an early age which consequences spreading hate online has for the affected user and TikTok should limit the options to post certain expressions. Even if TikTok needs to increase its safety by working on its privacy management and content moderation, the main goal should be to promote media education in formal and non-formal education to prepare the young people for the online world. Education should encourage teenagers to think critically about what happens with their data online. Besides this it is important to help them understand that empathy, respect, and kindness are as important on social media, as it is in the real world.

7. References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Retrieved from https://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf [05.03.2021].

Acquisti A., Gross R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: G. Danezis, P. Golle (Eds.) Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, 4258. Berlin, Heidelberg: Springer.

Acquisti, A. & Grossklags, J. (2007). What can behavioral economics teach us about privacy. In: A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. di Vimercati (Ed.) Digital privacy: theory, technology, and practices. Auerbach Publications (p. 363–77).

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. Presented at the 2nd Annual Workshop on Economics and Information Security-WEIS 3, 1-27, Berkeley, CA. Retrieved from http://infosecon.net/workshop/downloads/2003/pdf/Final_session6_acquisti.pdf [03.02.2021].

Adorjan, M., & Ricciardelli, R. (2019). A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. Canadian Review of Sociology, 56 (1), 8–29.

Alhojailan, M. I. (2012). Thematic Analysis: A critical review of its process and evaluation. West East Journal of Social Sciences, 1 (1). Retrieved from http://westeastinstitute.com/journals/wp-content/uploads/2013/02/4-Mohammed-Ibrahim-Alhojailan-Full-Paper-Thematic-Analysis-A-Critical-Review-Of-Its-Process-And-Evaluation.pdf [22.04.2022].

Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, crowding. Monterey, CA: Brooks/Cole Publishing.

Austin, L. (2003). Privacy and the question of technology. Law & Philosophy, 22, 119–166.

Bailey, J., & V. Steeves. (2015) eGirls, eCitizens. Ottawa: University of Ottawa Press.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11. Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312 [03.02.2021].

Bartsch, M. & Dienlin, T. (2016) Control your Facebook: an analysis of online privacy literacy. Computers in Human Behavior, 56, 147–154.

Bauman, L. J., & Adair, E. G. (1992). The use of ethnographic interviewing to inform questionnaire construction. Health Education Quarterly, 19(1), 9-23.

BBC (2021). TikTok sued for billions over use of children's data, BBC, 21 April 2021. Retrieved from https://www.bbc.com/news/technology-56815480#:~:text=Lawyers%20will%20allege%20that%20TikTok,being%20done%20with%20that%20information [09.04.2022].

Beaney, W. M. (1966). The Right to Privacy and American Law, Law and Contemporary Problems, 31, 253-271.

Beauchamp, T.L. (2009). Autonomy and consent. In F. Miller & A. Wertheimer (Ed.), The Ethics of Consent: Theory and Practice, (p. 55–78). Oxford: Oxford University Press.

BEE SECURE (2022). Formale Bildung. Retrieved from: https://www.bee-secure.lu/de/trainings/formale-bildung/ [18.03.2022].

Blank, G., Bolsover, G. & Dubois, E. (2014). A New Privacy Paradox: Young People and Privacy on Social Network Sites. SSRN Electronic Journal. Retrieved from https://www.researchgate.net/publication/323981092_A_New_Privacy_Paradox_Young_People_and_Privacy_on_Social_Network_Sites [03.02.2021].

Boyd, D. (2010). Making sense of privacy and publicity. Retrieved from http://www.danah.org/papers/talks/2010/SXSW2010.html [20.01.2021].

Boyd, D. (2007). "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. Retrieved from: https://www.danah.org/papers/WhyYouthHeart.pdf [05.03.2021].

Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1). Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2008.00408.x/full [03.02.2021].

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? First Monday, 15(8). Retrieved from http://firstmonday.org/article/view/3086/2589 [05.03.2021]

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. Social Psychological and Personality Science, 4(3), 340–347.

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), APA handbook of research methods in psychology: Vol. 2. Research Designs, (pp. 57–71). American Psychological Association.

Brown, B. (2001). Studying the internet experience. Retrieved from: http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf [05.02.2021].

Byers, P. Y., & Wilcox, J. R. (1991). Focus groups: A qualitative opportunity for researchers. Journal of Business Communication, 28, 63-77.

Calder, B. J. (1977). Focus groups and the nature of qualitative marketing research. Journal of Marketing Research, 14, 353-364.

