Contradictions between public perception of privacy and corporate privacy policy: A case study of TikTok

by

Luhao (Andrew) Xue

B.B.A., Shanghai Institute of Technology, 2016

Extended Essay Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Communication (Dual Degree Program in Global Communication)
Faculty of Communication, Art and Technology

SIMON FRASER UNIVERSITY
Summer 2020

Approval

Name:	**Luhao (Andrew) Xue**
Degree:	**Master of Arts**
Title:	**Contradictions between public perception of privacy and corporate privacy policy: A case study of TikTok**
Program Director:	**Katherine Reilly**

Katherine Reilly
Senior Supervisor
Associate Professor

Katherine Reilly
Program Director
Associate Professor

Date Approved: August 31, 2020

Abstract

While artificial intelligence and big data technology are booming in the platform economy, it is hard to ignore how the business practices that take up these technologies are changing people's perceptions of privacy and the implications lying beneath these practices. This paper used a systematic review and discourse analysis, respectively, to contrast how individuals perceive privacy with corporate privacy claims. Based on these results, the paper describes and analyzes the contradictions at play between personal and corporate relationships to privacy. Based on a case study of TikTok's privacy policy, the study finds that people are generally not aware of the consequences of TikTok's collection and use of personal data, and an unequal relationship has been established between the company and its users through business practice. I argued that protecting personal privacy should be considered as a part of people's subjectivity which should not be harmed, while the centralization of information and knowledge is putting people's subjectivity in greater danger than at any previous time.

Keywords: artificial intelligence; big data; platform economy; privacy perception；business practices；contradictions；systematic review；discourse analysis

Table of Contents

Chapter 1.

Introduction

"Big Brother is watching you." This short sentence appeared countless times in George Orwell's novel, *1984*. Big Brother has become a symbol for resistance against totalitarianism and surveillance, posing impacts on the western world for over half a century. In the novel, nobody has seen Big Brother in person, but everyone knows Big Brother is watching them, and freedom of thought is a serious violation of the law. The depiction of this abstract character raises awareness about what life would be like when people are living in an extreme surveillance society.

Today we rely on digital devices and software in everyday life more than ever. Data we leave on the Internet are collected, analysed and used by the institutions which provide us services and offer us hardware. This data can used to infer who we are, what we are thinking of, and even what we are going to do. Although not as extreme, there are obvious similarities between what we are expecting in today's digital reality, and the world depicted in *1984*. The data flow throughout the Internet makes people more transparent than ever. Those who are able to collect personal information are able to utilize this information for their own benefit, and these benefits can be contradictory to the wellbeing of Internet user themselves.

Privacy is a theme that has been discussed for centuries, and how people perceive the notion has varied in different time periods, not only because the technology environment has changed consistently, but also because of how people perceive themselves. Perceiving privacy can be a part of knowing one's self, and perception is affected by the changing environment, as well as people's own process of self-discovery. What people think of privacy today can be significantly different from how people understand it decades ago, even as privacy remains a core value that holds steady through time. Therefore, it is important to consider how people perceive privacy in the contemporary world, given big data, artificial intelligence as well as other cutting-edge technologies that have emerged in the platform economy, and also changes in how people perceive the interface between themselves and their outwards relationships.

Google, Facebook, other high-tech firms in Silicon Valley and around the world have realized the significance of raw data, which is used for marketing, optimizing services, improving internal operations and many other aspects. Some newly-emerged companies like Bytedance even set data analysis as the foundation of their business model. Bytedance, a Beijing based high tech company, has launched several apps both into Chinese and overseas markets, including TikTok, the well-known short-form video platform. Most of those apps are algorithmic based, which means that they feed users content according to an analysis of their user behavior and preferences.

In this paper, I analyze TikTok, which places algorithmic analysis at the centre of its business model. Analyzing TikTok's privacy policy can shed light on how today's high tech companies treat users' data and their privacy. I selected TikTok because it is less complicated in terms of privacy than larger companies like Google or Facebook. The latter have many interrelated connections. For example, one personal Google account can be used to log in to YouTube, Google Search, Google Doc and so on, and the privacy policies of each of these platfroms may differ from each other. This makes the privacy frameworks of these large companies very complicated. However, data is so important to TikTok that the company cannot survive without it. This raises questions about how high tech companies like Bytedance employ user data, and how they try to understand it.

In this work, I look at both corporate privacy policy and user perceptions of privacy. Understanding the two sides' relationships to personal data allows me to explore the contradictions between them. Since companies have more control over data than individuals, the balance of power leans towards companies. People are generating more and more individual data, but they tend to lose control over how this data can be used. The companies that have the capability to process individual data can construct individual perceptions of data and privacy. General public perceptions of privacy should be studied in order to compare with company claims of user privacy, so that some contradictions can be revealed to see if there are ways for mitigating public privacy concerns and solving privacy related issues.

In total, my research question is what are the contradictions between public perceptions of privacy and TikTok's claim of privacy. This question can be divided into two sub-questions which are how people perceive privacy nowadays and how TikTok

tries to comprehend the data they have collected according to its privacy policy. These two sub questions require systematic review and discourse analysis to find out the answers, and the results of these two piece of analysis will lead me to answer my overall answer.

Theory

When Karl Marx alleged surplus value in his 1887 book *Capital: Critique of Political Economy*, he could not have imagined how his theory would be developed and interpreted by generations to come. The notion of surplus value has had profound implications for academia and social practices as well as behaviors were built on this initial thought. He argued that labor as a precious resource can provide value to capitalists through working. The deception is that people cannot see workers' value, which is not compensated by their salaries. Instead how much value they have created can exactly exceed the incomes they have been paid. The additional value does not go to workers themselves, but to capitalists, and this kind of additional value is called surplus value (Marx, 1887) allowing capitalists to exploit the value of labourers through hiring them to work for them. Build on this fundamental notion, Marx argues that capitalism is regarded as a system of exploitation posing structural oppression onto the working class and widening the gap between the rich and the poor (ibid).

Relating Marx's theory with communication studies, one classical theory is called audience commodity (Smythe, 1977), which argues that audiences becomes the target of exploitation for media and advertising companies. This theory further scrutinizes the asymmetrical power dynamic between audience and media. Smythe alleged that people cannot watch or listen media content for free, but rather, advertising fees are included in the price of products that audiences want to purchase after view ads on freely offered media. In other words, media produce audiences and then those audiences are "sold" to advertisers. After that, advertisers have to create media content which can attract audiences' attention and when audiences actually focus on or pay attention to something, they are selling their time and consciousness to advertisers. This theory is even more evident now than before, considering that there are so many privacy concerns around how social media platforms are collecting personal data to push direct marketing messages out to individual audience members. This circulation of messages is built on personal data harnessed by high tech companies.

Scholars of the political economy of communication have further developed the theory of the audience commodity. In Vincent Mosco's book *The Political Economy of Communication*, he synthesized audience commodity and related arguments into the notion of commodification (Mosco, 2009). He argues that commodification can be divided into three parts, which are commodification of contents, the audience commodity, and personal information as commodity. As clearly seen in the book, commodification is a social process in which players, environment and motives and effects must be pinpointed and explained in relation to each other so as to understand the overall trend of commodification. Mosco's work offered an overview of the contemporary field of political economy of communication which set the basis for further research.

