TikTok and Surveillance Capitalism:

A Survey of Users on Power Imbalances and Potential Harms

By

Boxi Chen

Supervisor: Dr. Sara Bannerman

A Major Research Paper/Project

Submitted to the Department of Communication Studies and Media Arts

in Partial Fulfillment of the Requirements

for the Degree

Master of Arts

in Communication Studies and Media Arts

McMaster University

Introduction

TikTok is developed by ByteDance, a Chinese company that has been suspected of "its links to the Chinese Communist Party" (Abraham, 2022). ByteDance's Chinese employees were reported to repeatedly access TikTok's U.S. database, which potentially "threaten the U.S. to ban the app" (White, 2022). The activities of TikTok conflict with "a corporate executive's sworn statement before the US Senate" (Tabac, 2022), and the security risks associated with TikTok escalated to become a national security issue. TikTok "emphasized that its data is stored in the U.S." (White, 2022), but the behaviours of China-based employees have posed severe security concerns. TikTok gathers crucial information that concerns the nation and even endangers national security; therefore, it is important to study TikTok's practices and any potential repercussions.

TikTok's data mining and related analysis require the use of personal data; TikTok collects various types of private information by employing algorithms and recording activities such as liking, commenting, and sharing. TikTok often requires users' authorization to use their private information. If users refuse to agree to TikTok's terms of use on information collection, they are unable to access TikTok. It means that when users obtain the right to use the service, they must unconditionally obey all the conditions that deprive users of their rights including consent to the collection of their private information.

Social media users may feel helpless about the lack of privacy protection on social media. While "people value their privacy as one of the top priorities" (McDonald & Cranor, 2010), many users have unwittingly exchanged their privacy for free social media services, leading to further unintended consequences. To some extent, consumers are required to give up privacy in exchange for free services under current social media business models, but that does not indicate that such behaviour is acceptable, nor does it mean that TikTok collecting users' private information is correct.

Are the users able to have full control over their personal data, and how unbalanced is the relationship that TikTok has established with its users? I hope my research will be able to find the answers to these questions. TikTok is a relatively new social media platform that has not been fully examined in the research literature; this project will contribute to the understanding of power relationships, data collection and usage, privacy policy, and privacy harms on TikTok, and encourage the public to value their privacy.

This research project uses survey research, posing a series of questions to investigate TikTok users' usage and perceptions of privacy, their comprehension of the privacy policy, the power imbalances between TikTok and its users, and the potential consequences of privacy infringement. This study shows that TikTok has built a severely unequal relationship with its users by incorporating unjust statements into legal agreements to limit its users' authority.

Many users are aware that the power dynamics on TikTok are imbalanced, yet they continue to engage in such connections.

This paper first provides a background of the literature, examining the definition of privacy, social media and privacy, big data and algorithms, TikTok's algorithm and use of data, TikTok's privacy policy and vulnerability of data, TikTok data collection and storage, and the potential harms of TikTok's uses of personal data; some of the criticisms that have been levelled against TikTok's use of data. This paper then outlines Shoshana Zuboff's work on surveillance capitalism to narrow the study's focus and specifies the particular viewpoints I use in evaluating and interpreting the research data. Through the lens of surveillance capitalism, this research contributes to the analysis of TikTok and the possible harm it causes to its users. After outlining the methodology and research questions of this study, I explain the results of the survey I conducted, reflecting on the responses received by drawing on the concept of surveillance capitalism. In conclusion, I argue that TikTok's privacy practices result in a number of potential harms, and I provide some possible recommendations for prospective social media regulation measures.

Literature Review

Defining Privacy

Privacy is a basic human need, it is "anthropologically and psychologically rooted in the sense of shame and the need for bodily integrity, personal space, and intimacy in interpersonal relationships" (Debatin, 2011). Privacy is the most

lasting societal challenge associated with information technologies, through profound technological innovations from advanced computers to "electronic devices, video and radio systems, and biometric identification equipment" (Nissenbaum, 2004).

Privacy is hard to define. It is "an ambiguous term, with definitions ranging from the right to be let alone (Warren & Brandeis, 1890, as cited in Bryce & Klang, 2009), to the development of personality (Stromholm, 1967, as cited in Bryce & Klang, 2009), to the right to control information about oneself" (Fried, 1970, as cited in Bryce & Klang, 2009). Defining personal information can be “a contradictory maze between what privacy regulators ascribe as personally identifiable, what individuals understand as identifiable, and what the companies operating themselves” consider needing legal protection (Parsons et al., 2015, as cited in Parsons, 2015).

Social Media and Privacy

Providing an appropriate level of privacy protection raises difficult questions in today’s social media environment. The control of privacy allows "individuals to selectively disclose personal information and engage in behaviours appropriate to and necessary for creating and maintaining diverse personal relationships" (Mooradian, 2009), but the loss of online privacy can "endanger most, if not all areas of our offline life, and thus appropriate online behaviour is important" (Bartsch & Dienlin, 2016). Although social media sites offer privacy tools to provide more autonomy for users to protect their privacy, these tools are

trivial against the erosion of privacy, and “that default privacy settings are the norm” (Fiesler et al., 2017), due to the fact that the privacy setting options are often difficult to understand.

Social media companies make use of many types of data. DeNardis & Hackl (2015) indicated that "private information such as names, email addresses, gender, and birth date are required on most social media networks" to establish social network profiles or ensure the accuracy and authenticity of information about their users. Although users' profiles may remain private, other private information such as "the friendship links and group affiliations are often visible to the public" (Zheleva & Getoor, 2009). Users are continuously monitored on "the basis of their metadata or, more broadly, their online data" (Raley, 2013; Van Dijck, 2014, as cited in Büchi et al., 2020). The mining of social media data can be used to gain "insights into the opinions, moods, networks, and relationships of ordinary social media users and key influencers" (Kennedy et al., 2017).

Because the data is so powerful, good data usage practices must be in place, and all parties should "collaborate to ensure the long-term success of data management" (Hashem, 2015) in a contemporary computing environment. However, there are several instances where TikTok has failed to maintain good data usage practices or to protect users' privacy. Badillo-Urquiola et al. (2019) indicated TikTok "violated the Children’s Online Privacy Protection Act (COPPA)” by unethically obtaining personal information from children under 13. Other than that, TikTok also failed to provide a “Privacy Policy in Dutch for Dutch users" (Tan

& Ta, 2021). Any collection of Dutch users' private data should be "concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular, the special protection children merit with regard to transparency and clear and plain language" (Autoriteit Persoonsgegevens, 2021, as cited in Tan & Ta, 2021), but TikTok failed to do so. Furthermore, TikTok has "sparked intense debates on privacy protection" (Su & Lu, 2021), and TikTok's "data mining practises imply more fundamental questions about the governance of our personal data" (Faison, 2021), prompting the public to reflect on the security risk that TikTok poses, as well as possible ways to regulate TikTok to prevent it from inflicting privacy harm.

Big Data and Algorithms

The term "big data" has become widely used with the glut of online information generated, and big data "is intertwined with considerable technical and socio-technical issues, and predominantly associated with two ideas: data storage and data analysis" (Ward & Barker, 2013). By enabling organizations to precisely identify the data that would provide useful insights about user behaviour, big data analysis has "unleashed new organizational capabilities and values" (Davenport et al., 2012). Smith et al. (2012) indicate that algorithmic big data processing becomes "a sociological problem when private information is collected by various parties."

Businesses and organizations collect data generated by their users to develop an understanding of the mass population, and "the data is often collected

with tools that communicate with the respective API (Application Programming Interface) of the social media platform, if one exists, and crawl the data" (Stieglitz et al., 2018). With the users' active engagement on social media platforms, personalized recommendation systems have been developed and applied by platforms to "overcome the information overload problem and easily collect useful information that fulfil people's requirements and interests" (Cui et al., 2017).

Algorithms are an integral part of many social media platforms. Algorithms on social media have the ability to "direct users' attention" (Bannerman, p. 240, 2020) and are used to "filter, arrange, and customize information based on user data" (Milan, 2015) that have considerably aided corporations in identifying the most valuable data traces to generate unique datasets. "Each TikTok user will receive a completely personalized video feed based on the match between their own personalities, content labels, and the characteristics of their environment" (Zhao, 2021), as recommended by the algorithm. TikTok applies such "AI-based algorithms to analyze its users' behaviour and deliver content, as opposed to simply making recommendations" (Davis, 2019). The tremendous amount of online user-generated data can be used to enrich user content by "analyzing a user's relationships and other sensitive and private information" (Beigi & Liu, 2020), as well as " to accurately recommend videos that users are interested in" (Zhang & Liu, 2021).

TikTok's Algorithm and Data Uses:

TikTok is a private platform that is ruled and governed by its owner. TikTok's success is "due in significant part to its innovative recommendation system" (Chan, 2018).

TikTok's powerful recommendation mechanism delivers precise promotion for commercial profit activities and has helped TikTok data "expand by 21.4 percent in 2019 and has defeated other social media platforms like Facebook and YouTube" (Huang, 2021). Its video feed "for viewing entertainment is a continuous stream, never-ending thanks to artificial intelligence that provides tailored entertainment based on collected user data" (Jacqueline, 2020). "Product positioning, content variety, and uniqueness" (Hou, 2018) are key features that contribute to TikTok's current popularity. The recommendation system is "foreseen to be one of the most important services that can provide personalized multimedia content to users" (Wang, et al., 2013), and "individuals' excessive participation in social media is exacerbated by the usage of a recommendation system and a lack of self-control" (Su et al., 2021).

TikTok's recommendation algorithm relies on the capture of huge amounts of data. It uses "real-time training and learning from features such as the correlation between content and user information, user behaviour, and trends" (Wang, 2020, as cited in Gray, 2021). Omar & Dequan (2020, as cited in Masciantonio et al., 2021) suggested that TikTok is seen as a "recording tool rather than a social media app" that constantly collects sensitive information as well as empowers users to self-document. Users recognize "the recording and

sharing culture" (Du et al., 2020) on TikTok, and they freely capture and share their personal lives.

The willingness of users to engage on social media have posed threats to their privacy. Privacy of personal communication offers people the opportunity to "communicate without being intercepted and the capacity to be able to control which personal information is exposed to whom" (Plank, 2022). However, users are unable to guarantee their privacy due to the volume of private information TikTok collects and their willingness to self disclose.

Social media uses analyzed data for various purposes that may lead to privacy consequences. The data can be used to “identify or categorize individuals and predict their behaviour” (Monteiro, 2021), and private information "is accessed, stored, manipulated, data-mined, shared, bought and sold, analyzed and potentially lost, stolen or misused by countless parties, often without our knowledge or consent" (Buchanan et al., 2006). “The unprecedented availability of individuals’ personal information, data, behaviour, communication, and transactions" (Büchi, 2016) has sparked substantial debate and study into the concerns associated with loss of privacy, privacy invasions, and surveillance. People may lose control of their privacy due to their active engagement in social media activities, as their private information is “monitored and assembled into data packages, and these packages are sold and shared between big commercial platforms” (Brousseau & Penard, 2007).

As users become more accustomed to online life, their digital profiles become more sophisticated. People have become "so accustomed to sharing our thoughts on products, writing blogs, and answering polls about our political preferences that they seldom even think twice before posting all kinds of information that used to be private" (Nolan & Wilson, 2015). They "appear to be comfortable living a part of their lives openly and freely through online networks, often oblivious to the risks" (Rosenblum, 2007, as cited in O'Brien & Torres, 2012) of the excessive number of online interactions. Richards (2021) indicated that TikTok's algorithms effectively “forecast our preferences, target us with consumer goods, and then share these predictions with third parties, users are trapped in a world of surveillance and life as a commodified product." Individuals are also exposed to potential liability due to "the availability of data sets that can be used to re-identify personal information" (Office of the Privacy Commissioner of Canada, 2017). Unfortunately, Capers (2021) disclosed that "it is virtually impossible to totally remove personal information from internet sites." However, by enhancing privacy settings to lessen the occurrence of digital traces, the chance of private information being compromised can be decreased.

Advertising is one of the main reasons that social media companies such as TikTok are desperate for private data, and "the digital era is significantly increasing advertising and the use of data for sales purposes; online advertising space is expanding, and much of this expansion is propelled by social media" (Ruckenstein & Granroth, 2019). The new advertising strategy on TikTok "has the

persuasive elements that influence consumers' attitudes and behaviours" (Han, 2020), and Tang (2019) suggested that the way that TikTok "combines short video and interesting entertainment with aesthetics" leads to its success.