Ceci, L. (2022). TikTok – Statistics & Facts. Retrieved from: https://www.statista.com/topics/6077/tiktok/#topicHeader__wrapper [10.04.2022].

Child, J. T., & Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. Computers in Human Behavior, 28, 1859–1872.

Child, J.T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright & L. M. Webb (Eds.), Computer-mediated communication in personal relationships (pp. 21– 40). New York: Peter Lang.

Cho, H., Lee, J.S. & Chung, S. (2010). Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. Computers in Human Behavior, 26(5), 987–995.

Choi, H., Park, J. & Jung, Y. (2018) The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51.

Clark, R. (2012). What's privacy? In J. Healey (Ed.), Privacy and Information Rights (pp. 1 - 5). Australia: The Spinney Press.

Cook, J. (2019), "Far-Right activists are taking their message to Gen Z on TikTok", Huffpost, 18 April 2019. Retrieved from: https://www.huffpost.com/entry/far-right-tiktok-genz_n_5cb63040e4b082aab08da0d3 [09.04.2022].

Cox, J. (2018a). TikTok has a Nazi problem, Vice, 18 December 2018. Retrieved from: https://www.vice.com/en_us/article/yw74gy/tiktok-neo-nazis-white-supremacy [09.04.2022].

Cox, J. (2018b). TikTok, the App Super Popular With Kids, Has a Nudes Problem, Vice, 6 December 2018. Retrieved from: https://www.vice.com/en_us/article/j5zbmx/tiktok-the-app-super-popularwith-kids-has-a-nudes-problem [10.04.2022].

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Thousand Oaks: Sage Publications

Creswell, J.W. (2013). Qualitative inquiry and research design: Choosing among five approaches. Thousand Oaks: Sage Publications.

Debatin, B., Lovejoy, J.P., Horn, A.K. & Hughes, B.N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83–108.

Dencik, L. & Cable, J. (2017). The advent of surveillance realism. International Journal of Communication, 11, 763–781.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45, 285–297.

Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and their Antecedents—Measurement Validity and a Regression Model. Behavior and Information Technology, 23 (6), 413–423.

Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80.

Draper, N.A. & Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society, 21(8), 1824–1839.

Ellison, N., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143–1168.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R. & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In: S. Trepte & L. Reinecke, Privacy online (p. 19–32). Berlin, Heidelberg: Springer.

Erikson, E.H., (1968). Identity: Youth and Crisis. Oxford: Norton.

Etzioni, A. (1999). The Limits of Privacy. New York: Basic Books.

European Union (2020). Data protection and online privacy. Retrieved from: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm [02.02.2021].

Floyd, D., Prentice-Dunn, L.S. & Rogers, R.W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology, 30 (2), 407–429.

Fox, E. (2021). Empowering our community to take control of their privacy, TikTok, 14 September 2021. Retrieved from: https://newsroom.tiktok.com/en-gb/empowering-our-community-to-take-control-their-privacy [10.04.2022].

Gavison, R. (1980). Privacy and the Limits of Law, The Yale Law Journal, 89 (3). Retrieved from https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6581&context=ylj [01.09.2021].

Gellman, R. & Dixon, P. (2011). Online Privacy: A Reference Handbook. Santa Barbara: ABC-CLIO, LLC.

Gerber, N., Gerber, P. & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computer & Security, 77, 226-261.

Gibbs, A. (1997). Focus Groups. Retrieved from https://sru.soc.surrey.ac.uk/SRU19.html [24.10.2021].

Goss, J.D. & Leinbach, T.R. (1996). Focus groups as alternative research practice, 28(2), 115-123.

Graeme, L. (2002). Genetic Privacy. Cambridge: Cambridge University Press.

Han, E. (2021). Strengthening privacy and safety for youth on TikTok, TikTok, 13 January 2021. Retrieved from: https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth [01.09.2021].

Hargittai, E. & Marwick, A. (2016) “What can I really do?” Explaining the privacy paradox with online apathy. International Journal of Communication, 10, 3737–3757.

Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people’s job search. IEEE Security & Privacy, 11(3), 38–45.

Heidegger, M. (1962). Being and Time. Oxford: Blackwell Publishing.

Hern, A. (2019). TikTok’s local moderation guidelines ban pro-LGBT content, The Guardian, 26 September 2019. Retrieved from: https://www.theguardian.com/technology/2019/sep/26/tiktoks-local-moderation-guidelines-ban-pro-lgbt-content [09.04.2022].