This work has given rise to more specific studies of political economy of communication in specific fields of interest. In a book published last year, Zuboff argued that capitalism has evolved into an unprecedented version which she calls surveillance capitalism (Zuboff, 2019). In this form of capitalism, products and services have become hosts for parasitic operation that free raw materials for hidden commercial practices of extraction, prediction and advertising. She argues that there is a new instrumentarian power emerging within the society, based on collection of personal data, and that it can gain strength from ubiquitous digital devices in everyday life. Instrumentarians leverage the surveillance capitalists' dominance over general public to modify people's behaviors by manipulating datum (Zuboff, 2019).

Given the power asymmetry between platform companies like Google and users, people have cultivated a rational indifference towards surveillance, and this may result in capitalists like Google organizing, herding and tuning society to achieve a similar social confluence: group pressure and computational certainty (Zuboff, 2019). Individual information is brought together into a large amount of anonymous data flow that is judged by its volume, depth and range (Zuboff, 2019). Greater social distance brought about by social networking has made it difficult for individuals understand that they are being cultivated through self-disclosure in daily lives.

While Zuboff sees those daily ubiquitous surveillance as instrumentarian power to cultivate general public rational indifference and the centralization of control and knowledge (Zuboff, 2019), another Marxist David Harvey has alleged the notion of

“accumulation by dispossession”, showing that capitalism uses force and theft to rob the world of value (Harvey, 2005). He argued that there is a naked transfer of wealth from the working class and the poor to the ruling class. Applying this notion to the big data setting, scholars argue that individuals are dispossessed of the data they generate in everyday life, suggesting big data is a capitalist form of data expropriation and dispossession (Thatcher, O’ Sullivan, & Mahmoudi, 2016).

These theories suggest that, in the age of bid data, high tech companies like Google try to harness, replicate, accumulate and evaluate all the data within their reach. In other words, Google is using users themselves to build Google’s own products (Vaidhyanathan, 2011) . Scholar also regard Facebook as the regime of wanting to be seen, and data are consistently used and gathered through users’ self-willing presentation of themselves on the platform (Bucher, 2012). TikTok claims to be the most creative social media platform in the world. Powered by AI, it encourages people to show their creativity and knowledge directly through short form videos on mobile phones (Cuofano, 2020). To be specific, the so-called ‘content hub’ powered by machine learning is grounded on massive data, and generates content that people like and encourages them to post more onto the platform (Cuofano, 2020). That means this application is largely dependent on users’ data to achieve business success. This makes TikTok a good case study of how high techs companies use personal data.

Therefore, in this study, I explore the unequal relationship between TikTok’s privacy claims and public perceptions of personal privacy. The unequal relationship between these two groups can be learned through studying their relative positions.

Methodology

The overall goal of this study is to learn how TikTok’s privacy claims can be contrasted with general public perception of personal privacy. In order to learn this question, it can be divided into two sub questions: what is the contemporary public perception of personal privacy, and what does TikTok claim about personal privacy.

In order to uncover this information, I conduct a discourse analysis of company privacy policies to find out how and why do they want to use data and if there are some risks lying beneath the claims. The goal of this work is to delineate how high tech companies such like TikTok claiming their ‘legal’ rights to use the personal data of their

users. On the other hand, while many apps (especially those providing information) can use the data as a mean of success in the competitive market, it is important to know how people decide to offer their personal records, through methods of systematic literature review. In total, I need to interpret the relevance and contradiction between the two sides, hoping to find some significance for current privacy debate.

Following the strategy discussed above, I use discourse analysis and systematic review as main methods for conducting this paper. Both can be understood in terms of the paradigm of constructionism (Berger & Luckmann, 1967). Social constructionism is a paradigm that sees all knowledge, even foundational knowledge, as produced through human interaction. As a result, all human actions are based on their perspective or their understanding of reality, and their behaviors can reinforce this reality. The construction of reality is built up through consistent interactions among people. Human typifications, signification and institutions are presented as part of reality, but actually arise out of human interactions (Berger & Luckmann, 1967). Discourse analysis is used to deconstruct the how discourses are constructed and come to be naturalized. Systematic review, meanwhile, is highly subjective which means that the output is relative based on the author's interpretation.

Systematic review can refer to meta-analysis, narrative reviews and meta-syntheses (Siddaway, 2019). In either case, the work is mainly qualitative, and depends heavily on the author's interpretation. In this case, I use narrative reviews to conduct an analysis of previous studies of users' perceptions of privacy in the digital economy. Gathering literature for systematic review should follow steps from scoping review, define include criteria and question, searching, screening, eligibility and study quality (Siddaway, 2019). For this research, I decided to focus on privacy perception, instead of other related concepts like privacy attitudes. I will explain this further in the next chapter. Following the search plan I established, and using Simon Fraser University's Online Library Resource as the main database, I have located over 70 relevant journal articles. Then, through screening process, I eliminated 40 articles, leaving 35 articles for full-length analysis using NVivo. This resulted in 44 nodes which were interpreted to produce the results found in Chapter 2 of this work. As for the search plan and criteria, it can be found in Appendix 1 at the end of this document.

Company attitudes and claims can be shown in their policies, as those documents establish the principles of corporate operations. Privacy policies reflect mainly how companies try to address consumers' privacy. However, the claims and attitudes cannot be understood thoroughly without seeing meanings and significance beneath surface of texts, and that is why I use discourse analysis. This methodology can reveal the deep structure of those documents, and give rise ot inferences about how companies like TikTok wishing to use the personal data collected in their own platforms. For the analysis, I mainly use three discourse analysis tools suggested by Mautner that are lexis, transitivity and modality (Mautner, 2008). I established privacy as the core term for lexis, and then I try to find alternative terms throughout the TikTok privacy document, such as disclosure, chose, choose, control, share and so on. As for transitivity, I apply "who is doing what to whom" to the documents and categorize nodes like Internal data analysis and Improving customer service. Modality is the third tool I used in this paper, and by using this tool, the degree of precision can be shown. Modality shows if the policy makes clear assertations or is ambiguous. Using NVivo, this analysis produced 30 nodes, which were extracted from one policy document. These were used to produce the discourse analysis presented in Chapter 3.

This major paper consists of four parts. This chapter offers the introduction, theoretical framework, and explanation of methodology. The second chapter presents my analysis of how people perceive privacy as uncovered during a systematic review. This work demonstrates people's frustration towards controlling their own data. How TikTok deals with users' data is presented in the third chapter, and the final chapter offers reflections and arguments about contradictions that emerge between user perceptions and corporate policies. The paper concludes that corporate approaches to privacy management in general, and TikTok's control over user data in particular, harm individual freedom and subjectivity.

Chapter 2.

Systematic Review

While the technology of artificial intelligence is booming in today`s world, it is hard to ignore the fact that data plays a fundamental part in training the AI capability. Computers are using those massive amounts of data for better computational performances, and being regarded as the cutting-edge technology of machine learning. Some of the best ones can even beat the best professionals in certain areas. For example, Alpha Go can defeat the best Weiqi Athlete in the world.

These big data are being captured and processed through AI for machine learning for business purposes. Those who are using services provided by data-reliant companies leave digital tracks which those companies are happy to harness for operating their services. The company's data use suggests there are some implications on people's perception of privacy. Privacy perception is not as simple as it looks, it should be viewed in the perspective of a dynamic relationship between the user and the company. While user data are highly correlated with personal privacy, public perception of privacy requires further scrutiny. Thus, in this chapter, I try to answer the question: What is the public perception of privacy towards companies who use their data for business in big data age?