Overall, the algorithm plays an important role in TikTok's operation. Ma and Hu (2021) indicated that "TikTok touted the algorithm as computer vision to extract and categorize visual information" such as images and videos that rely on users' behaviours and interests, and TikTok achieves its power "on commercial monetization, content distribution, and acquisition of data sources through its infrastructural ambition of building a 'video encyclopedia' that can be salable, ranked, and archived" (Zhang, 2020).

TikTok's Privacy Policy and Vulnerability of Data:

Legal agreements are typically used by social media networks to establish relationships with users. The agreement "manifests the intent of the contracting parties to deal with particular contingencies in particular ways" (Spann, p. 233, 1989), and it requires theoretical mutual consent from both parties. Social media platforms offer agreements that "users must agree and comply to engage in social networking" (Bianco, p. 308, 2009), but the complexity of the agreements challenges the users' ability to understand or consent. Zagar and Poljak (2015) revealed that social media companies are constantly altering their legal agreements to distribute the resources that each user has access to and embed the "hierarchical relationship implicit in the opposition that has been specified, grounding the hierarchy in its policy justifications" (Spann, p. 232, 1989).

. The public cares deeply about their privacy online, but those sensitivities have been ill-served by technology companies that stand to profit" (Madden, 2012). Social media users “engage in virtual space where they have contractual agreements that govern their usage of the services” (Kutler, 2011), but social media companies "normally do not expect their consumers to comprehend or even read the legal agreements" (Barnes, p. 665, 2011). Xue (2020) indicated that “TikTok leverages user data, but offers little guidance to users on how they can protect their privacy,” and Steinfeld (2016) further suggested that “if users have the option of accepting legal terms and conditions without reading a policy, they will generally forgo reading the document,” and “users largely give in to the TikTok tradeoff, meaning they do not consider but rather tolerate the app’s privacy policy in return for favourable user experiences and beneficial content” (De Los Santos & Klug, 2021).

TikTok provides users with complicated and lengthy legal agreements. TikTok users generally "take 31.4 minutes for users to read TikTok’s Terms of Service" (Nahmias et al., p. 410, 2020), and the Terms of Service is only one of the legal agreements that users have to examine. Social media services, including TikTok, take advantage of their users by providing broad and vague agreement. The legal agreement “does not specify why TikTok needs this data. Nor does it explain how it would go about seeking the required permission from users" (TPerez, 2021). Users would typically be overwhelmed by the length and complex texts of the legal policies due to the reason they "tend to be very

complicated" (Obar, 2022). Obar & Oeldorf-Hirsch (2018) indicated that "I have read and agree that the terms are the biggest lie on the web.” Users are influenced by "the colourful, bold, prominently displayed join button and the small format of the legal agreements, which make users feel that reading the terms of service seems like a waste of time" (Obar & Oeldorf-Hirsch, 2018). "Gender, education, ethnic background, and age" (Hofstra et al., 2016) are other the factors that may affect users' understanding of privacy agreements; users are "hindered by the clear lack of conceptual clarity in the platform's legal agreements" (Gorwa & Guilbeault, 2020) and “also lack the knowledge of the agreements to comprehend the dangers of utilizing social media services” (Livingston, p.627, 2011).

The contemporary internet policies commonly consist of pitfalls, and social media platforms generally offer the “clickwrap agreement,” which is a "digital prompt that facilitates consent or circumvents consent materials by affording users the opportunity to quickly accept or reject digital media policies" (Obar & Oeldorf-Hirsch, 2018). People often click "agree before accessing, reading, and understanding digital service policies, and the length of terms of service and privacy policies may be contributing to these policies’ ignoring behaviours" (Obar & Oeldorf-Hirsch, 2018, as cited in Obar, 2022).

It seems that users are unable to protect themselves from privacy violations. Cocozza (p.365, 2014) raised an interesting question:" How much control over personal freedom users must give up to access and participate in a

world steeped in social media?" The "power imbalance between the user and the service provider in the regulative change process is a step in the wrong direction" (Bechmann, 2014). However, the contemporary social media ecosystem is still continuing on the same erroneous path by embedding unequal and unfair statements in agreements to exacerbate power disparities.

TikTok Data Collection and Storage

Private data can be considered a valuable resource, as Sherman (2022) described it, "TikTok is disguised as a social media that purposefully gathers user data." When data mining occurs on TikTok, it "may raise privacy issues as users' details are generally disclosed and monitored, but no one is certain how TikTok uses collected data" (Omisola, 2022). "The recommendation system is a proprietary technology that helps make each social network unique, and TikTok without exception kept its algorithms secret" (Newberry, 2022). TikTok also collects controversial data, such as "unique biometrics and personal digital replicas of appearance, behaviour, and expression, and such data is comparable to fingerprints as they can help others identify, surveil, and profile people of interest" (Wouters & Paterson, 2022). Furthermore, Neyaz (2020) disclosed TikTok may share information with “various third parties without clarifying the usage in detail and does not encrypt the videos and thumbnails while transferring it from senders to receivers,” which makes private information become vulnerable. Users' privacy concerns are exacerbated by uncertainty and unknown platform behaviour, yet there is no practical approach to mitigate such issues.

Privacy is "an ever-evolving, locally-constructed phenomenon" (Abukhodair & Vieweg, 2016), but current "regulation and institutional efforts are not enough to protect online users from online privacy incidents" (Chai et al., 2009).

Technology provides social platforms with the possibility of endlessly storing private data; thus, further promoting the idea that once users enter the online spaces, their digital behaviours are constantly being recorded and stored, and "the deletion of online information is difficult to apply in practice" (Weber, 2011). The inability to delete private data keeps users trapped in the online world, and the collected data "may be crawled and utilized for a variety of purposes, including user/usage profiling and behaviour prediction" (Mitrou, 2014) that further possibly leads to privacy concerns.

The Potential Harms of TikTok's Uses of Personal Data:

There are many consequences involved with TikTok's data practices. Obar and Mcphail (2018) indicated "big data-driven automated decision-making expands and exacerbates discrimination, making us all susceptible to inaccuracies, illegalities, and injustices." TikTok algorithms accompany tailoring content to "categorize users on the app into various identities, articulating what it means to be of a certain social identity, and actively suppressing content related to marginalized social identities" (Karizat et al., 2021). Simpson & Semaan's study (2021) found that "TikTok's For You Page algorithm constructs contradictory identity spaces," that both support marginalized groups and also transgress and violate the identities of these users, and individuals who are

viewed as “too unattractive, poor, or disabled” (Boffone, p. 29, 2021) are often discriminated against. The content that is created by individuals who belong to such communities is often demoted, which reinforces the idea that TikTok has the authority to restrict or eliminate any subordinate groups.

TikTok was not promoting personal diversity, and it has admitted to "shadow-banning or otherwise suppressing content created by people from LGBTQ+ communities, intersex, fat, disabled, and racialized people" (MacKinnon, 2021), and such actions deprive them of their basic rights as well as show "the discriminatory potential of algorithmic decision-making, as well as the law's inability to confront prejudice in the complicated domain of algorithms" (Selmi, p. 615, 2021).

TikTok secretly collects data from all populations, it was also “accused of collecting children's personal information, such as their phone numbers, exact locations, and biometric data, without the consent or knowledge of the children or their parents" (Altuglu et al., 2022). Harriger et al. (2022) revealed that TikTok is "aware of the harm and negative impact posed by their implementation of social media products and algorithms, particularly on the mental health and body image of young, vulnerable users." Youngsters are unconsciously influenced by social media algorithms, and Albrechtslund (2008) further argued that they apparently need to be “trained in a code of conduct with regards to online activities to learn how to protect themselves.”

Most users are often unaware of the potential implications of TikTok's data collection. Roth et al.'s (2021) study showed that if the TikTok users "had known about the potential harm, they would not have engaged in certain online activities." TikTok users "are often young" (Montag et al., 2021) between the ages of "20-29" (Yang et al., 2019), but Ellis et al. (2022) revealed that "young people were not concerned about privacy and security in general, or that any apps on their smartphones could track their location." TikTok is mainly used by young individuals, which further leads such a population to become more vulnerable to potential harm.

There are many online harms involved in data collection, and online harms are “often repetitive, permanent, searchable, widely shared, and cumulative, resulting in an amplification of injury” (Liane & Cooper, 2021). Other possible consequences include “identity theft, financial loss, and information loss” (He, 2013) as a result of social media platforms' abusive usage and sharing of data. A person’s digital dossier can betray them in the physical world, resulting in harms like “the denial or loss of employment, shame and embarrassment, denigration of reputation, or merely exposure in an unwanted light, and the only way to control the dossier or reverse the caused harm is to participate actively in shaping it, rather than renounce entirely online participation" (Sánchez Abril et al., 2012). Users appear to be imprisoned in the online world once they consent to enter it; additionally, the strategies employed by “social networking have resulted in user confusion as to what information is accessible to the public, thus exposing them

to an unnecessary risk of harm" (Powell, 2011). "It is important to take into consideration the perception of privacy held by the individuals using the site" (Hudson & Bruckman, 2004; Bowker and Tuffin, 2004; Elgesem, 2002, as cited in Merriman, 2014) as social media platforms "can exert only limited control over user activities and cannot force users to exercise good judgment" (Koohikamali et al., 2017).

The governmental legal provisions could regulate the behaviour of social platforms to a certain extent, but Zenone et al. (2021) argue that “TikTok’s commercial and political activities still need to be monitored to ensure accountability of its platform and actions.” Tan and Ta (2021) suggested that “the collection or processing of personal data should be a “concise, transparent, intelligible, easily accessible form, and should be stated in clear and plain language.” This would further grant users more autonomy over their private data and reduce the possibility of potential harm.

Theoretical Framework

Zuboff (p. 11, 2019) introduced the concept of surveillance capitalism, which refers to an economic system centred on the commodification of personal data, and its core purpose is profit. Surveillance capitalism translates online interactions into behavioural data (Zuboff, p. 13, 2020) and it functions through extraordinary disparities in power and information (Zuboff, p. 16, 2020). In the digital environment, surveillance capitalists seize power and control, promising the appeal of boundless information and countless ways to anticipate our

demands and alleviate the problems of our busy lives (Zuboff, p. 41, 2020). Under this new system, the very instant that our demands are satisfied is the exact moment that our privacy is being taken away for behavioural data and the economic benefit of surveillance capitalists.' (Zuboff, p. 41, 2020).

In the context of surveillance capitalism, social media companies are composed of unanticipated and sometimes undetectable systems of extraction, commodification, and control that successfully isolate people from their own behaviour while creating new markets for behavioural prediction and modification (Zuboff, p. 75, 2015). The user's digital persona is continually being improved as a result of data mining by the technology company. Whether it is because users intentionally share, or because of the passive sharing of their electronic devices, companies are accurately learning the behaviours of these users to dominate the market and achieve profitability. Users provide their private information to social media businesses for free, and social media companies promptly collect such data to improve the effectiveness of their algorithms (Zuboff, p. 51, 2020).

The essence of capitalism is to plunder resources by abusing power, and surveillance capitalism originates in the act of “digital dispossession" (Zuboff, p. 71, 2020). The balance of power in surveillance capitalism is unachievable; if platforms and users aim to have more balanced relationships, “there would be financial risks and possibly ineffective for social media organizations to charge consumers for services " (Zuboff, p. 53, 2020). Surveillance capitalists' operations are hidden from the public view to exacerbate power disparities by relying on

behavioural data privatization and gathering to achieve the power of knowing everything about everyone. Individuals who use digital devices are subject to new types of control, and privacy violation becomes a predictable part of social inequality. Its defence demands a "reframing of privacy language, legislation, and judicial reasoning" (Zuboff, p. 127, 2020).

The utopian dream of surveillance capitalists is complete freedom. They do not wish "to be bound by the disciplines typically imposed by the private market realm of corporate governance or the democratic realm of law" (Zuboff, p. 71, 2020). Because such laws pose an existential danger to their operations, they strenuously push to abolish online privacy protection, limit regulations, weaken privacy-enhancing legislation, and resist every attempt to circumscribe their methods (Zuboff, p. 74, 2020).