Hillebrandt, I. S. (1979). Focus group research: Behind the one-way mirror. Public Relations Journal, 35(2), 17-33.

Hoffmann, C.P, Lutz, C. & Ranzini, G. (2016) Privacy cynicism: a new approach to the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 10(4). Retrieved from https://cyberpsychology.eu/article/view/6280/5888 [20.03.2021].

Humphrey, T. (2003). Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. Retrieved from https://www.researchgate.net/publication/268342423_Most_People_Are_Privacy_Pragmatists_Who_While_Concerned_about_Privacy_Will_Sometimes_Trade_It_Off_for_Other_Benefits [05.03.2021].

Husserl, E. (1983) Ideas Pertaining to a Pure Phenomenology and to a Phenomenological Philosophy. The Hague: Martinus Nijhoff Publishers.

Inness, J. (1992). Privacy, Intimacy, and Isolation. New York: Oxford University Press.

Kamberelis, G. & Dimitriadis, G. (2013). Focus Groups: From Structured Interviews to Collective Conversations. London & New York: Taylor & Francis Group.

Kehr, F., Kowatsch, T., Wentzel, D. & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus, Information Systems Journal. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1111/isj.12062 [05.03.2021].

Kelion, L. (2019). TikTok supprressed disabled user's videos, BBC, 3 December 2019. Retrieved from: https://www.bbc.com/news/technology-50645345 [09.04.2022].

Kirwan, G. (2016). Privacy and trust online. In I. Connnolly, M. Palmer, H. Barton & G. Kirwan. An Introduction to Cyberpsychology (pp. 172 – 186). London & New York: Routledge.

Kitzinger J. (1995). Introducing focus groups, British Medical Journal, 311, 299-302.

Kitzinger, J. (1994) The methodology of focus groups: the importance of interaction between research participants, Sociology of Health, 16(1), 103-21.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122-134.

Krasnova, H., Günther, O., Spiekermann, S. & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society, 2(1), 39–63.

Krueger, R. A. (1994) Focus Groups: a Practical Guide for Applied Research. London: Sage.

Krueger, R.A. & Casey, M.A. (2000). Focus Groups: A Practical Guide for Applied Research (3rd ed.) Thousand Oaks: Sage Publications.

LaRose, R. & Rifon, N.J. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal of Consumer Affairs, 41, 127–149.

Leander, L. & Burriss, S.K. (2020). Critical Literacy for a Posthuman World: When People Read, and Become, with Machines, British Journal of Educational Technology, 13 March 2020. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12924 [09.04.2022].

Lee, H., Park, H. & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. International Journal of Human-Computer Studies, 71(9), 862–77.

Lee, T. L. (2013). Privacy and Social Media. In A. B. Albarran (Ed.), The Social Media Industries. New York: Taylor & Francis Group.

Lin, P. (2021). TikTok vs Douyin. A Security and Privacy Analysis. Retrieved from https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/ [09.04.2022].

Lindgren, J. H., & Kehoe, W. J. (1981). Focus groups: Approaches, procedures and implications. Journal of Retail Banking, 3(4), 16-22.

Litosseliti, L. (2003). Using Focus Groups in Research. London: Bloomsbury Publishing Plc.

Litt, E. (2013). Understanding social network site users' privacy tool use. Computers in Human Behavior, 29(4), 1649–1656.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy, and self-expression. New Media & Society, 10, 339 - 411.

Lutz, C. & Strathoff, P. (2014). Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425132 [05.03.2021].

Lutz, C., Hoffmann, C.P. & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. new media & society, 22(7), 1168–1187.

Lwin, M. O., Wirtz, J. & Williams, J.D. (2007). Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. Journal of the Academy of Marketing Science, 35 (4), 572–585.

Machackova, H., Cernikova, M. & Smahel, D. (2015). Children's Privacy Management on Social Network Sites. In P., Lorentz, D. Smahel, M. Metykova & M.F. Wright (Ed.), Living in the digital age: Self-presentation, networking, playing, and participating in politics (p. 95-109). Brno: Muni Press.

MacIntosh, J. (1981). Focus groups in distance nursing education, Journal of Advanced Nursing, 18, 1981-1985.

Maddux, J. E. & Rogers, R.W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. Journal of Experimental Social Psychology, 19, 469–479.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16 (7), 1051 - 1067.

Masur, P. (2018). Situational Privacy and Self-Disclosure. Cham: Springer

Meral, K.Z. (2021). Social Media Short Video-Sharing TikTok Application and Ethics. In M. N. Nurdan Taskiran & F. Pinarbaşi (Ed.), Multidisciplinary Approaches to Ethics in the Digital Era (p. 147-165). Pennsylvania: IGI Global.