In order to learn about public perception of privacy, we must first establish some foundational concepts. Privacy attitude is an emotional response towards privacy that are build upon privacy perceptions, while privacy concern is a degree concept that describes how much a person may worry about sharing personal data. Privacy willingness and intention are also degree concepts which capture how much a person wants to give out personal data. Thus, the privacy perception is a term that can contain a wide range of meanings being discussed and studied. Conducting this term, instead of others, allows me to present the result of systematic review more comprehensively and to have more resources to be analyzed in the final chapter.

Privacy perception is an individual understanding towards privacy and personal data. The empirical results of studies that gather interview data provide a greater understanding of privacy perceptions. These studies can show relatively reliably how

people think about privacy and personal data. After examining these studies, I explored people's privacy perceptions, and synthesis them into my own narrative. The material presented on continuation shows my results of systematic review.

Privacy as self-drawing boundary

Recent research suggests that privacy can be divided into valued-based and cognate-based approaches, the former meaning the 'right to be left alone' and the latter emphasizing control over information access and dissemination (Quinn, Epstein, & Moon, 2019). The latter is arguably more suitable in the digital age. In other words, today, privacy is usually regarded as self-drawing boundary between public and private, which suggest a sense of autonomy (Sarikakis & Winter, 2017). This means that the understanding of privacy is highly personal and subjective, and what one person may regard as privacy may be highly depend on their own understanding towards situations, data type and context (Marwick & Hargittai, 2019). And also, researchers define privacy as a social, physical boundary and access regulation (Teutsch, Masur, & Trepte, 2018), suggesting that privacy is a matter of self-drawing boundary.

Furthermore, researchers conclude certain types of information is more likely regarded as private, and they are the topic of the self, romantic relationships, problem of any kind, professional and private aspirations, personal achievement and experience, financial situation and sexual orientation (Teutsch, Masur, & Trepte, 2018). One empirical research shows that people tend to show what they are online, but that they are less likely to reveal chatting history or browser history (Bhatia & Breaux, 2018), indicating that data type is also a factor that affect people's revelation or not. From another perspective, when privacy related data is unimportant, people are inclined to trade their data for perceived benefits, such as free online services, whereas they are not willing to give out data if those data are more important (Mourey & Waldman, 2020). Whether people decide to share information with others illustrates their autonomy to set boundaries and determine what will remain secret and what will be open to disclosure.

Is privacy only about autonomy?

However, this literature reviews show that public perception of privacy is not only arbitrary, but it is also ambiguous and dynamic. The disclosure of information can be incentivized by various of factors, and such incentivization can affect people's boundary

drawing behaviors. There are many studies exploring the disclosure of personal information as a trade-off for certain benefits, regardless of rationally or irrationally, suggesting that people's perception of privacy can be altered by numerous factors.

For example, research shows that incentives can be financial benefits, health benefits, convenience and necessity, while disincentives can be lack of trust, fears of online harassment and fears of discrimination (Marwick & Hargittai, 2019). And also, a case study that examined how people perceive the consent processes used by nearly every websites and application found that what people really want it is a "quick", "simple", "easy" and "convenient" way to access the online service. They want this rather than being distracted by a tangential discussion about privacy and consent, or to be educated about their personal data (Obar & Oeldorf-Hirsch, 2018). This case study also shows that the design of online platforms can also incentivize users to enjoy the desirable services, regardless of their initial worry about privacy.

Therefore, privacy is not totally dependent on autonomy. Many factors can affect how people perceive privacy in a particular situation, even making the disclosure behavior contradictory to their definitions of privacy. In other words, public perception of privacy is not purely about their own autonomy of drawing boundary between private and public, but an area that various of factors and structural power tangled and affect with each other, resulting in people's instant decision of disclosure, as well as long term perception of privacy.

The imagined audience

When it comes to privacy, people tend to focus on whether certain kinds of information have been exposed to appropriate audiences. That is to say the appropriateness of exposure can depend on whether people are comfortable with the audience who receives that information. We know that information shared on digital platforms is not only received by other users on the platform, but is also tracked by the online platform provider who uses personal data for analysis and service delivery. This suggests that the sending-receiving relationship can be divided into two parts: social privacy and institutional privacy. Social privacy concerns privacy relationships with other individuals such as friends, relatives or strangers online, whereas institutional privacy

reflects people's understanding about how their information is collected, analyzed and reused by companies that provide online services.

In recent years, institutional privacy has become increasingly prominent, however people still tend to neglect the fact that companies and organizations are watching and listening to their online behaviors and voices. Empirical research shows that social media users view their own social networks as their primary audience, as opposed to platform sponsors or other institutions (Quinn, Epstein, & Moon, 2019). Taking Tinder as a case study, study participates revealed that they were more concerned about their social privacy than their institutional privacy. Long-time users have more institutional privacy concerns than short-time users, but even still, they cared more about having personal information exposed to appropriate persons (Lutz & Ranzini, 2017).

Drawing from my own experience with social media, what gets me most embarrassed is the possibility that someone in my social network finds out personal information that I did not want them to see, but I have absolutely no idea that how my personal data might be used by platform providers. So, as we can see, the general public sets their social networks as their main audience in terms of privacy, and they care about whether someone else might access certain personal information and use that information against them. On the contrary, they care less about those institutions, such as social media platform providers or any other Internet service provider according to privacy concerns. Therefore, people tend to neglect the very existence of institutional platform providers and underestimate the potential risks those institutions may post to them.

The imagined audience offers a starting point to go beyond the illusion of privacy autonomy of self drawing boundary. Noticing who has been emphasized and who has been relatively overlook raises questions about why people think about privacy in this way. Is there any asymmetry in the power structures between platform providers and platform users, and does this shape perceptions of privacy? What could contemporary perceptions of privacy really be if we penetrated the illusion of autonomy?

Innocence towards existence of institutions

As I have discussed above, people's ignorance of institutions listening and watching them can be shown in numerous ways. Participants in one study showed that

although they mistrust institutions, whether governments or corporations, they frequently mischaracterized the extent to which information could be aggregated and mined (Marwick & Hargittai, 2019). Another study provided participants with a variety of privacy settings to examine how they try to protect their privacy while browsing through an application. The result showed that people use privacy settings to control and limit the recipients but seem to ignore the major player in the networks, such as the service providers (Evjemo, Castejón-Martínez, & Akselsen, 2019). Actually, this kind of innocence can be shown more specifically in different aspects, and researches have conducted many researches that pinpointed certain parts of it.

Some scholars tried to connect the concept of 'legal consciousness' with privacy infringement from institutions (Sarikakis & Winter, 2017). From the legal angle, while connecting their legal rights to privacy, people are not able to link relevant legal frameworks with their own situation in which their privacy are infringed, suggesting they do not have sufficient legal background to negotiate the potential violation from institutions. This research shows that although people generally are aware of having rights to privacy, they feel that those legal claims are far from their everyday life, and thus they cannot utilize legal tools in a correct way to protect privacy. This incapability further implies what companies do with user data is less likely to be identified by normal people who can potentially supervise institutions' usage of data through legal approaches.

The unawareness of applying legal tool shows people's ignorance about institutional privacy from the law respective. In addition, when ignoring consent materials is a common practice suggested by a research, this can promote an ignorance culture towards consent materials just like one participates said: a cultural norm not to read it (Obar & Oeldorf-Hirsch, 2018). If it is a common practice, it can have terrible consequences that loopholes cannot be seen by users, and the usage of those holes can be noticed by few persons, which provide possibilities for institutions like high tech companies to manipulate data according to their willingness.