Surveillance capitalist holds the ultimate power. The survival and success of surveillance capitalism depend upon “engineering collective agreement through all available means while simultaneously ignoring, evading, contesting, reshaping, or vanquishing laws that threaten free behavioural data” (Zuboff, p. 74, 2020). By providing cynically conveyed terms-of-service agreements with similarly obfuscated and opaque clauses, the surveillance capitalists claim the right to manage behavioural data and ignore considerations of "individuals' rights, interests, awareness, or comprehension" (Zuboff, p. 120, 2020). They also reinforce their authority, legitimacy, and power by "camouflaging their purpose

with illegible machine operations, sheltered secretive corporate practices, and mastering rhetorical misdirection in legal compliance" (Zuboff, p. 128, 2020).

The individuals who are willing to enter the social media spaces all must expect to be tracked and monitored in exchange for rewards such as “convenience, safety, and services” (Zuboff, p. 82, 2015). The privately administered system of surveillance capitalism is perpetuated by unilateral rights (Zuboff, p. 83, 2015), and surveillance capitalists exist in the absence of legitimate authority and are largely free from detection or sanction (Zuboff, p. 83, 2015). The users have to agree and obey the rules created by the social media owners to retain their status of being a community member and can not have unacceptable behaviours that challenge the sovereignty power; otherwise, they will be deprived of the right to use platform services.

The laws allow the surveillance capitalists to legalize the actions of invading and utilizing users' private information, and they apply the law to "advance their social goals by enticing the subordinate groups into legal strategies" (Lobel, p. 939, 2007). The law has created a power hierarchy that "protects capital owners and alienates subordinate people to ensure security and social order that permits capitalism to continue producing and exploiting" (Bannerman, p. 18, 2020). The exploitation of users by social media companies depends not only on the creation of laws by social platform owners, but also on how technology and power are possessed and used in the existing system. It is

crucial to investigate how unbalanced power dynamics exist in such a system and also discover the possible ways to restore equality on social media.

Knowledge Gap

Are users able to have full control over their personal data? Clearly, the answer to the question is no. TikTok has rarely been examined through the lens of surveillance capitalism and the harms it potentially brings on its users. Users typically forgo reading the privacy policy because its acceptance is a premise of accessing the free service, which further shows that TikTok is maintaining an unfair relationship with its users, but does not indicate how unbalanced relationships are. Faced with the challenge of big data to personal privacy information, users reluctantly upload their private information to the Internet, and their privacy is being invaded.

There is extensive research showing that TikTok's success is due to its algorithms, and the company implements the algorithms to collect private data for various purposes, such as advertising, to obtain economic benefits. All social platforms infringe on user privacy, and users are aware of privacy invasions such as private data collection, but they are unsure of what kind of data is being collected or used. Most TikTok users are teenagers and young adults, but they do not typically hold the perception of harm from abandoning their privacy. TikTok users may experience various harms as a result of the loss of privacy and excessive usage of TikTok, but have little idea about the potential consequences

that these harms could have on their offline lives. I hope my project contributes to the field of power relationships, data collection and usage, privacy policy, and privacy harms on TikTok, and further encourages the public to value their privacy.

Methodology

For the method for my research project, I carried out an evaluation of users' usage of TikTok. I used McMaster LimeSurvey as my survey platform. I recruited participants through online social media platforms; I joined relevant online communities (TikTok Canada, TikTok Growth Tips, and Best of TikTok) on Facebook to send out surveys. Since social media platforms such as Instagram, Twitter, and TikTok have a character limit, I shared a picture that consists of all of the necessary information and commented on any posts that are relevant to TikTok and privacy to allow potential participants to access the survey on those platforms. Another place that I recruited participants is through sub-forums (r/SampleSize, r/SurveyCircle, r/takemysurvey, etc.) on Reddit, which were great spaces to reach a large number of possible participants.

I received responses from 59 participants, and the participants were recruited by answering a list of screening questions to determine their age, location, language, and use of TikTok in order to verify their eligibility for the study. They also had to agree to the required forms such as a Letter of Information and a Consent Preamble to be qualified to participate in the research study. The survey would take approximately 10 minutes for the participants to complete, and the survey included both multiple-choice and short-answer

questions to test the usage of TikTok, the user's understanding of privacy, perceptions of the privacy policy, and possible harm from privacy invasions. Participants were given the opportunity to avoid any items that they were uncomfortable answering. The survey data was collected through the online survey platform in both quantitative and qualitative form, and I was responsible for analyzing the data using both statistical analysis and textual analysis.

A low survey response rate, trouble reaching potential participants, recruiting posters being removed by the online community moderator, and the Instagram recruitment account being blocked were some of the challenges encountered while doing this research. This study did not involve compensation to be awarded to the participants who participated in the survey. As a result, the individual's enthusiasm for this questionnaire was not high, and I was not able to receive 100 responses as I had expected. A number of 204 survey participants did not pass the screen questions, either because they are not TikTok users or because they are not from North America. The online world is composed of individuals with different characteristics and from different areas of the world, and the shortage of suitable participants might be another reason that completed survey responses were lower than expectations.

Furthermore, the recruitment posts that I published on those Facebook online communities were removed due to violating the rules established by the community administrator. I had to join other relevant online communities (Research Survey Filling, Survey Sharing, Survey Exchange, Surveys Focus

Group for Canada & US, Pls Do My Survey, Student Survey Exchange, and Research Survey Exchange Group) to recruit participants, but fortunately, the survey received enthusiastic responses in these communities. Lastly, Instagram has suspended my account for violating the platform's rules, and Instagram users are not permitted to publish survey recruiting postings. Nevertheless, because Instagram does not contain many social media and privacy-related topics and posts, I decided to abandon Instagram and concentrate my survey distribution efforts on TikTok, Facebook, and Reddit.

The purpose of this study is to answer the following research questions:

1) How unbalanced is the relationship that TikTok has established with its users?

2) Are TikTok users aware of the type of data being collected?

3) Are TikTok users aware of how TikTok uses their private data?

4) What are users' perceptions of the harm caused by the abandonment of privacy?

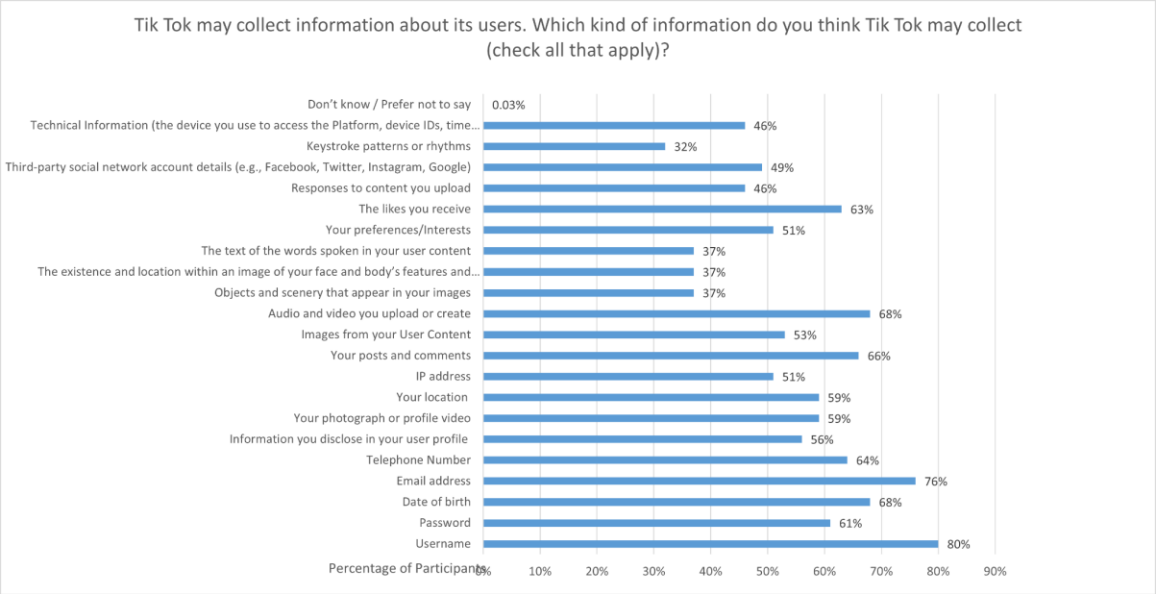
5) Have TikTok users experienced any kind of harm from TikTok's privacy invasions?

By finding answers to these research questions, I hope the research can lead people to understand the importance of privacy while simultaneously

allowing them to realize the consequences of not valuing their privacy. I believe there is an urgent need to regulate social media platforms' abusive use of user data; furthermore, the implementation of transparent data collection or usage could aid users in having a more power-balanced relationship with the platform.

Research Findings

After my survey was live for two weeks, the majority of responses came from Facebook, Reddit, and TikTok. However, the survey response on Twitter was not very encouraging, and it may be because my absence of Twitter followers makes me appear unreliable and leads people to believe that the survey is a fraud. Most participants identified themselves as females and males and are represented by White and Asian ethnic heritage. The majority of them fall into the age groups of 18 to 24 and 25 to 34 and typically hold at least undergraduate degrees. The majority of the participants were moderately addicted to TikTok, spending one to four hours every day on it. 56% of the participants use other short video apps with similar functions to TikTok, and the rest of the participants only use TikTok.

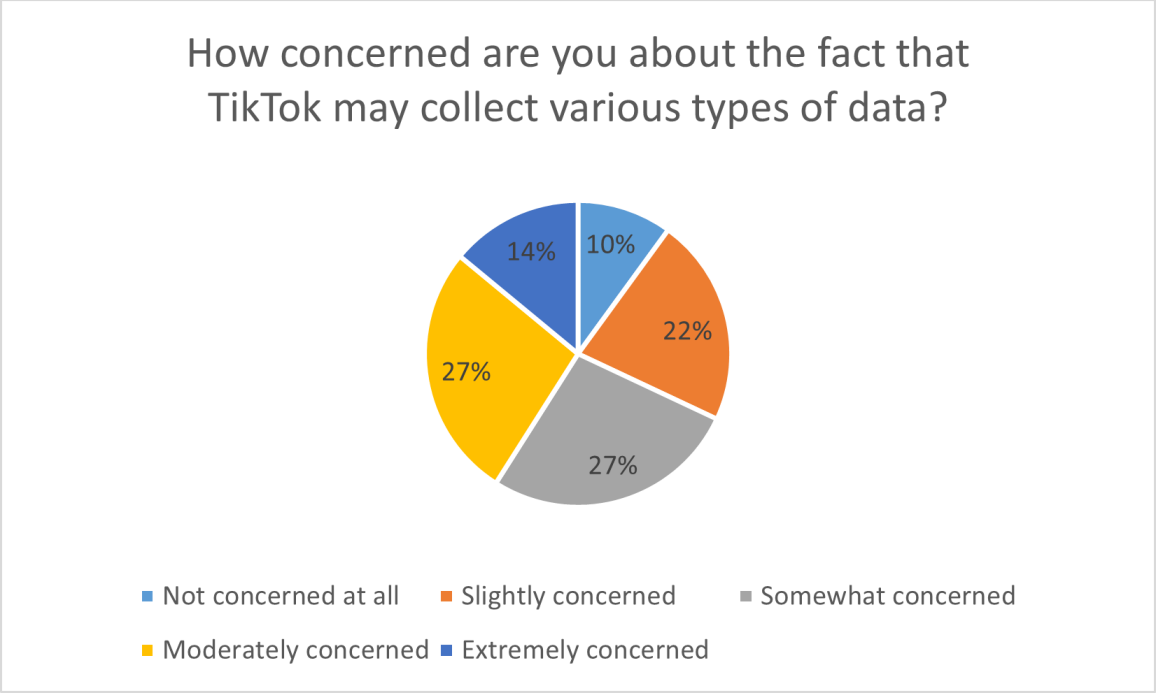


(Graph 1: Level of comprehension of the data collected by TikTok)

Most participants hold a decent degree of understanding about the types of private information that TikTok collects, but their understanding was not comprehensive enough. TikTok gathers "approximately 21 distinct categories of private information from its users" (Privacy Policy, 2022); however, objects and scenery that appear in user images, the existence and location within an image of users' faces and bodies' features and attributes, the text of the words spoken in user content, and keystroke patterns or rhythms were some common types of private information that many participants did not recognize.