Miller, A. (1971). The Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor: The University of Michigan Press.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. Journal of the Association for Information Science and Technology, 66(4), 839–857.

Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse (2021). Digital sciences: un nouveau cours au lycée à partir de septembre 2021. Retrieved from

https://men.public.lu/en/actualites/communiques-conference-presse/2021/05/18-digital-sciences.html [17.04.2022].

Morgan D. (1996) Focus groups. Annual Review Sociology 22, 129–152. Retrieved from https://www.annualreviews.org/doi/abs/10.1146/annurev.soc.22.1.129 [10.06.2021].

Morgan, D. L. (1997). Focus groups as Qualitative Research. Thousand Oaks, CA: SAGE.

Namey, E., Guest, G., Thairu, L. & Johnson, L. (2008). Data Reduction Techniques for Large Qualitative Data Sets. Retrieved from http://qualquant.org/wp-content/uploads/cda/Namey%20and%20Guest%20Data%20Reduction.pdf [22.04.2022].

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79, 119–157.

Norberg, P., Horne, D. & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. The Journal of Consumer Affairs, 41(1), 100-126.

Official Journal of the European Communities (2000). Charter of fundamental rights of the European Union (2000/C 364/01). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf [01.09.2021].

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. In G. Cockton & P. Korhonen (Ed.), Proceedings of the ACM Conference on Human Factors in Computing Systems (pp. 129-136). New York: Association for Computing Machinery.

Park, Y. J. (2013). Digital literacy and privacy behavior online. Communication Research, 40(2), 215–236.

Petronio, S. (2002). Boundaries of Privacy: Dialectics of Disclosure. Albany: State University of New York Press.

Posner, R. (1981). The Economics of Justice. Harvard: Harvard University Press.

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. Journal of Broadcasting & Electronic Media, 60 (1), 61 - 86.

Rabiee, F. (2004). Focus-group interview and data analysis. Retrieved from https://www.cambridge.org/core/services/aop-cambridge-core/content/view/E5A028A3DA12A038A7D49566F73416B8/S0029665104000874a.pdf/focusgroup_interview_and_data_analysis.pdf [18.10.2021].

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook, First Monday 15(1). Retrieved from: https://firstmonday.org/ojs/index.php/fm/article/view/2775/2432 [05.03.2021].

Richardson, C.A. & Rabiee, F. (2001). A Question of Access – an exploration of the factors influencing the health of young males aged 15–19 living in Corby and their use of health care services. Health Education Journal, 60, 3–6.

Rifon, N J., LaRose, R. & Choi, S. M. (2005). Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. Journal of Consumer Affairs, 39, 339–362.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91 (1), 93–114.

Rosen, J. (2000). The Unwanted Gaze: The Destruction of Privacy in America. New York: Vintage Books.

Sim, J. (2010). Addressing conflicts in research ethics: consent and risk of harm. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/pri.483 [06.04.2022].

Sim, J. & Waterfeld, J. (2019). Focus group methodology: some ethical challenges. Retrieved from https://link.springer.com/content/pdf/10.1007/s11135-019-00914-5.pdf [20.10.2021].

Slater, J. (2020). India bans TikTok and dozens of other Chinese apps in wake of deadly clash, Washington Post, 29 June 2020. Retrieved from: https://www.washingtonpost.com/world/asia_pacific/india-china-tiktok-ban/2020/06/29/6b361eac-ba24-11ea-97c1-6cf116ffe26c_story.html [09.04.2022].

Slovic, P., Finucane, M., Peters, E. & MacGregor, D.G. (2002). The affect heuristic. In: T. Gilovich, D. W. Griffin, D. Kahneman (Ed.), Heuristics and biases (pp.397–420). Cambridge University Press: Cambridge.

Smith, B. (2021). How TikTok Reads Your Mind, The New York Times, 5 December 2021. Retrieved from https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html [09.04.2022].

Smith, J. A, Flowers, P. & Larkin, M. (2009). Interpretative Phenomenological Analysis: Theory, Method and Research. Los Angeles London, New Delhi, Singapore, Washington: Sage.

Solove, D.J. (2002). Conceptualizing Privacy, California Law Review, 90 (4), 1087-1155.