Another interesting research try to capture how people perceive the mobile phone sensors that may expose the PIN leaking, and the result shows that those interviewees can notice some parts of mobile sensors such as accelerometer and gyroscope, but most of them cannot identify those sensor's functionalities. In other

words, study participants did not know how these sensors worked (Mehrnezhad, Toreini, Shahandashti, & Hao, 2018). Those mobile sensors can build channels between users and institutions, allowing personal information like PINs to flow through the channels. The ignorance of functionalities suggests that users are less likely to correctly perceive the risk of PIN leaking resulting from insecurity of channels. In other words, they have no idea how those institutions are processed with their information like PIN, and do not know if they are able to secure those data within their willingness.

However, on the other hand, some researchers may argue that people do not totally forget the existence of institutions. For example, those who have relatively high self-acceptance, sensibility, role expectation, stability, goal-directedness, and personal relationships were found more aware of those institutions are watching and listening to them (Jin, 2018). This means that they can be aware of the potential institution censorships, but they cannot tell how those institutions are conducting censorships, as well as through exactly what kind of channels and media to do those censorships.

The reasons why people tend to overlook the harm those platform providers could bring has been explored in some studies. A major reason can be that users perceive institutions to be less relevant to themselves, compared to other they have known. From a study, if the social and physical distance between users and institutions increases, research participants were more likely to expose personal data about themselves (Bhatia & Breaux, 2018). This study gave the example that when potential recipients changed from friends or families to someone in the country, then those participates' willingness to share personal data increased (Bhatia & Breaux, 2018). The changing social and physical distance affecting the willingness of information disclosure suggests the reason why people tend to view their social network as their main audience, rather than those Internet media sponsors, is that institutions have more social and physical distance to users than their close social networks.

Another explanation can be that social media companies are cultivating a more relaxed attitude about privacy (Tsay-Vogel, Shanahan, & Signorielli, 2018). Social media are regarded as a collective symbolic environment that encourage the common theme and associated actions of information disclosure, resulting in people being less concerned about privacy and more likely to share information through social media

(Tsay-Vogel, Shanahan, & Signorielli, 2018). This relaxed attitude can refer to less likelihood of noticing risk of privacy to third parties.

Pro-surveillance?

People's ignorance about how platform companies use personal data, or their so called innocence about data uses, can lead to several outcomes, one of which is that people have the attitude of pro-surveillance more than ever. This can be expressed as: if you have nothing to hide, then you have nothing to fear (Ellis, 2020). This kind of argument echoes a five-year study which shows that Facebook is cultivating a more relaxed attitude of self-disclosure (Tsay-Vogel, Shanahan, & Signorielli, 2018). Also, Ellis (2020) alleges that there is a politics of fear being promoted: fear of terrorism, fear of crime, fear of war and general fear of the other. People are willing to share personal data in exchange for a sense of security, in the hope that technology institutions can offer protections. In another focus-group based study respondents said argued that "We have nothing to hide so that we have nothing to lose" (Marwick & Hargittai, 2019). Supporting pro-surveillance seems to be contrary to the general perception of privacy, but actually this attitude represents the fact that the ubiquitous monitoring technology has made people feel themselves powerless to control their information flow. Since they may feel that they can do nothing about it, they may as well embrace the bright side of it which is trading information about benefits and gaining a sense of security from institutions.

Another reason why people may not worry about giving out data is that institutions may have trustworthy images that make people feel comfortable about self-disclosure. Taking business websites for example, several factors are found to affect consumer trust, such as the websites' content, reach, people's expectations, reputation and endorsement (Frik & Mittone, 2019). Since managing privacy is difficult as well as important, customers may perceive greater trust in the expertise of online companies for managing their personal data (Mourey & Waldman, 2020). Other research also confirms this point: trust in online business positively affects perceived effectiveness of business privacy policies (Wang, 2019). However, this type of trust is not based on people totally comprehending how companies use personal data, but on corporate imagines that institutions want customers to believe in. In other words, customers do not have simple and effective options to choose whether or which data are collected, power over relevant information (Bornschein, Schmidt, & Maier, 2020), and they have not got the capability to

negotiate how companies use their data, but still they give credit companies that have a good reputation and image, and on this basis, they allow them to manage their data.

Feeling powerless about controlling data

When people are unable to control their personal data, they may develop frustrations about privacy. Many scholars have developed several notions to describe this situation confronted by the general public. Routine institutional practices encourage a sense of helplessness for people trying to control what institutions can know about them, and this situation can result in a sense of ‘digital resignation’ (Draper & Turow, 2019). In Draper and Turow’s research, 58% of participates exhibit features of ‘digital resignation’, and they have mainly two statements: “I want control over what marketers can learn about me” and “I’ve come to accept that I have little control over what marketers can learn about me” (Draper & Turow, 2019). Digital resignation refers to individuals, not the collective, leaving people indecisive and frustrated. They worry about how companies are using digital data, but as individuals, they cannot cope with the situation, which also reduces the chance of collective resistance.

Other researchers have arrived at similar conclusions. Surveillance apathy means that, “as there is no avoiding these systems and not much one can do about them, why consciously worry about them?” (Ellis, 2020). This perception does not necessarily mean that people are not interested in managing privacy, but rather it is a rational response to undesirable affects, feelings and emotions because of the futility of not being able to cope with it (Ellis, 2020). Another author used the concept of ‘rational fatalism’ as a theoretical framework to explain the fact that those who think they cannot manage the data flow by themselves are less likely to take action to protect privacy online, even when they know the potential risks of sharing personal data (Xie, Fowler-Dawson, & Tvauri, 2019).

This kind of response suggests that people think it is evitable to project some personal information to enjoy certain online services, although they are worrying about consequence of privacy risks referring to online harassment, and harm to employment, marriage and so on. Those possible risks seem so remote to everyday life, and the desire for using those services is so instant, that people feel it is futile to manage their data. A case study of WeChat, the dominant social media platform in China, found

similar results about powerlessness. A study found that Wechat has become an essential part of modern social communication, and people feel a decline in their sense of freedom and the right to privacy, but they cannot abandon the platform, as their social connections are heavily connected through it (Chen & Cheung, 2018). Doubting the reliability of cost-benefit privacy calculus model in another empirical research, when participates were asked how they perceived privacy on SNS, they responded that privacy violation as inevitable and social media use is necessary (Marwick & Hargittai, 2019).

Conclusions

Overall, through the systematic review, we can see that in principle, what people perceive as privacy is about how they understand the line between public and private in different contexts. However, in reality, people can hardly gain the autonomy by themselves, and the society has various forces that mitigate self-decisiveness. The general perception of privacy is about the appropriateness of social networks seeing certain information, while overlooking the very existence of institutions including digital companies that offer platform services. On the other hand, as people are using online services, those personal information become the resource for trading benefits. Nothing is completely free. This tendency may be promoted or exploited by digital media companies, which are very distant from the everyday lives of users. Normal people can do nothing but follow the familiar pattern that you should provide information if you want to have the service. Because they feel powerless, they are unable to decide how and what data to offer, so they end up sharing it all.

Chapter 3.