TikTok collects an excessive variety of information, maybe going beyond what is necessary for service development, and further commercializes such data for revenue and privatization. The technologies and algorithms are designed to render our experiences into data and typically occur outside of our awareness and consent, and the social media services are like digital interfaces that make

users' experiences available to become “a continuous of raw-material supplies for surveillance capitalism” (Zuboff, p. 152, 2020). Indeed, my research confirms that, in many cases, fewer than half of participants are aware of the types of data that TikTok collects. Users have unintentionally provided too much personal information to the operators of social media platforms; as social platforms accumulate more personal data, the power of surveillance capitalists is maximized. The surveillance capitalists unabashedly assert their rights as “conquerors’ plunder by scraping and stockpiling our behaviour data” (Zuboff, p. 129, 2020), but users are powerless against such privacy exploitation and do not realize the type of data is being collected.



(Graph 2: Level of concern about TikTok’s collection of various types of data)

Participants were concerned about the fact that TikTok may have collected all of this information (Graph 1); 86 percent of participants were “slightly,” “somewhat,” “moderately,” or “extremely” concerned, and only 14 percent of participants are “not concerned at all.”

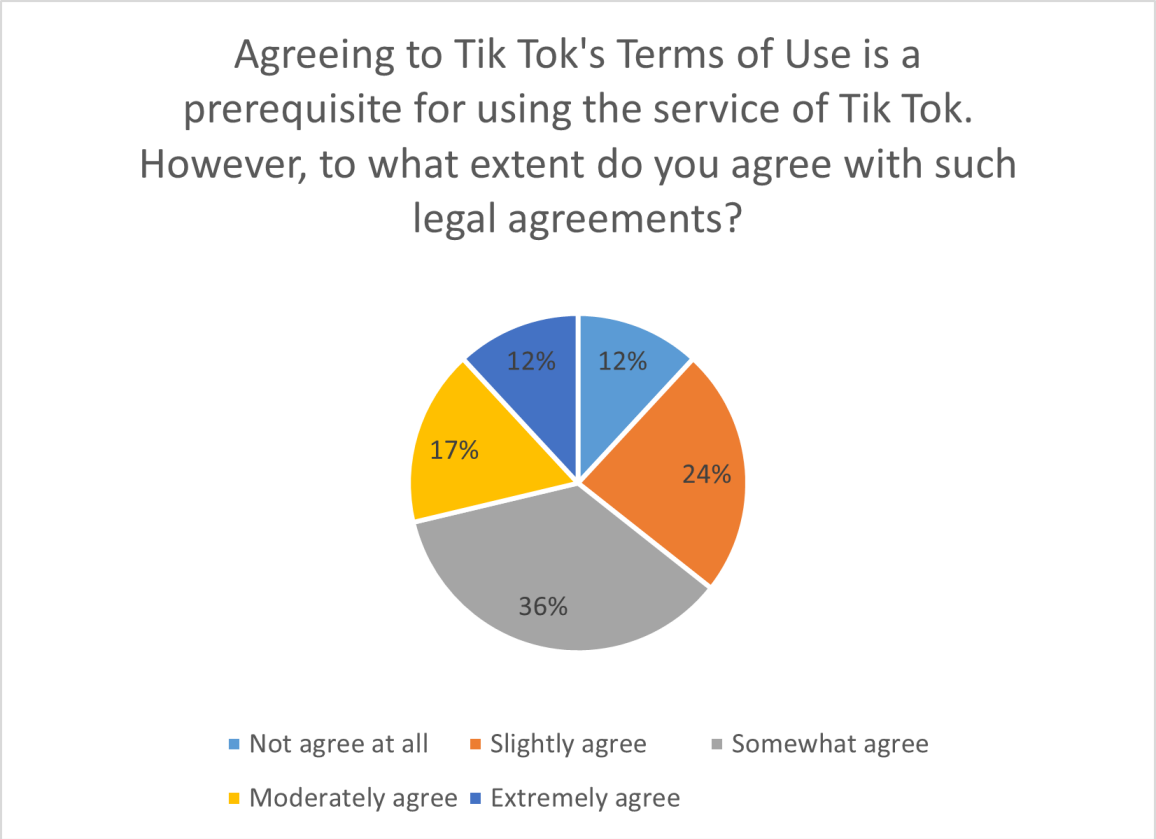
Despite privacy concerns, it is unclear if TikTok genuinely gathers personal information for the aim of service enhancements or whether such data collecting is required owing to the opaqueness of TikTok's data analysis techniques. Nonetheless, participants expressed satisfaction with the personalized video streams created by TikTok employing algorithms, demonstrating the effectiveness of the algorithms in accurately understanding user preferences based on data analysis.

TikTok largely controls what TikTok users watch on the platform. Users are less likely to watch videos outside of their video feed because of TikTok's strategy of creating individualized video streams for each user. Approximately 86% of the participants commonly agreed with the statement that "TikTok users are subject to TikTok's control and are compelled to watch only the videos TikTok wants them to watch while using TikTok." It indicates they acknowledge the unbalanced power relationship that exists on TikTok, but they continuously and actively engage in such power dynamics.

TikTok uses technology to analyze every inconspicuous detail to achieve the purpose of controlling user behaviour, and users have become accustomed to these behaviors. Surveillance capitalists have the ability to “change people’s

behaviour through carefully crafted and personalized content that resonates with them” (Zuboff, p. 178, 2020), and “personalization derives from prediction, and prediction derives from ever richer sources of behavioural data” (Zuboff, p. 178, 2020).

Users' future behaviour has been predetermined by the precision of the algorithms, and users trapped in the digital world due to the personal information that has been collected, analyzed, and cannot be erased. Zuboff (p. 164, 2020) disclosed that "the dark data continent of our inner life, our intentions and motives, meanings and needs, preferences and desires, moods and emotions, personality and disposition, truth-telling or deceit," is analyzed in creating personalized services and profit. “The mechanical intrusion behaviour of the surveillance capitalist is prosecuted under the banner of personalization" (Zuboff, p. 164, 2020), a term that can alleviate consumers' concerns about information collection while simultaneously masking the primary objective of data gathering. Even though some participants had found the reality behind the disguise, I argue they would still actively engage in such relationships due to their addiction and TikTok's powerful algorithms that reinforce the addictive behaviors.

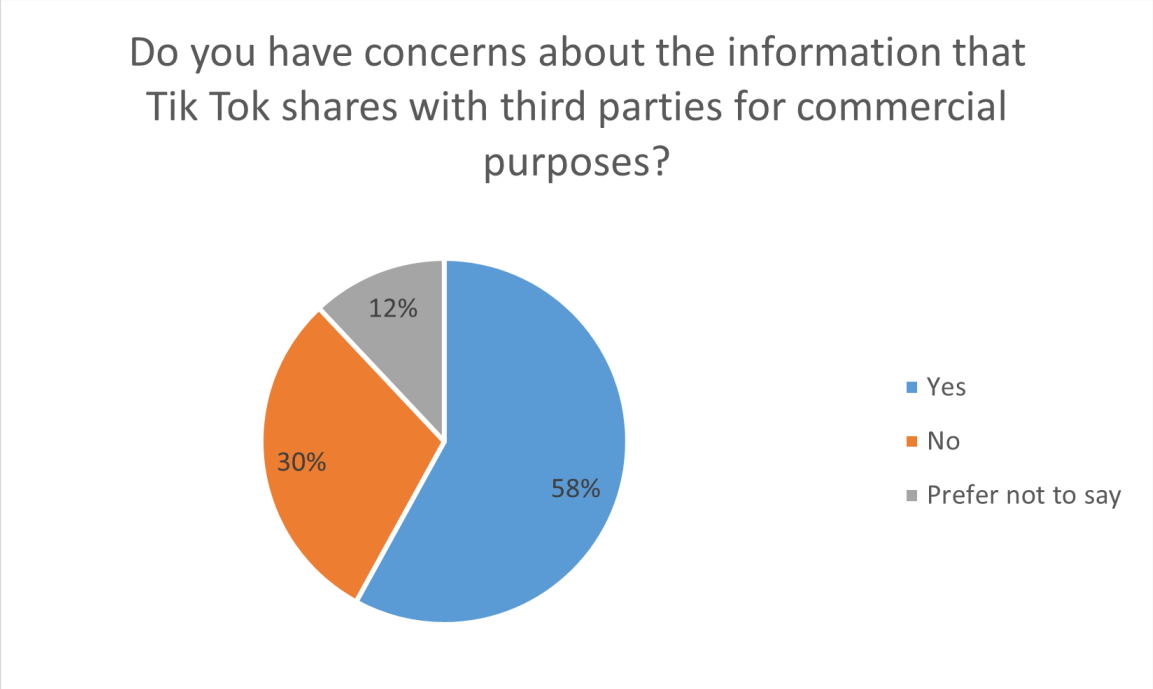


(Graph 3: Level of the agreement to TikTok's Terms of Use)

TikTok's Terms of Use is a prerequisite for using the service, but participants hold various extents of approval towards such legal agreements. The majority (60 percent) of participants agreed with TikTok's legal documents in a moderate way (slightly or somewhat). At the same time, only 12 percent fully or "extremely" agree indicating that most users do not totally agree with all of the statements made in the legal agreements. Should consent obtained in this way be considered valid? To be bound in a legal relationship, "both parties must consent" (Spann, p. 233, 1989), but making the thin consent of clicking "I agree"

a requirement to access the service appears to disregard the nature of true consent.

The implementation of take-it or leave-it conditions in such agreements has left the users with the choice of accepting the unfair terms and using the tempting costless services, and "the ubiquitous terms-of-service agreements are the most pernicious component" (Zuboff, p. 38, 2020). Similar to other platforms, TikTok employs "the usual onerous terms to obtain an affirmation of consent" (Zuboff, p. 153, 2020) to use users' private information; furthermore, the consequences of agreeing to such a type of agreement could include: "oppressive privacy and security consequences in which sensitive information is shared, third parties for the purposes of analysis and ultimately for trading in behavioural futures markets, and actions that ricochet back to the owner in the form of targeted ads" (Zuboff, p. 153, 2020). TikTok constantly invades the privacy of its users and hopes to obtain the legal authority to fully monopolize and control user information in order to fully advance its business objectives. The agreements support TikTok's owner, as a surveillance capitalist, establishing a contractual relationship, suppressing the users, and strengthening their power in the power dynamic by self-granting the right to manage users' data.



(Graph 4: Whether participants have concerns about the information that Tiktok shares with third parties)

Fifty-eight percent of the participants have concerns about the information that TikTok shares with third parties; nevertheless, owing to a lack of transparency, users are once again uninformed of how third parties or TikTok utilize their personal information.

Participants are somewhat divided in their views of TikTok's data collection and its relation to third party data sharing, but the majority (58 percent) of participants have concerns about TikTok sharing information with third parties (Graph 4).

According to participants' comments in their survey responses, many participants in the survey believe TikTok's collection of private data has greatly

invaded their privacy. One of the participants suggested that "TikTok seems to be a data collection service thinly veiled as a social network," while another indicated that TikTok "collects so much data that it's impossible to know whom they sell it to or what they use it for."