Spiegel (2017). Chinesische Firma kauft Musical.ly, Spiegel, 10 November 2017. Retrieved from: https://www.spiegel.de/netzwelt/apps/musically-fuer-bis-zu-eine-milliarde-dollar-nach-china-verkauft-a-1177320.html [09.04.2022].

Spiekermann, S., Grossklags, J. & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM conference on electronic commerce. October 14–17 Florida, USA.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. Journal of Privacy and Confidentiality, 4(2).

Sujon, Z. (2018). The triumph of social privacy: understanding the privacy logics of sharing behaviors across social media. International Journal of Communication, 12, 3751–3771.

Taddicken, M. (2014). The “privacy paradox” in the social Web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248–273.

Tardáguila, C., Funke, D. & Benkelman, S. (2019). Misinformation makes its way to TikTok, Poynter, 31 October 2019. Retrieved from https://www.poynter.org/fact-checking/2019/misinformation-makes-its-way-to-tiktok/ [09.04.2022].

Thomas, L., MacMillan, J., McColl, E., Hale, C. & Bond, S. (1995). Comparison of focus group and individual interview methodology in examining patient satisfaction with nursing care. Social Sciences in Health, 1, 206–219.

TikTok (2022a). Our Mission. Retrieved from https://www.tiktok.com/about?lang=en [09.04.2022].

TikTok (2022b). Privacy Policy. Retrieved from https://www.tiktok.com/legal/privacy-policy-eea?lang=en [10.04.2022].

TikTok (2021a). Thanks a billion!, TikTok, 27 September 2012. Retrieved from https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok [09.04.2022].

TikTok (2021b). Community Guidelines Enforcement Report, 30 June 2021. Retrieved from https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2021-1/ [20.04.2022.

TikTok (2020a). Privacy Policy. Retrieved from: https://www.tiktok.com/legal/privacy-policy?lang=en#section-1 [01.09.2021].

TikTok (2020b). How TikTok recommends videos #ForYou, TikTok, 18 June 2020. Retrieved from https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you [01.09.2021].

TikTok (2020c). New on TikTok: Introducing Stitch, TikTok, 3 September 2020. Retrieved from https://newsroom.tiktok.com/en-us/new-on-tiktok-introducing-stitch [09.04.2022].

TikTok (2019). Terms of Service. Retrieved from https://www.tiktok.com/legal/terms-of-service?lang=en [01.09.2021].

Todres L. & Holloway I. (2004). Descriptive phenomenology: lifeworld as evidence. In F. Rapport, New Qualitative Methodologies in Health and Social Care Research (Ed.), pp. 79–98. London: Routledge.

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. Social Media + Society, 1 (1).

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society, 28(1), 20–36.

Vaughn, S. R. (1996). Focus Group Interviews in Education and Psychology. Thousand Oaks: Sage Publications.

Vaughn, S., Shay Schumm, J., Sinagub, J. (1996). Focus Group Interviews in Education and Psychology. Thousand Oaks: SAGE Publications.

Vigdor, N. (2020). U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning. Retrieved from, The New York Times, 4 January 2020. https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html [09.04.2022].

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4 (5). Retrieved from https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf [01.09.2021].

Weimann, G. & Masri, N. (2020). Research Note: Spreading Hate on TikTok, Studies in Conflict & Terrorism. Retrieved from https://doi.org/10.1080/1057610X.2020.1780027 [09.04.2022].

West, S.M. (2019). Data capitalism: redefining the logics of surveillance and privacy. Business & Society, 58(1), 20–41.

Westin, A. F. (1967). Privacy and freedom. New York: Athenaeum.

Wolfers, L.N. & Utz, S. (2022). Social media use, stress, and coping. Current Opinion in Psychology. Retrieved from https://www.sciencedirect.com/science/article/pii/S2352250X22000070 [17.04.2022].

Wu, P.F. (2019), The privacy paradox in the context of online social networking: A self-identity perspective. Journal of the Association for Information Science and Technology, 70, 207-217.

Yao, M. Z. & Linz, D.G. (2008). Predicting Self-Protections of Online Privacy. CyberPsychology & Behavior, 11 (5), 615–617.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. Journal of Broadcasting & Electronic Media, 49(1), 86–110.

Youn, S. (2009), Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. Journal of Consumer Affairs, 43, 389-418.

Young, A.L. & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. Information, Communication & Society, 16(4), 479–500.

Zheleva, E., Terzi, E. & Getoor, L. (2013). Privacy in Social Networks. San Rafael: Morgan & Claypool Publishers

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power. New York: PublicAffairs.