Discourse analysis of TikTok's privacy policy

The systematic review presented in Chapter 2 showed how individuals regard privacy. This chapter presents the results of a discourse analysis of TikTok's privacy policy, which allows me to analyze the contradiction between TikTok privacy claims and individual privacy perceptions. The latter are presented in Chapter 4. Before presenting the discourse analysis, this chapter first introduces TikTok and its parent company, Bytedance.

Bytedance and TikTok

TikTok is a short form video application that encourages people to make less than 1 minute videos and share with other users through the platform. TikTok was founded by a Chinese high tech company called Bytedance owned by Zhang Yiming. Media outlets cited TikTok as the seventh most downloaded mobile application of the decade, and it is also the most-downloaded one on the i-Store in 2018 and 2019 (Wikimedia Foundation, 2020). The parent company, Bytedance, has many mobile products including Douyin, the Chinese version of TikTok, and all of them are based on algorithmic analysis of user data to feed users different contents. The business model of Bytedance is based on the sale of personalized advertisements which are also based on arithmetic analysis.

Artificial Intelligence plays a key role in the operation of TikTok's business, and it established the AI Lab that develops the technology to serve for company development. As the mission of the lab stated:

> "…the AI Lab's main research focus has been the development of innovative technologies that serve the purposes of ByteDance's content platforms…… The vast data and diverse application scenarios on our platforms enable us to continuously improving AI models and algorithms, and developing innovative products, with which we keep enhancing the user experience." (ByteDance, 2020).

From this statement, the significant role of AI technology can be seen evidently. While artificial intelligence relies heavily on the collection of huge data sets (Mazurek & Małagocka, 2019), TikTok is using a huge volume of raw data collected from users to run its own business.

Once a new user registers on the platform, TikTok starts to collect their data, ranging from meta data, chatting message, and contact phone number to user generated content and payment information. So, TikTok is trying all the avenues to collect data so that it can improve its internal AI technology, as well as exterior products and services. Furthermore, those data is not kept within the company, but can be shared with third parties, and those third parties can be direct marketing advertisers, research institutions, legal departments as well as other departments in the ByteDance group. Therefore, it is significant to scrutinize the privacy policy of TikTok and to see the privacy claim behind the official document. In this chapter, I present the results of discourse analysis, and to demonstrate what TikTok and Bytedance behind it try to perceive and use personal data.

Discourse analysis

Company attitudes and claims can be shown in their policies, as those documents are principles of company operations. The privacy regarded texts reflect mainly how companies try to grapple with consumers' privacy. However, the claims and attitudes cannot be understood thoroughly without seeing meanings and significance beneath surface of texts, and that is why I try to use discourse analysis as approach to do the research, as the methodology could guide me see the deep structure of those documents, and infer how companies like TikTok wish to use people's data collected in their own platforms. As described in the methods section in Chapter 1, in this analysis, I mainly use three tools: lexis, transitivity and modality (Mautner, 2008). These tools help me examine the official document from three perspectives. In terms of lexis, I choose privacy as core term, and alternatives to see how the document use it. With regard to transitivity, it is about 'who did what to whom'. And modality is to examine the attitude towards user privacy is assertive or abstract. By using these tools, TikTok's privacy claim can be read and interpreted.

Function based on personal data

As stated in ByteDance's privacy document, there are many ways to operate the platform by using personal data they have collected (ByteDance, 2020). TikTok's privacy policy indicates that the company will use personal data "to fulfill requests for services and internal operations", "to customize the content you see", "to send promotion materials", "to improve and develop platform", "to measure and understand the effectiveness of the advertising", and so on (ByteDance, 2020). Through those statements, it is clear that most of TikTok's functions rely on algorithmic analysis. Whether it is feeding users customized short form videos, sending promotional materials, or improving services, they will all be build upon personal data.

Personal data are the central privacy concern that ByteDance's privacy policy addresses. As indicated in chapter two, privacy is about individuals managing their personal information relative to particular situations. This policy does indicate that users can 'choose', 'manage' and 'delete' their information in the TikTok application, but the range of options or power to do this is limited. For example, the word 'manage' occurs in the document where TikTok suggests users can decide they can see certain personal ads in the application or not, while the word can be barely seen in other parts of the policy. Hence 'management' is limited to specific scenarios. The same happens with the word 'control'. The only place where 'control' appears refers to to user autonomy when it suggests several tools are provided to control who can view, comment and send messages to users (ByteDance, 2020).

Since TikTok's functions cannot be accessed by users without their granting TikTok use of their personal data, the privacy document indicates TikTok is using data once users 'choose' to provide their information and digital traces through the application (ByteDance, 2020). TikTok tries to explain what types of data are used to do what in the most parts of the policy, but many areas require further explanation, leaving more questions than clarifications. This means that the ability to truly 'choose' to share data is limited, because consent is not fully informed.

There are other words like 'disclose', 'protect' and 'security' that originally refer to self-decisiveness around privacy, but they are seldom used to suggest users are able to manage privacy in the application. Those words are used to indicate TikTok is able to secure the platform, share with third parties and cooperate with their own legal department if necessary by using personal data.

These observations about lexis and word choice reveal that TikTok does not care about users' ability to assert their own privacy. The company does not try to show how it can protect users data, but rather focuses on how it can make use of personal data. Although it offer some transparency by explaining how data functions on the platform, the fact that there is a lack of information about how individuals can protect their privacy is still problematic. If it does not explain approaches of protecting privacy in the privacy policy, there may be no other places for Tiktok to illuminate those approaches. And this suggests that TikTok, as well as its parent ByteDance, do the minimum to respect individual's personal data and privacy.

What worse is that users are not aware of the issue here and indulge in the pleasure created by themselves providing personal data. Once a user opens TikTok on their mobile phones, all the services they enjoy and all the content they encounter must have relation with data they have provided. Those customized feeds are more likely to attract user's interest, compared to not customized ones. If a user likes a certain video, this can make TikTok feed the same type of video to the user, which enhances the users' interest in the feed. In other words, people should allow TikTok to collect their data otherwise they cannot enjoy the services offered by the company. This given an impression to users that giving out data is essential to enjoy the TikTok services.

Since the whole is built upon arithmetic analysis and users are quite satisfied with the designs and feeds, the suggestion is that users will not question how TikTok is using their data. Most people will not think this mechanism of data collecting and analysis is problematic because it allows them to enjoy a customized entertainment feed. However, data is not only used to enhance video feeds. It is also used to target customers with customized promotional materials which generate advertising fees for ByteDance, which is ultimately a media company.

Use it or leave it

TikTok's privacy policy is published by ByteDance onto its official website, and the company can revise it from time to time. Generally speaking, this policy sets the guidelines for how TikTok with use personal data. The policy has three parts according to the regions where TikTok operates: the policy for the United States (US), a policy for the European Economic Area (EEA) and Switzerland, and a policy for other jurisdictions.

The three parts share similar contents but can vary slightly different according to different government laws. As what the policy is about, the US version says: “This Privacy Policy covers the experience we provide for users age 13 and over on our Platform.”, while the EEA and Switzerland version says:” This policy sets out the basis on which we process any personal data we collect from you, or that you provide to us.”, and the other version is “This policy explains our practices concerning the personal data we collect from you, or that you provide to us.” (ByteDance, 2020). Overall, the policy states what types of data they are collecting, how they use those data as well as what other parties might have access to those data.