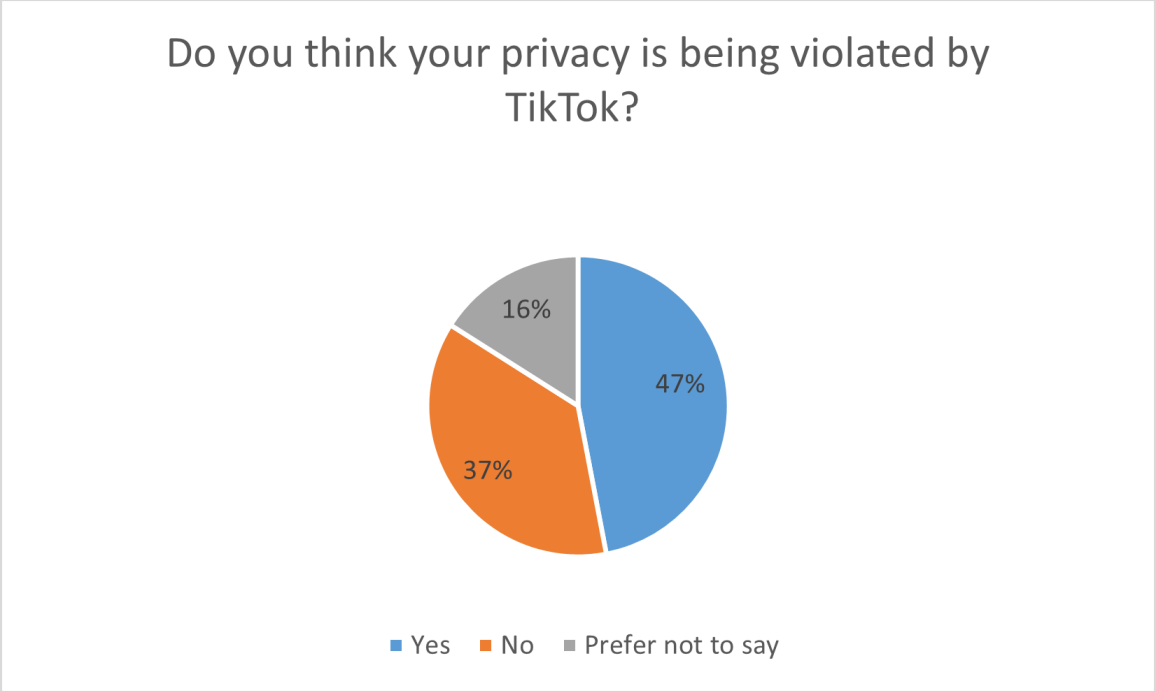
One participant also offered an amusing personal anecdote about how TikTok tracks what "they verbally discuss on the phone, and then relevant items may begin appearing on their TikTok page," which he and his friend discovered. Another participant stated that "China has a poor reputation for keeping information safe and private," and TikTok, as software from China, is very controversial. Furthermore, some participants were "concerned with how many unseen methods these applications are gathering data and whomever they are selling it to without their knowledge," which demonstrates that TikTok raised public concerns about privacy.

One respondent considered that "every application collects private data but offers no privacy protection in North America," which contributes to the idea of contemporary social media users being unable to defend their privacy. Certain participants also disclosed that they did not really care about their privacy or were happy with it as long as their information was not leaked; also, a few participants suggested that social media platforms must rely on profiting from private data to keep the platform running, and TikTok's collection of personal information has little impact on their daily lives.

Furthermore, another respondent stated that she is "very cautious with her online social media activities in order to avoid being targeted," therefore she is not too worried about her information being shared with third parties. She could see why some people are concerned about TikTok's data sharing and giving her privacy to TikTok and other social media causes her anxiety. She intended to be forgotten in the online world, but the digital traces she left behind and the information gathered about her made this impossible, as well as threatened her ability to preserve her anonymity.

Within the framework of surveillance capitalism, social media platforms aim for "ubiquitous intervention, action, control, and achieve their power by modifying real-time actions in the real world" (Zuboff, p. 187, 2020). The vast quantity of personal data gathered by TikTok advances its ability to forecast users' future actions, such as influencing users' real-life consumption patterns through individualized advertisements and videos. Many participants have acknowledged the control and intervention of TikTok are a result of infringing on their private lives and becoming cautious about privacy protection. However, the private data that social media platforms share with their third parties, has the possibility of "these third parties sharing with other third parties, and so on" (Zuboff, p. 161, 2020), leading to infinite and unpredictable consequences. The incompetence of users and the acquiescence of TikTok's privacy violations encouraged TikTok's unscrupulous behaviour; TikTok unreservedly trespasses

on the privacy of its users, but keeps its operations secret from the public, reflecting the extreme inequality of power.



(Graph 5: Whether participants think their privacy is being violated by TikTok)

Fifty-six percent of the respondents agreed that TikTok infringed on their privacy. However, there were opposing viewpoints that disagreed with statements that their privacy had been violated or their private information was not endangered. One respondent indicated that "he is fine with TikTok's algorithm using his actions on the platform to personalize his experience, but he does not agree with the action of TikTok collecting extra information on his phone or selling such information to third parties."

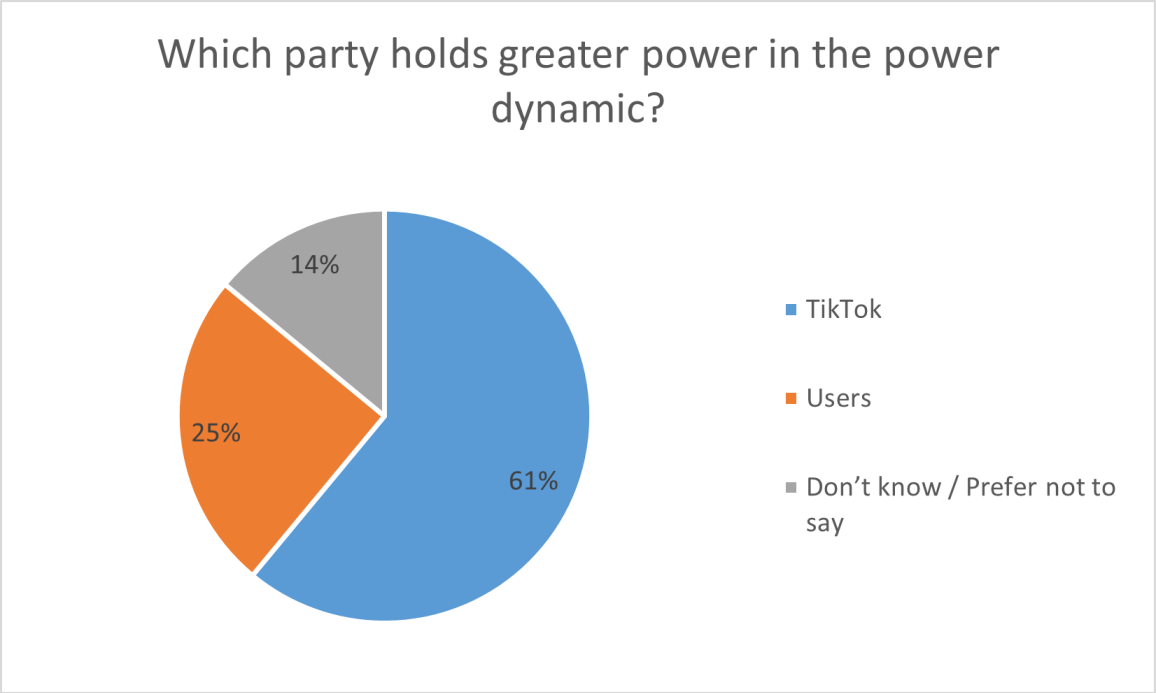
Furthermore, a few participants were horrified by the fact that TikTok knows about what they desire or that their behaviours have been discovered. TikTok collects too much information about its users, and it should not share the private information without "clearly stating what they will be sharing" or “with whom they will be sharing it.”

In addition, some respondents were fine with TikTok invading their privacy, but just worried about "personal data being stored without the knowledge of lots of people," and were concerned that “TikTok users could be potentially manipulated.” Zuboff (p. 284, 2020) disclosed that “individuals are easy prey to manipulation, with barely any defence against manipulation and exploitation." Without reading the agreements and entering the online spaces, which have become the norm, users give up their freedom once they choose to ignore the agreements without fully understanding the potential repercussions. Such behaviors indirectly contribute to the development of manipulation, and the “addictive nature of social media also plays an important role in supporting and breeding the manipulation of users” (Zuboff, p. 284, 2020). People use social media to socialize but are manipulated by power, influenced by privately personalized information. However, not many of them are willing to give up their use of social media, further resulting in the continuation of manipulation.

Lastly, forty-four percent of survey participants hold the perception that their privacy is not being invaded by TikTok, or even their private information is collected, it is safely stored and projected by TikTok. Although these participants

may not have been harmed by invasions of privacy and are unconcerned about TikTok's privacy protection, the rapid development of social media has made data-based privacy a far more complex issue. The data collected is not simply restricted to sharing within one party. Therefore, users should better protect themselves by strengthening their perceptions of privacy protection.

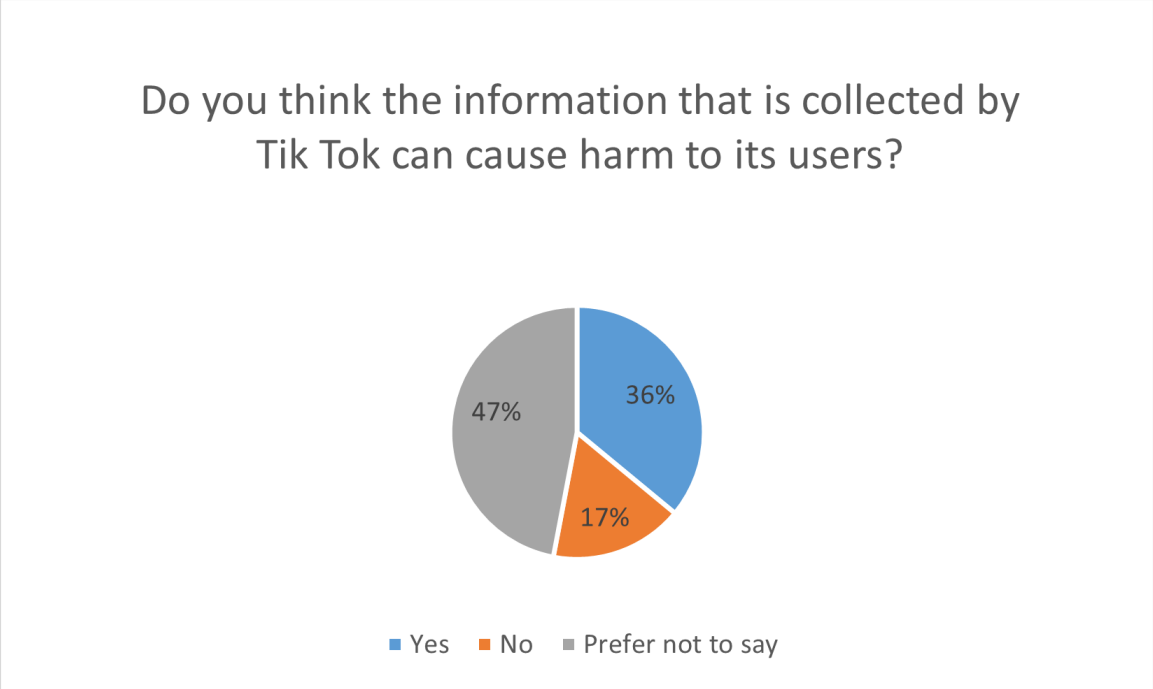
Even while some participants do not really think TikTok is compromising their privacy or are comfortable with it, they undoubtedly are a part of TikTok's data collection. TikTok has concealed its algorithms to silently obtain personal information by evading users' understanding and right to informed consent and manipulating their behaviour by displaying tailored content. TikTok, algorithms, and surveillance capitalism guarantee continued benefits by encouraging prolonged user engagement, and users unwittingly controlled by tailored content to work towards the maximum profitability of TikTok.



(Graph 6: Participant's perception of the power dynamic between TikTok and its users)

In the relationship between TikTok and its users, 71% of participants believed TikTok holds greater power than its users, which clearly shows that the majority of participants have acknowledged the unbalanced relationship. TikTok, under surveillance capitalism, operates through unprecedented asymmetries of knowledge and power, promoting rather than reducing social inequality. "Human consciousness itself is a threat to surveillance capitalism because awareness endangers the larger project of behaviour modification" (Zuboff, p. 196, 2020). TikTok is designed to keep users addicted to the streams of personalized content, and users unknowingly spend most of their free time generating vast amounts of exploitable data.

In order to fulfil users' demands, advanced algorithm technology not only accommodates users' viewing preferences but also stimulates their interest and ensures that users' desires can be satisfied. Senator Ervin (1974, as cited in Zuboff, p. 205, 2020) disclosed that behavioural modification techniques empower "one man to impose his views and values on others. Concepts of freedom, privacy, and self-determination inherently conflict with programmes designed to control not just physical freedom, but the source of free thought as well." TikTok and other algorithm-based platforms dream of ultimate control over users and their behaviour, and this excessive control breeds and reinforces even greater power disparities. Users' autonomy and privacy are gradually taken away while using social media, as they are unable to resist intrusions including control and exploitation, reinforcing the research finding that TikTok and its users have wildly unbalanced relationships.



(Graph 7: Participant's perception on whether TikTok can cause harm to its users)

Forty-seven percent of the participants do not know or prefer not to say whether the information that is collected by TikTok can actually cause harm to the users. A small portion of participants (17 percent) believed that TikTok is harmless, but 36% of the participants believed TikTok can cause harm by invading users' privacy. Respondents who said TikTok does not cause harm often think that the private information collected is really not precise enough to cause harm, or that similar private information is collected by all social media sites and still has not caused them any harm. Respondents with opposing viewpoints were frequently concerned about harms like social, political, discrimination, identification, harmful addiction, and data security on TikTok; and

what would happen if their personal information was hacked and ended up in the wrongful hands. The hackers would “expose the user's private life to the public or possibly sell it to the highest bidder who wants to buy such private data.”

Furthermore, one participant disclosed that she often encounters discrimination, which makes her feel a lack of validation of her body image on TikTok. It further indicates that the extensive involvement of TikTok's algorithm analysis affects users' perceptual body image and cognitive body image by constantly featuring such types of personalized content; In addition, users may feel frustrated about their body image by constantly comparing themselves to the perfect bodies shown in the videos.

Another participant has revealed that he has seen "religious/cult recruiting, pyramid schemes, and right-wing propaganda advertisements are rising "due to TikTok's ability to track and identify specific audiences. He is concerned that his private data could ever be leaked or sold to such organizations, and TikTok's algorithms could further trap users in self harm feeds." The users are not able to reset the algorithmic recommendation and further become vulnerable to "malicious actors looking to make money off of them or recruit them into abusive situations." Lastly, one participant raised one interesting point regarding the addictive nature of the algorithms and the addictive behaviour to TikTok, which could result in a decrease in “the quality of life and detract from everyday responsibilities and social connections in real life."

Forty-four percent of the participants believed that TikTok is not essential for work, employment, or career goals and 56% of the participants had opposing viewpoints and felt TikTok is important to some certain extent. TikTok is believed to be important in maintaining social relationships, although 34 percent of participants disagree. In terms of finding or maintaining romantic relationships, 65% of the participants suggested that TikTok is not important or slightly important in such relationships. Many participants did not spend money on TikTok to buy digital currencies or had ever cashed out the digital currencies. Exceptionally, 17% of the participants disclosed that they have spent money and cashed out the digital currencies on TikTok, which leads to the idea that TikTok could possibly become a money-making tool for users.

Forty-seven percent of the participants said they would lose nothing if they quit using TikTok, while 53% of the participants expressed that they would lose friendship, entertainment, happiness, and cultural knowledge. TikTok is a video-sharing network that lets users share the entertaining elements of their lives, which helps to strengthen social bonds. Participants may feel excluded during conversations since many people around them remain to use TikTok and discuss intriguing trends, implying that peer pressure is one of the key reasons why some individuals continue to use TikTok. A handful of the participants also mentioned that TikTok helps them stay informed about the current prevailing trends across the world and that it also helps them engage in real-life conversations or enhances their ability to "fit in" with their age group.

I argue that users have an addiction to TikTok despite the fact that TikTok is moderately essential to people's daily lives. Other social media platforms can also provide users with the services that TikTok offers, but why are users only keen on using TikTok? TikTok allows users to “get rid of boredom and monotonous time” (Kaur, 2020) and to "escape from realities and find a moment of gratification or satisfy the desire to socialize by allowing the users to show and share between friends" (Yang, 2020). "Self-expression, social connection, and escapism are important indicators of users’ TikTok usage” (Omar & Dequan. 2020), and TikTok further “manipulates the reach of user- generated content through algorithmic or regulatory means” (Zeng & Kaye, 2022) to encourage TikTok addiction in users.

Personalized content distribution strategies are intimately tied to people's addiction to TikTok. Surveillance capitalists aim “to consume the maximum possible amount of users’ time and consciousness and make users never have to look away" (Zuboff, p. 283, 2020). It is feasible to more accurately guess and forecast users' preferences by continually gathering private data and upgrading algorithms, which will further improve users' frequency of software usage and foster their continued attention and dependency. Although it does not appear that users must pay to use TikTok, social media has turned users' privacy and attention into commodities. The users have been "lured to the social mirror, their attention riveted by its dark charms of social comparison, social pressure, and social influence. As they fixate on the crowd, the technologically equipped

commercial harvesters circle quietly and cast their nets" (Zuboff, p. 292, 2020). I contend that users of technology frequently lose the ability to ponder and question, as well as the perception and resistance to possible danger, due to their naive optimism and dependency on it. Although technology has made our lives more efficient and convenient, we still need to free ourselves from the grip of surveillance capitalists to ensure our basic rights.

Overall, most participants felt their privacy was being invaded and thought that TikTok had maintained some kind of unbalanced relationship with them based on its legal agreements. They have to be controlled by TikTok in exchange for its free service, which includes being forced to view the personalized videos prepared by the algorithms. Many respondents were aware of some implications of TikTok's collection of private data and sharing of personal information, but were unaware of the full extent of the harm that such actions would cause. The majority of participants used TikTok as a source of amusement to pass the time, but they did not completely agree with TikTok's data practices or legal policies. Due to a lack of transparency with data practices and incapability in the power dynamic, users could not protect their privacy from being invaded.

Conclusion

From conducting the survey research, I am delighted that I have received enough responses that allow me to answer my research questions. TikTok has established a very imbalanced relationship with its users by embedding unfair statements in legal agreements in order to restrict the users' power. Many users

acknowledge the existence of such power dynamics, but they still insist on engaging in such relationships to sacrifice their privacy for purposes such as entertainment. Most users do agree that they are being compelled to watch personalized videos created by TikTok's algorithms, but they do not have the power to resist it other than by quitting the application completely. Users are moderately satisfied with TikTok's legal agreements and also moderately concerned about the privacy threats or possible harm that TikTok poses, maybe because they have never been harmed as a result of TikTok's actions, and their attitudes might change if they had experienced such circumstances.

Participants had just a rudimentary comprehension of TikTok's legal provisions, and they did not know much about the specific types of private data obtained by TikTok. In fact, not only TikTok, but many social media sites are also infringing on the privacy of users by recording personal information for the purpose of obtaining economic benefits. Furthermore, TikTok users are aware of the usual uses of their personal data by TikTok, which include personalized advertisements and video streams. However, they are worried about the information TikTok provided to third parties and how those third parties used it, as TikTok does not indicate the identities of third parties or how they would use the information lawfully in its Privacy Policy (2022).

Faced with the prospect of personal private information on social media platforms, users should not publish personal data to the Internet carelessly. The virtual environment of social media, one can display one's true self, yet there is

no distinction between the virtual and actual worlds, individuals share the same self in both worlds. Even some of the users may not care about their privacy or have to use TikTok due to personal reasons. I hope social media users should strengthen their understanding of personal privacy protection to safeguard their interests. Before consenting to any conditions and engaging in any relationship, they should carefully comprehend and understand the applicable legal statements to determine whether engaging in such a space is appropriate.

The perceptions of the harm among TikTok users are generally two-sided: one side believes TikTok must collect private information to optimize the user experience and share the private data with third parties to ensure the platform's operation. Another side argues that TikTok collects too much information about its users beyond the purpose of providing services and that TikTok's data procedures involve data security issues that might expose users to varying degrees of risk. Both sides make reasonable arguments, but the operation of social networks and the preservation of users' privacy are fundamentally contradictory. Social platforms need to mine users' private data to maintain operations, so the behaviour of users sacrificing private information is inevitable to a certain extent, and the resulting potential harm is also unavoidable. However, I think that by educating people about privacy protection and reinforcing the notion of the importance of privacy, the likelihood of privacy harm will be considerably decreased.

TikTok users of this research have highlighted a number of potential consequences of TikTok's privacy, including invasion: social, political, discrimination, identification, harmful addiction, and data security. They are worried that data collection and transmission could result in private data leakage that would further damage them in economic or social ways. The utilization of one-sided algorithms can trap users in self harm video streams and possibly influence them into joining undesirable organizations or engaging in harmful behaviour. TikTok's algorithm can accurately understand users' interests and behaviours by analyzing their private information, resulting in users becoming addicted to the application, which has a negative impact on their lives by harming real-life social interactions and creativity. There is still much potential harm left to be discovered, but I think to reduce the occurrence of harm is to regulate TikTok's data practices, increase the transparency of data processing, and empower users' autonomy in managing their private data. It is critical to monitor social media platforms' inappropriate use of user data; also, implementing transparent data gathering or utilization might help consumers have a more power-balanced relationship with the social media platforms.

The systems under surveillance capitalism are successful due to "structural independence from people, collectivist ambitions, and the necessity of sustained exploitation" (Zuboff, p. 319, 2020). Zuboff (p. 320, 2020) used “tyranny” to describe the surveillance capitalists, where they rule "in accordance with their own will and interest, rule one against all, and oppress the powerless

individuals." They use the power of technology and data privatization to control individuals' behaviour with "irresistible inducements and the replacement of legitimate contract, the rule of law, politics, and social trust with a new form of sovereignty and its privately administered regime of reinforcements" (Zuboff, p. 320, 2020). Their behaviours are "unlikely to be altered" (Zuboff, 2015), but how can powerless conformity secure their rights or ensure democracy?

It is our responsibility to correct the misbehaviours of surveillance capitalists and "never forfeit a human future to powerful companies and rogue capitalism that fail to honour our needs or serve our genuine interests" (Zuboff, p. 324, 2020). Surveillance capitalism has promised to meet our needs for an effective life, but it has also “usurped so many of our rights in these domains. It is a scandalous abuse of digital capabilities, and it is not contributing toward a human future" (Zuboff, p. 324, 2020). George Orwell (1946, as cited in Zuboff, p. 325, 2020) indicated that individuals are accompanied by "cowardice and partly in the worship of power, obeying the instinct to bow down before the conqueror of the moment, to accept the existing trend as irreversible." Surveillance capitalism and its instrumentation power seem to be invisible, but we should never stop resisting the unfairness rather than surrendering. Zuboff (p. 326, 2015) demands surveillance capitalism to "operate as an inclusive force bound to the people it must serve and defend their rights to become a genuine democracy." Even society is structured in such an unfair way, and individuals may recognize they are powerless in the face of the privileged capitalists. As members of the digital

world, we should not admit our fate, and we all need to fight back and reclaim what belongs to us.

Whether it is through using a VPN or other privacy-protecting software or by avoiding the customized information that the algorithm suggests, it is impossible to fully restore equality. Social media and algorithmic technologies exist to control and exploit the information of their users. However, I believe reducing the frequency of social software use and relying on personal self-control and motivation, or more cynically, resisting the temptation to use the 'free' social media services can possibly resist the domination. Is the inability to put down your phone causing addiction? Is social media just a tool we use? Are algorithms and technologies neutral? All social media platforms are merely attention-grabbing social tools, packaging users into commodities that are sold to advertisers. If we do not recognize and agree with the same truth, we cannot be united and cannot find solutions to any problem.

Surveillance capitalism becomes even more vicious as its system destroys the users it depends on, through constant invasion of privacy, but the problem might be solved through collective solidarity resistance. I think if people resist and coordinate to delete or stop using their accounts to boycott a social media company, it could give users some leverage to make their demands. But new questions have arisen: TikTok has billions of users and how many people does a social media boycott need to derail a giant like TikTok? Would such a boycott be successful in addressing social media privacy violations? Investigating

companies' data practices, imposing fines for violations, and working to strengthen privacy protections are other solutions, but did they really work?

I classify this research as a pilot study, which may be defined as a "small scale version[s], or trial run[s], done in preparation for the big study" (Polit et al., 2001, as referenced in Van, 2011) or "trying out or pre-testing a specific research instrument" (Baker, 1994, as cited in Van, 2011). I did not obtain enough replies to qualify as a large-scale research study since my research does not have substantial funds to compensate participants for their effort; but, I did receive enough responses to classify it as a trial or to offer valuable insights for the prospective large-scale study on such topics.

Future research into TikTok and other prevailing social media studies should focus on the methods to regulate the legal agreements to create a power-balanced model on social media, innovate a new privacy boundary consensus and establish a reliable privacy protection mechanism. Users, TikTok, and legal authorities must look forward to the future rather than merely their own short-term goals and collaborate to create systems that may possibly benefit all parties.