After those quotes, the policy says that if someone does not agree with this document, then they should not use TikTok. This announcement reveals much about how TikTok treat’s user’s. Once you have agreed with this policy, TikTok has the “right” to manipulate data according to its willingness, whereas if you do not agree, as the document suggests, you cannot use the platform. This is arbitrary, leaving platform users less choices and power to control their own data.

TikTok does not supply enough tools for users to manage their personal data. In the US version of the policy it does say that you can manage third-party advertising preference in the settings, but none of the other places in the document shows other approaches to manage institutional privacy, implying that TikTok does not provide sufficient tools for users to manage their data. Throughout the policy, the most evident way for users to negotiate their data with TikTok is via the company’s email address: privacy@tiktok.com. Email is a popular but less efficient way to communicate, compared to some direct communication, such as instant messaging or phone. Using email to contact the company requires a user to spend more time and to have relevant previous knowledge, which many users may lack.

The policy also mentioned how to delete information from the platform, but people have to email TikTok and ask them to delete certain kinds of information. Furthermore, if user try to delete or disable cookies, some of the functionality of the service will be lost. These statements imply that there are barriers for platform users who wish to retrieve certain data, and the harder they try to delete those information, the more likely they will leave the TikTok service. It is also possible that when they try to delete data, they will get frustrated about the challenge of doing so, and may end up

simply leaving personal data on the company's servers. Those difficulties show that TikTok users cannot control their own data unless they choose to close the account.

Data as an asset

Throughout the policy document, TikTok regards privacy as its own asset more so than as an individual's right or a territorial responsibility. Through using the tool of transitivity, the analysis finds that TikTok is trying to explain more about how it can utilize data after user consent, instead of how it can protect user data. Once users consent to provide their data, TikTok is able to use data to do several things, which can be divided into three parts: advertising, improving customer services, and internal data analysis.

Advertising is considered one of the main revenue source, and TikTok can target audiences with customized advertisements and location-based advertisements based on user data analysis. Effectiveness of advertising is measured by TikTok as well. Advertisers want their promotions to target the right customers, and they need users' viewing data to improve advertising strategies and tactics. And at the same time, the more effective the advertising, the more fees TikTok can gain.

With regard to improving customer service and optimizing internal business operations, the data still plays a fundamental role. Supported by data analysis, TikTok can make sure content presented can meet users' specific interests. Hashtags and campaigns can gain large following on the platform. Data can also be used to improve internal operations including troubleshooting, improving algorithms and enhancing AI technology.

Since TikTok is a media application that feeds each user customized short-form videos, advertising fees are its main revenue resource, and the effectiveness of advertisements relies totally on data accuracy for targeting potential consumers. Furthermore, the effectiveness of targeting is a major advantage of arithmetic data analysis, as this technology allows companies to know a consumer from various perspectives and pinpoint their demands, as well as desires, to lure them into buying products. Therefore, those profile information, browsing and liking history, data collected from other platforms and so on becomes very profitable, because every user can be targeted as potential consumers.

The other two things relevant to data usage also suggest data has become a tool to organize, separate and manage users on the platform so that TikTok can deliver a high quality service. For example, when users run into technical issues and contact customer service, troubleshooting data provides precious feedback. The resulting improvement helps enforce the platform's overall effectiveness and attractiveness to users, making it more likely to attract users, and increasing its profile in society. Thus, these data are not just information consisting of bits, they are valuable assets to create revenue for the company.

Data is not only used within the company, but can be shared with other businesses and applications. Illustrated clearly in the privacy policy, data is shared with others for various purposes:

> "research, payment processing and transaction fulfillment, database maintenance, administering contests and special offers, technology services, deliveries, email deployment, advertising, analytics, measurement, data storage and hosting, disaster recovery, search engine optimization, marketing, and data processing." (ByteDance, 2020)

These business purposes include many business transactions which create value for the company, regardless of how data are being used specifically. But it is difficult for users to know how their personal data will be used. Even if a user notices that his or her data may be leveraged by the company, they cannot understand how TikTok is using data exactly, as they cannot grasp what terms like database maintenance and email deployment mean.

Another quote shows obviously how data is asset to the company:

> "In the event that we sell or buy any business or assets (whether a result of liquidation, bankruptcy or otherwise), in which case we will disclose your data to the prospective seller or buyer of such business or assets; or if we sell, buy, merge, are acquired by, or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets." (ByteDance, 2020)

Although people can see the statement in TikTok's privacy policy, they can barely do anything to protect data if TikTok is in the process of acquisition, merger or bankruptcy. As we know, calculating the value of a corporation is important to the processes of acquisition, merger or bankruptcy. For platform companies, data is regarded as a significant 'transferred asset' which tells us that data is also a core asset to develop the business.

Lack of transparency

While TikTok is trying to tell you how they are dealing with privacy, it generally uses an ambiguous tone when discussing its privacy protections. For example, if a person accesses third-party services on the platform, those third parties are probably collecting data. The modality used in the policy is relatively loose given expression like "may be able to collect information about you" or "they may notify your connections on the third-party services". This shows that TikTok is not sure about the actions of third parties, and it just predicts the collecting, as well as notification behavior can happen. Alternatively, TikTok's statements are broad and imprecise to create leeway for dealings with third party companies.

Speaking about the security of information transmission, the declaration also offers low modality: "Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, for example, by encryption, we cannot guarantee the security of your information transmitted via the Platform; any transmission is at your own risk." It is interesting to see that TikTok makes information sharing with third parties central to its business. In particular, users can log in to TikTok using Facebook or Twitter. However, once a data leak happens, TikTok says that "the transmission is at your own risk." This shows that TikTok will likely avoid taking responsibility if data breaches take place. Finally, TikTok tells its user that the third parties it shares information with can "use information to display advertisements tailored to users' interests, preferences and characteristics" but that TikTok is not responsible for the "privacy practices" of those companies.

Conclusion

Overall, data is a valuable asset in many ways, and it has a significant role for the business development of TikTok and ByteDance. As an application based on

arithmetic analysis, the major function of TikTok cannot operate without analyzing user data. Lexical analysis of the company's privacy policy indicates how TikTok leverages user data, but offers little guidance to users on how they can protect their privacy. In terms of transitivity, TikTok can share information with various third parties without clarifying the usage in detail. Therefore, TikTok, as well as its parent ByteDance, claim data as asset to develop the business rather than providing approaches to mitigate users' privacy concerns. This is the main modality that is presented by their privacy policy.

Chapter 4.

Contradictions

Generally speaking, while “the right to be left alone” was introduced decades ago, the concept of privacy become a public concern only recently. Initially, the right to privacy referred to physical distance from outsiders to people living in a private estate, and people has the right to keep their private things from being seen by others. For example, sexual relationships would be considered a bedroom secret, and anyone who learned about the details of such activities would have violated the right to privacy of the people involved.

However, nowadays, physical private space is invaded by digital technology to a large extent. Data left on mobile phones, laptops, wearable devices, and so on, can transmit data about your activities through the Internet. That data can reveal details about your persona, and could even be used to modify your behaviours. “The right to be left alone” is not suitable for describing the issue people encounter nowadays in terms of data extraction, prediction and modification, since personal secret space is shrinking as a result of advances in digital technology.

Privacy in relationships

Privacy harms cannot happen without context, but rather must happen in certain kinds of situations and relationships. Privacy exists in a three-way relation between a subject (A), a set of propositions, (B) and a set of individuals (C). Privacy exists when proposition B about subject A cannot be known by certain individuals C (Blaauw, 2013). This kind of relationship indicates that the infringement of privacy can only take place if this three-way relationship is damaged.