References :

Abraham, E. (2022, July 1). *Here's what data Tiktok collects from its users*. indy100. Retrieved July 2, 2022, from https://www.indy100.com/science-tech/tiktok-data-access-china-us

Abokhodair, N., & Vieweg, S. (2016). Privacy & social media in the context of the Arab Gulf. *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, 672–683. https://doi.org/10.1145/2901790.2901873

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday, 13(3)*. https://doi.org/10.5210/fm.v13i3.2142

Altuglu, V., Kumar, V., Mani, V., & Corus, S. (2022). Estimating Harm in Invasion of Privacy and Data Breach Disputes. In *Class and Group Actions Laws and Regulations 2022* (pp. 23–28). Chapter 4, Cornerstone.

Badillo-Urquiola, K., Smriti, D., McNally, B., Golub, E., Bonsignore, E., & Wisniewski, P. J. (2019). Stranger Danger!: Social Media App Features Co-designed with Children to Keep Them Safe Online. *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, 394–406. https://doi.org/10.1145/3311927.3323133

Bannerman, S. (2020). *Canadian communication policy and law.* Canadian Scholars.

Barnes, W. R. (2012). Social Media and the Rise in Consumer Bargaining Power. *University of Pennsylvania Journal of Business Law*, 14(3), 661–699. https://doi.org/1097-4938

Bartsch, M., & Dienlin, T. (2016). Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Bechmann, A. (2014). Non-informed consent cultures: Privacy policies and app contracts on Facebook. *Journal of Media Business Studies*, *11*(1), 21-38. https://doi.org/10.1080/16522354.2014.11073574

Beigi, G., & Liu, H. (2020). A survey on privacy in Social Media. *ACM/IMS Transactions on Data Science*, *1*(1), 1–38. https://doi.org/10.1145/3343038

Bianco, J. S. (2009). Social Networking and Cloud Computing: Precarious affordances for the "prosumer". *WSQ: Women's Studies Quarterly*, *37*(1-2), 303–312. https://doi.org/10.1353/wsq.0.0146

Boffone, T. (2021). *Renegades: Digital dance cultures from Dubsmash to TikTok*. Oxford University Press.

Brousseau, E., & Penard, T. (2007). The economics of Digital Business Models: A framework for analyzing the economics of platforms. *Review of Network Economics*, *6*(2), 81–114. https://doi.org/10.2202/1446-9022.1112

Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information Security Technical Report*, *14*(3), 160–166. https://doi.org/10.1016/j.istr.2009.10.007

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2006). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, *36*, 1-38. https://doi.org/10.1016/j.clsr.2019.105367

Büchi, M., Just, N., & Latzer, M. (2016). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278. https://doi.org/10.1080/1369118x.2016.1229001

Capers, Z. (2022, March 22). *How to remove personal information from internet sources for free*. GetApp. Retrieved July 3, 2022, from https://www.getapp.com/resources/remove-personal-information-internet/

Chan, C. (2018, December 3). *When AI is the product: The rise of ai-based Consumer Apps*. Andreessen Horowitz. Retrieved June 10, 2022, from https://a16z.com/2018/12/03/when-ai-is-the-product-the-rise-of-ai-based-consumer-apps/

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, *52*(2), 167–182. https://doi.org/10.1109/tpc.2009.2017985

Cocozza, N. (2014). Instagram Sets a Precedent by an Insta Change in Social Media Contracts and Users' Ignorance of Instagrams's Terms of Use May Lead to Acceptance by a Simple Snap. *Journal of High Technology Law* , *XV*, *15*(2), 363–394. https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/files/2015/05/Cocozza-Insta1.pdf

Cui, W., Wang, P., Du, Y., Chen, X., Guo, D., Li, J., & Zhou, Y. (2017). An algorithm for event detection based on social media data.

Neurocomputing, 254, 53–58. https://doi.org/10.1016/j.neucom.2016.09.127

Davenport, T. H., Barth, P., & Bean, R. (2012). How Big Data Is Different. *MITSloan Management Review*, *54*(1), 43–46. https://www.hbs.edu/ris/Publication%20Files/SMR-How-Big-Data-Is-Different_782ad61f-8e5f-4b1e-b79f-83f33c903455.pdf

Davis, J. (2019, June 27). *The Tiktok Strategy: Using AI platforms to take over the world*. INSEAD Knowledge. Retrieved May 10, 2022, from https://knowledge.insead.edu/entrepreneurship/the-tiktok-strategy-using-ai-platforms-to-take-over-the-world-11776

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. *Privacy Online*, 47–60. https://doi.org/10.1007/978-3-642-21521-6_5

Decision to Impose a Fine on TikTok. (2021, April 9). Autoriteit Persoonsgegevens. Retrieved June 17, 2022, from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

De Los Santos, M., & Klug, D. (2021). The TikTok tradeoff: Compelling algorithmic content at the expense of personal privacy. *20th International Conference on Mobile and Ubiquitous Multimedia*, 226–229. https://doi.org/10.1145/3490632.3497864

Du, X., Liechty, T., Santos, C. A., & Park, J. (2020). 'I want to record and Share my wonderful journey': Chinese millennials' production and sharing of short-form travel videos on TikTok or Douyin. *Current Issues in Tourism*, 1–13. https://doi.org/10.1080/13683500.2020.1810212

Ellis, B., Bird, J., Bould, H., Biddle, L., & Moore, R. (2022). Co-designing an experience sampling method digital platform to investigate self-harm among young people. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–6. https://doi.org/10.1145/3491101.3519861

Faison, A. (2021). TikTok Might Stop: Why the IEEPA Cannot Regulate Personal Data Privacy and the Need for a Comprehensive Solution. *Duke Journal of Constitutional Law & Public Policy Sidebar*, 16, 115-145. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1197&context=djclpp_sidebar

Fiesler, C., Dye, M., Feuston, J. L., Hiruncharoenvate, C., Hutto, C. J., Morrison, S., Khanipour Roshan, P., Pavalanathan, U., Bruckman, A. S., De

Choudhury, M., & Gilbert, E. (2017). What (or WHO) is public? *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 567–580. https://doi.org/10.1145/2998181.2998223

Gray, J. E. (2021). The geopolitics of 'platforms': The tiktok challenge. *Internet Policy Review*, *10*(2), 1–26. https://doi.org/10.14763/2021.2.1557

Goel, S. (2015). Anonymity vs. security: The right balance for the smart grid. *Communications of the Association for Information Systems*, *36*, 23–33. https://doi.org/10.17705/1cais.03602

Gorwa, R., & Guilbeault, D. (2018). Unpacking the social media bot: A typology to guide research and policy. *Policy & Internet*, *12*(2), 225–248. https://doi.org/10.1002/poi3.184

Han, Y. (2020). Advertisement on TikTok as a Pioneer in New Advertising Era: Exploring Its Persuasive Elements in the Development of Positive Attitudes in Consumers. *The Frontiers of Society, Science and Technology*, *2*(11), 81–92. https://doi.org/10.25236/FSST.2020.021113

Harriger, J. A., Evans, J. A., Thompson, J. K., & Tylka, T. L. (2022). The dangers of the rabbit hole: Reflections on social media as a portal into a distorted world of edited bodies and eating disorder risk and the role of algorithms. *Body Image*, *41*, 292-297. https://doi.org/10.1016/j.bodyim.2022.03.007

He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, *21*(5), 381–400. https://doi.org/10.1108/imcs-12-2012-0068

Heyman, R., De Wolf, R., & Pierson, J. (2014). Evaluating social media privacy settings for personal and advertising purposes. Info, 16(4), 18–32. https://doi.org/10.1108/info-01-2014-0004

Hofstra, B., Corten, R., & van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, *60*, 611–621. https://doi.org/10.1016/j.chb.2016.02.091

Hou, L. (2018). Study on the perceived popularity of TikTok. *BU Research*, 1-52. http://dspace.bu.ac.th/handle/123456789/3649

Huang, B. (2021). The reasons for Douyin's success from the perspective of business model, algorithm and functions. *Proceedings of the 6th International Conference on Financial Innovation and Economic Development (ICFIED 2021)*, 166, 320-325. https://doi.org/10.2991/aebmr.k.210319.058

Jacqueline, B. M. (2020). Children's rights and social media: An analysis of TikTok's Terms of Service through the lens of a young user. *IDEALS*. http://hdl.handle.net/2142/106069

Karizat, N., Delmonaco, D., Eslami, M., & Andalibi, N. (2021). Algorithmic folk theories and identity: How tiktok users co-produce knowledge of identity and engage in algorithmic resistance. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1–44. https://doi.org/10.1145/3476046

Kaur, P. (2020). Tik-Tok: Influence on Youth in India. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(6), 4194-4207. https://mail.palarch.nl/index.php/jae/article/download/1658/1658

Kennedy, H., Elgesem, D., & Miguel, C. (2017). On fairness: User perspectives on social media data mining. *Convergence*, 23(3), 270-288. https://doi.org/10.1177/1354856515592507

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior*, 69, 29–42. https://doi.org/10.1016/j.chb.2016.12.012

Kumar, S., Jigyasu, S., & Singh, V. (2021). Network Traffic Monitor and Analysis Using Packet Sniffer. *International Journal of Research in Engineering and*

Science (IJRES), *9*(7), 77–82. https://www.ijres.org/papers/Volume-9/Issue-7/Series-3/I09077782.pdf

Kutler, N. (2011). Protecting Your Online You: A New Approach to Handling Your Online Persona After Death. *Berkeley Technology Law Journal*, *26*(4), 1641–1670. https://www.jstor.org/stable/24118668

Livingston S. J., (2011) Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online social media Setting. *Journal of Science and Technology,* 21(3), 591-636. https://www.albanylawjournal.org/article/19340-invasion-contracts-the-privacy-implications-of-terms-of-use-agreements-in-the-online-social-media-setting

Lobel, O. (2007). The Paradox of Extralegal Activism: Critical Legal Consciousness and Transformative Politics. *Harvard Law Review*, 120(4), 937–988. https://doi.org/https://www.jstor.org/stable/40041996

Ma, Y., & Hu, Y. (2021). Business Model Innovation and experimentation in transforming economies: ByteDance and TikTok. *Management and Organization Review*, *17*(2), 382–388. https://doi.org/10.1017/mor.2020.69

MacKinnon, K. R., Kia, H., & Lacombe-Duncan, A. (2021). Examining TikTok's potential for community-engaged digital knowledge mobilization with

equity-seeking groups. *Journal of Medical Internet Research*, *23*(12). https://doi.org/10.2196/30315

Madden, M. (2012). Privacy management on social media sites*. Pew Internet Report*, 24, 1-20. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf

Masciantonio, A., Bourguignon, D., Bouchat, P., Balty, M., & Rimé, B. (2021). Don't put all social network sites in one basket: Facebook, Instagram, Twitter, Tiktok, and their relations with well-being during the COVID-19 pandemic. *PLOS ONE*, 16(3). https://doi.org/10.1371/journal.pone.0248384

McDonald, A. M., & Cranor, L. F. (2010). Americans' attitudes about internet behavioral advertising practices. *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society - WPES '10*, 63–72. https://doi.org/10.1145/1866919.1866929

Merriman, B. (2014). Ethical issues in the employment of user-generated content as experimental stimulus: Defining the interests of creators. *Research Ethics*, 10(4), 196–207. https://doi.org/10.1177/1747016114560764

Milan, S. (2015). When algorithms shape collective action: Social Media and the dynamics of cloud protesting. *Social Media + Society*, *1*(2), 1–10. https://doi.org/10.1177/2056305115622481

Mitrou, L., Kandias, M., Stavrou, V., & Gritzalis, D. (2014). Social media profiling: A Panopticon or Omniopticon tool? *The 6th Conference of the Surveillance Studies Network,* 1-15. https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf

Montag, C., Yang, H., & Elhai, J. D. (2021). On the psychology of TikTok use: A first glimpse from empirical findings. *Frontiers in Public Health*. https://doi.org/10.3389/fpubh.2021.641673

Monteiro, S. (2022). Gaming faces: Diagnostic scanning in social media and the legacy of racist face analysis. *Information, Communication & Society*, 1–17. https://doi.org/10.1080/1369118x.2021.2020867

Mooradian, N. (2009). The importance of privacy revisited. *Ethics and Information Technology*, *11*(3), 163–174. https://doi.org/10.1007/s10676-009-9201-2

Nahmias, Y., Dror Feldman, D. K., Richter, G., & Raban, D. R. (2020). Games of Terms. *Vermont Law Review*, *45*, 1–50. https://ssrn.com/abstract=3638598

Newberry, C. (2022, February 22). *How the TikTok algorithm works in 2022 (and how to work with it)*. Social Media Marketing & Management Dashboard. Retrieved July 3, 2022, from https://blog.hootsuite.com/tiktok-algorithm/

Nolan, C, & Wilson, A. (2015, November 1). *Social media and "the right to be forgotten".* The Data Administration Newsletter. Retrieved July 3, 2022, from https://tdan.com/social-media-and-the-right-to-be-forgotten/18484

Nissenbaum, H. (2004). Symposium: Technology, Values, and the Justice System: Privacy as Contextual Integrity. *Washington Law Review*, 79(1). 119-198. https://advance-lexis-com.libaccess.lib.mcmaster.ca/api/document?collection=analytical-materials&id=urn:contentItem:4BYH-TMY0-00CV-600G-00000-00&context=1516831.