Applying this concept to the case of TikTok, privacy is about how individual users’ data should be known by companies like TikTok. To what extent can TikTok collect user data and how they can share data with others? How can user privacy be harmed by the collection of data? Given the analysis presented in Chapters 2 and 3, we can see that individuals and TikTok are in an unequal relationship. TikTok knows much about users than users know about TikTok, especially about how it leverages user data

for business purposes. Through its algorithm, TikTok can draw a user profile in seconds, but users can only get to know how their data can be operated through the very abstract words presented in privacy policy documents.

Furthermore, this unequal relationship can be uncovered by the benefits users received through using TikTok's platform. The instantaneous job that users take from TikTok's service makes them forget the potential privacy hazard this incur from using the platform, even if rationally they understand the potential for harm. The perceived risks of personal information leaks do not outweigh the decision to enjoy this service in the moment, suggesting that users have adopted relaxed privacy attitudes in the platform economy.

Owning privacy is about Subjectivity

As social media grow in popularity, privacy becomes more relevant to the management of social exposure. In other words, privacy becomes the means by which people manage who can know certain things, and who will be refused access to personal information. In this setting, privacy is more likely to move from managing physical distance to managing social distance. Whatever it is online or offline, managing information flows within their own social networks has a more significant bearing on people's perception of privacy, suggesting that privacy perception is turning from value-based to cognate-based (Quinn, Epstein, & Moon, 2019).

Managing information flow within people's own social networks is more about self-decisiveness and free of will, rather than the maintenance of a collective norm. What could be regarded as privacy to a person does not mostly rely on how they perceive themselves as a member of collective, but more likely about how they perceive themselves and manage information according to their own will. In other words, subjectivity has become closely tied to privacy management.

This means that subjectivity becomes tied to how we think about personhood, agency, and the importance of individual ownership of self (contributors, 2020). Although privacy has been argued to having social value, it has more to do with individual standing than societal cohesion. And we can see the concept of privacy tends to celebrate subjectivity and individualism rather than collectivity and social formation. It is

about human agency and individual dignity, allowing people themselves to decide what kinds of messages should be revealed to which people.

Furthermore, what can be considered privacy generally are topics like personal health, marriage and so on. Considering the origin of the concept: the right to be left alone, it is the right to protect information from outside invasion and to keep it in a personal space. Therefore, privacy as a part of subjectivity has at its core the idea of keeping away from public affairs. In other words, privacy does not position people as citizens, but instead, it positions people as individuals in their own personal space, managing their relationship to their social network. This kind of thinking echoes the idea that people care more about privacy when their personal information is exposed to people who have a relatively short social distance from them, whereas if the distance becomes longer, concern about privacy could decline (Bhatia & Breaux, 2018).

This means that the attribute of self-decisiveness in privacy is intertwined with personal access, information, behavior and so on, rather than the collective and community. It is the nature of privacy that subjectivity can be maintained and enhanced by controlling personal affairs, instead of public affairs.

Centralization of knowledge and freedom

The notion of “data banks” has been heavily discussed since the last century. A data bank makes individuals the mute subjects of organizations who gain validity and power by holding personal files and records (Igo, 2018). These data, extracted from general populations, start to distance individuals from their origins while strengthening their affiliation with institutions that know how to manage and run data banks, resulting in the growing power in those institutions themselves.

We can see ever more clearly the evolving nature of the “data bank” in contemporary society. Huge high-tech companies like TikTok, supported by researchers in its AI Lab, are able to collect digital information automatically from mobile devices, and with powerful algorithms and computational devices, those corporations can capture a person’s characteristics within seconds. Today’s data banks have more advanced technology which accelerates the process of data extraction making companies like TikTok the centers of knowledge gathering and power of our time. These institutions

have more freedom and capacity than the general public to leverage personal data as a source of power.

Technology development is always accompanied with enthusiasm. It is perhaps because it is motivated by the pressure of economic growth and political contests. Considering Silicon Valley, the distinctive place of computational innovation, things are moving so quickly that change is upon us before we have a chance to evaluate the implications (Zuboff, 2019). There is no doubt that artificial intelligence and big data have developed to a great extent, and such development is upheld by economic and political resources that serve the goal of market expansion. This technologically driven market expansion leaves societal problems in its wake to be solved, one of which is the privacy issue. On one hand, cutting-edge technologies truly help companies to grow, and they offer conveniences and economic benefits to society. But on the other hand, privacy concerns raise important considerations that need to be addressed. They raise questions about who is most likely to benefit from new innovations. States and corporate actors are enthusiastic about innovation and motivated to pursue new developments, while social problems are generally left for normal people and individuals to resolve. This suggests that corporate actors have more power over individuals in processes of socio-technical change.

While asymmetrical power relationships are reproduced, maintained and enhanced by accumulation through dispossession (Harvey, 2005), corporations are also centralizing data sets and putting in place measures that ensure their right to use that data. Persons who generate data are deprived of their own data, whereas data-intensive businesses become more and more able to leverage that data for profits. The centralization of data not only refers to knowledge, but also power. Once companies gain the power of handling data, they have more freedom than ever.

Contradiction

As discussed above, individual's efforts to draw a personal privacy boundary expresses their subjectivity. If there is a condition of so-called 'perfect privacy', the privacy can be only restored when organizations return all the data to the owner (Bennett, 2011). The 'perfect privacy' cannot be possible to gain in any circumstance, but it set a benchmark for measure how much human agency an individual can get in the

society. In other words, subjectivity can only be manifested a person's control over their own data, and how they use it to project their persona. But while on the one side personal data is the manifestation of subjectivity, on the other side is the centralization of knowledge and freedom.

Analysis of TikTok's privacy documents shows that the company aims to gaining access to user data because it sees that data as a potential asset. It wants to exercise the right to use personal data, while avoiding any responsibility when privacy hazards occur. Furthermore, TikTok establishes its position as a data manager, showing that TikTok is centralizing knowledge from user data to gain the freedom and power that comes from possess that data. Since TikTok is a typical example of how high tech companies operate in the data management setting, it is clear to see the contradiction lying between subjectivity and centralization in the context of privacy. People realize that data generated by and about them should be owned by themselves, whereas the trend is that increasing amounts and types of data are captured and processed by companies like TikTok.

As long as data is alienated from its original owner, and accumulation by dispossession (Harvey, 2005) is evident in the corporation operations of platform companies, there is no doubt that capitalism will be alive and thriving in the world. But the contradiction that allows capitalism to continue unabetted is not very evident. This is because the design of software and devices seem to cater to people's privacy needs by offering encryption solutions, and building brand image to gain trust from consumers. And the terms of consent are devised using tedious words that bored in seconds, which are presented in the moment when someone wants access to a new application, luring people to quickly accept so that they can gain the immediate enjoyment of using a new service. All those designs are trying to persuade individual to be comfortable with giving away their personal data.

Meanwhile, people are truly becoming less concerned about privacy even as we are becoming more exposed than at any other time in the history. This may be because people can enjoy massive amounts of entertainment and convenience online, and they do not really care about self-disclosure. Once they consent to what corporations wish them to offer, they can fulfill their desire to use applications, and any other online services, which no institutions in history could previous provide. It seems that people do

not care about giving out data as long as they are satisfied with the service. Another similar but different opinion is that they have to give out data so as to have the service, even if they do not want to. Both opinions about privacy have been indicated in the chapter two, and they shows the challenge of controlling personal data in reality, and suggests that this poses significant challenges to subjectivity in the digital age.

Overall, I am not here to say that companies should not collect any data from users, since those institutions still need to develop, and they will need some data about clients in order to offer services. Artificial intelligence, big data and cloud-based technologies are booming in today's era, and it is reasonable to expect that these technologies will be used to develop businesses. However, there should be a balance between collecting data and harming privacy, and evidently, the balance has not been realized so far. Bringing together the analysis presented in Chapters 2 and 3, we can clearly see that individual's subjectivity is threatened by todays' data management order. Surveillance has become a serious concern. Individuals should not forget or forgo the value of privacy, even when we are cultivated, convinced or deluded into doing so. Surveillance of individuals does not just reduce privacy. It can also affect their opportunities, life chances and lifestyle, and excessive surveillance also impact very nature of society (Bennett, 2011).

References

Bennett, C. J. (2011). In Defence of Privacy: The concept and the regime. Surveillance & Society, 485-496.

Berger, P. L., & Luckmann, T. (1967). The social construction of reality: A treatise in the sociology of knowledge. Garden City: Doubleday.

Bhatia, J., & Breaux, T. D. (2018). Empirical measurement of perceived privacy risk. ACM Transactions on Computer-Human Interaction, 1-47.

Blaauw, M. (2013). The epistemic account of privacy. Episteme, 167-177.

Bornschein, R., Schmidt, L., & Maier, E. (2020). The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. Journal of Public Policy and Marketing, 135-154.

Bucher, T. (2012, April 8). Algorithmic power and the threat of invisbility on Facebook. new media & society.

ByteDance. (2020). Home Page. Retrieved from ByteDance AI Lab: https://ailab.bytedance.com/

ByteDance. (2020, 2). Privacy Policy. Retrieved from TikTok Web site: https://www.tiktok.com/legal/privacy-policy?lang=zh_Hant

Chen, Z. T., & Cheung, M. (2018). Privacy perception and protection on Chinese social media: a case study of WeChat. Ethics and Information Technology, 279-289.

contributors, W. (2020, May 30). Subjectivity. Retrieved from Wikipedia, The Free Encyclopedia: https://en.wikipedia.org/wiki/Subjectivity

Cuofano, G. (2020). Tiktok business model. Retrieved from thefourweekmba: https://fourweekmba.com/tiktok-business-model/

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

Ellis, D. (2020). Techno-Securitisation of Everyday Life and Cultures of Surveillance-Apatheia. Science as Culture, 11-29.

Evjemo, B., Castejón-Martínez, H., & Akselsen, S. (2019). Trust trumps concern: findings from a seven-country study on consumer consent to 'digital native' vs. 'digital immigrant' service providers. Behaviour and Information Technology, 503-518.

Frik, A., & Mittone, L. (2019). Factors Influencing the Perception of Website Privacy Trustworthiness and Users' Purchasing Intentions: The Behavioral Economics Perspective. Journal of theoretical and applied electronic commerce research, 89-125.

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

Harvey, D. (2005). A Brief History of Neoliberalism. Oxford: Oxford University Press.

Igo, S. E. (2018). The Record Prison. In S. E. Igo, The Known Citizen：A History of Privacy in Modern America (pp. 221-264). Cambridge: Harvard University Press.

Jin, C. H. (2018). Self-concepts in cyber censorship awareness and privacy risk perceptions: What do cyber asylum-seekers have? Computers in Human Behavior, 379-389.

Lutz, C., & Ranzini, G. (2017). Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. Social Media and Society.

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. Information Communication and Society, 1697-1713.

Marx, K. (1887). Capital: Critque of Political Economy. Moscow: Progress Publishers.

Marx, K. (1887). The General Formula for Capital. In K. Marx, Capital: A Critique of Political Economy. Moscow: Progress Publishers,.

Mautner, G. (2008). Analyzing Newspapers, Magazines and Other Print Media. In G. Mautner, Qualitative Discourse Analysis in the Social Sciences (pp. 30-53).

Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. Journal of Management Analytics, 344-364.

Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2018). Stealing PINs via mobile sensors: actual risk versus user perception. International Journal of Information Security, 291-313.

Mosco, V. (2009). Commodification: Content, Audiences, Labor. In V. Mosco, The Political Economy of Communication (pp. 127-155). London: SAGE Publications Ltd.

Mourey, J. A., & Waldman, A. E. (2020). Past the Privacy Paradox: The Importance of Privacy Changes as a Function of Control and Complexity. Journal of the Association for Consumer Research, 162-180.

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media. Social Media and Society.

Quinn, K., Epstein, D., & Moon, B. (2019). We Care About Different Things: Non-Elite Conceptualizations of Social Media Privacy. Social Media and Society.

Sarikakis, K., & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. Social Media and Society.

Sarikakis, K., & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. Social Media and Society.

Siddaway, A. P. (2019). How to Do a Systematic Review : A Best Practice Guide for Conducting and Reporting Narrative Reviews , Meta-Syntheses. Annial Reviews, pp. 747-770.

Smythe, D. W. (1977). Communications: Blindspot of Western Marxism. Canadian Journal of Political and Society Theory, 1–28.

Teutsch, D., Masur, P. K., & Trepte, S. (2018). Privacy in Mediated and Nonmediated Interpersonal Communication: How Subjective Concepts and Situational Perceptions Influence Behaviors. Social Media and Society.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data Colonialism through Accumulation by Dispossession: New metaphors for daily data. Environment and Planning D: Society and Space, 990-1006.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media and Society, 141-161.

Vaidhyanathan, S. (2011). The Googlization of Us: Universal Surveillance and Infrastructural Imperialism. In S. Vaidhyanathan, The Googlization of Everything (pp. 82-115). Berkeley and Los Angeles: University of California Press.

Wang, E. S.-T. (2019). Role of Privacy Legislations and Online Business Brand Image in Consumer Perceptions of Online Privacy Risk. Journal of theoretical and applied electronic commerce research.

Wikimedia Foundation. (2020, July 17). TikTok. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/TikTok#Features_and_trends

Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. Behaviour and Information Technology, 742-759.

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

Appendix A

Systematic Review Searching Plan

Question for systematic review

What is the public perception of privacy towards companies who use their data for business in big data age?

Relevant search terms

- Privacy perception
- Institutional privacy
- Vertical privacy
- Privacy resignation
- Perception
- Privacy risk

Inclusion and exclusion criteria

- Research questions: What is the public perception of privacy towards companies who use their data for business in big data age?
- Definition: Privacy perceptions is about how public perceive the privacy relationship with companies who try to use their data for service as well as for benefits.
- Research design: empirical researches, including interview, questionnaires and so on.
- Participants: adult, and exclude specific kinds of people so as to know the general privacy perceptions
- Time frame: the last three years, as the latest articles analyzed by privacy paradox systematic reviews were published in or before 2017 (Gerber, 2018). Although the 2018 systematic review is about privacy paradox, it still has relevance with privacy perceptions, as that literature synthesize literatures about privacy concerns, attitudes, behaviors and so on. And mine can partly build on this one. Furthermore, the Cambridge Analytics Affair happened in 2018, which

brings much more attention of privacy in the context of big data. I set 2017 as the starting searching year to be a conservative way of getting more comprehensive results.