Neyaz, A., Kumar, A., Krishnan, S., Placker, J., & Liu, Q. (2020). Security, Privacy and Steganographic Analysis of FaceApp and TikTok. *International Journal of Computer Science and Security [IJCSS]*, *14*(2), 38-59. https://link.gale.com/apps/doc/A682600882/AONE?u=ocul_mcmaster&sid=bookmark-AONE&xid=95a3bb4e

Obar, J. A. (2022, June 23). *A policy complexity analysis for 70 Digital Services*. The Biggest Lie on the Internet. Retrieved July 9, 2022, from https://www.biggestlieonline.com/policy-complexity-analysis-2019/

Obar, J. A. (2022, June 23). *A policy length analysis for 70 Digital Services*. The Biggest Lie on the Internet. Retrieved July 9, 2022, from https://www.biggestlieonline.com/policy-length-analysis-2019/

Obar, J. A, & McPhail, B. (2018, April 12). *Preventing big data discrimination in Canada: Addressing design, consent and sovereignty challenges*. Centre for International Governance Innovation. Retrieved July 9, 2022, from https://www.cigionline.org/articles/preventing-big-data-discrimination-canada-addressing-design-consent-and-sovereignty/

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147. https://doi.org/10.1080/1369118x.2018.1486870

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, *4*(3), 1-14. https://doi.org/10.1177/2056305118784770

O'Brien, D., & Torres, A. M. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, 31(2), 63-94.

https://iamireland.ie/wp-content/uploads/2014/01/IJM-312-2012-Final_crop.pdf#page=73

Office of the Privacy Commissioner of Canada. (2017, September 21). *2016-17 Annual report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.* Office of the Privacy Commissioner of Canada. Retrieved May 2, 2022, from https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/

Omar, B., & Dequan, W. (2020). Watch, share or create: The influence of personality traits and user motivation on TikTok mobile video usage. *International Journal of Interactive Mobile Technologies (IJIM)*, 14(04), 121-136. https://doi.org/10.3991/ijim.v14i04.12429

Omisola, I. (2022, April 21). *The Tiktok Privacy Concern you don't know about: Data Mining*. MUO. Retrieved July 2, 2022, from https://www.makeuseof.com/tiktok-privacy-concerns-data-mining/

Parsons, C. (2015). Beyond privacy: Articulating the broader harms of pervasive mass surveillance. *Media and Communication*, *3*(3), 1–11. https://doi.org/10.17645/mac.v3i3.263

Perez, S. (2021, June 3). *Tiktok just gave itself permission to collect biometric data on US users, including 'Faceprints and Voiceprints'.* TechCrunch.

Retrieved July 2, 2022, from https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/#:~:text=In%20that%20case%2C%20TikTok%20collects,found%20in%20the%20device's%20clipboard.

Privacy policy. TikTok. (2022, April 2). Retrieved May 31, 2022, from https://www.tiktok.com/legal/privacy-policy-row?lang=en

Plank, S. (2022). Perception of privacy of young users on social media-Analysis of the privacy paradox on the application TikTok. *Lauda*, 1-83. https://urn.fi/URN:NBN:fi-fe2022061747326

Richards, A. (2021). TikTok: The Darkside of Surveillance. *Critical Reflections: A Student Journal on Contemporary Sociological Issues*. https://ojs.leedsbeckett.ac.uk/index.php/SOC/article/view/4614

Roth, R., Ajithkumar, P., Natarajan, G., Achuthan, K., Moon, P., Zinzow, H., & Madathil, K. C. (2021). A study of adolescents' and young adults' tiktok challenge participation in South India. *Human Factors in Healthcare*, 1, 1-7. https://doi.org/10.1016/j.hfh.2022.100005

Powell, C. D. (2011). "You already have zero privacy. Get over it!" Would Warren and Brandeis Argue for Privacy for Social Networking? *Pace Law Review*, *31*(1), 146–181. https://core.ac.uk/download/pdf/46713064.pdf

Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24. https://doi.org/10.1080/17530350.2019.1574866

Sánchez Abril, P., Levin, A., & Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal*, *49*(1), 63–124. https://doi.org/10.1111/j.1744-1714.2011.01127.x

Selmi, M. (2021). Algorithms, Discrimination and the Law. *Ohio State Law Journal*, 82(4), 611-651. https://ssrn.com/abstract=3961802

Sherman, P. (2022, June 2). *Tiktok and privacy: Why this invasive app is so dangerous*. VPNoverview.com. Retrieved July 2, 2022, from https://vpnoverview.com/privacy/social-media/tiktok-privacy/

Simpson, E., & Semaan, B. (2021). For you, or for"you"? *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW3), 1–34. https://doi.org/10.1145/3432951

Smith, M., Szongott, C., Henne, B., & von Voigt, G. (2012). Big Data Privacy Issues in public social media. *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), 1-6*. https://doi.org/10.1109/dest.2012.6227909

Spann, S. A. (1989). A Critical Legal Studies Perspective on Contract Law and Practice. *Georgetown University Law Center*, 223–257. https://doi.org/https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2952&context=facpub

Steinfeld, N. (2016). “I agree to the terms and conditions”: (how) do users read privacy policies online? an eye-tracking experiment. *Computers in Human Behavior*, *55*, 992–1000. https://doi.org/10.1016/j.chb.2015.09.038

Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social Media Analytics – challenges in topic discovery, data collection, and Data Preparation. *International Journal of Information Management*, 39, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Su, D., & Lu, Y. (2021). Infer user preferences from aggregate measurements: A novel message passing algorithm for privacy attack. *Performance Evaluation*, *145*, 1–2. https://doi.org/10.1016/j.peva.2020.102148

Su, C., Zhou, H., Gong, L., Teng, B., Geng, F., & Hu, Y. (2021). Viewing personalized video clips recommended by TikTok activates default mode network and ventral tegmental area. *NeuroImage*, *237*, 1-11. https://doi.org/10.1016/j.neuroimage.2021.118136

Tabac, A. (2022, June 21). *Leaked recordings show Chinese TikTok employees accessed US Data*. The Jerusalem Post | JPost.com. Retrieved July 21, 2022, from https://www.jpost.com/business-and-innovation/article-709969

Tan, C., & Ta, K. (2021). GDPR Case Study: Dutch DPA Fines TikTok Over Privacy Policy. *Brown University, 1-3*. https://cs.brown.edu/courses/csci2390/2021/assign/gdpr/ctan-kta1-tiktok.pdf

Tang, D. (2019). The New Situation of Marketing in the Self-Media Era-Taking TikTok as an Example. *2019 2nd International Workshop on Advances in Social Sciences (IWASS 2019)*, 1557–1560. https://www.webofproceedings.org/proceedings_series/ESSP/IWASS%202019/SS06281.pdf

Van Teijlingen, E. R., & Hundley, V. (2001). The importance of pilot studies. *Social Research Update*, 35, 1-4. http://hdl.handle.net/2164/157

Vizcaíno-Verdú, A., & Abidin, C. (2022). Music Challenge Memes on TikTok: Understanding In-Group Storytelling Videos. *International Journal of Communication*, 16, 883-908. https://ijoc.org/index.php/ijoc/article/view/18141

Wang, Z., Zhu, W., Cui, P., Sun, L., & Yang, S. (2013). Social media recommendation. *Social Media Retrieval*, 23-42. https://doi.org/10.1007/978-1-4471-4555-4_2

Ward, J. S., & Barker, A. (2013). Undefined by data: a survey of big data definitions. *arXiv preprint,* 1-2. https://doi.org/10.48550/arXiv.1309.5821

Weber, R. H. (2011). The Right to Be Forgotten: More than a Pandora's Box. *Journal of Intellectual Property, Information Technology, 120-130*. https://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf

White, E. B. (2022, June 20). *Leaked audio from 80 internal TikTok meetings shows that US user data has been repeatedly accessed from China*. BuzzFeed News. Retrieved July 2, 2022, from https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

White, E. B. (2022, July 8). *Senate Intelligence Committee calls on FTC to investigate TikTok for 'deception'*. Forbes. Retrieved July 21, 2022, from https://www.forbes.com/sites/emilybaker-white/2022/07/05/senate-intelligence-committee-calls-on-ftc-to-investigate-tiktok-for-deception/?sh=360103506bd5

Wouters , N., & Paterson, J. (2022, July 1). *Tiktok captures your face. Pursuit*. Retrieved July 2, 2022, from https://pursuit.unimelb.edu.au/articles/tiktok-captures-your-face

Xue, L. (2020). Contradictions between public perception of privacy and corporate privacy policy: A case study of TikTok. *Simon Fraser University, 1-37.* http://summit.sfu.ca/item/20753

Yang, Y. (2020). Understanding young adults' TikTok usage. *Dostupno na, 1-60*. https://communication.ucsd.edu/_files/undergrad/yang-yuxin-understanding-young-adults-tiktok-usage.pdf

Yang, S., Zhao, Y., & Ma, Y. (2019, July). Analysis of the reasons and development of short video application—Taking TikTok as an example. *Proceedings of the 2019 9th International Conference on Information and Social Science (ICISS 2019), Manila, Philippines,* 340-343. https://webofproceedings.org/proceedings_series/ESSP/ICISS%202019/ICISS19062.pdf

Youmans, W. L., & York, J. C. (2012). Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of Communication*, *62*(2), 315-329. https://doi.org/10.1111/j.1460-2466.2012.01636.x

Žagar, M., and Poljak. D. H. (2015) Have we been monetized and become commodity without our consent-Privacy in the time of Big Data technology. *ResearchGate, 1-6*. https://www.researchgate.net/profile/Marinko-Zagar/publication/308859264_Have_we_been_monetized_and_become_commodity_without_our_consent_-_Privacy_in_the_time_of_Big_Data_technology/links/5b39e8bea6fdcc8506e72db8/Have-we-been-monetized-and-become-commodity-without-our-consent-Privacy-in-the-time-of-Big-Data-technology.pdf

Zeng, J., & Kaye, D. B. V. (2022). From content moderation to visibility moderation: A case study of platform governance on TikTok. *Policy & Internet*, 14(1), 79-95. https://doi.org/10.1002/poi3.287

Zenone, M., Ow, N., & Barbic, S. (2021). Tiktok and public health: A proposed research agenda. *BMJ Global Health*, 6(11), 1-3. https://doi.org/10.1136/bmjgh-2021-007648

Zhang, Z. (2020). Infrastructuralization of TikTok: Transformation, power relationships, and platformization of Video Entertainment in China. *Media, Culture & Society*, *43*(2), 219–236. https://doi.org/10.1177/0163443720939452

Zhang, M., & Liu, Y. (2021). A commentary of TikTok recommendation algorithms in MIT Technology Review 2021. *Fundamental Research*, *1*(6), 846-847. https://doi.org/10.1016/j.fmre.2021.11.015

Zhao, Z. (2021). Analysis on the “Douyin (Tiktok) mania” phenomenon based on recommendation algorithms. *E3S Web of Conferences*, *235*, 1–10. https://doi.org/10.1051/e3sconf/202123503029

Zheleva, E., & Getoor, L. (2009). To join or not to join. *ACM Digital Library*, 531–540. https://doi.org/10.1145/1526709.1526781

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the New Frontier of Power*. Public Affairs.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum*, 28(1), 10–29. https://doi.org/10.1177/1095796018819461

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, *30*(1), 75-89. https://doi.org/10.1057/jit.2015.5