

**Concerned Enough to Act? Privacy Concerns & Perspectives among Undergraduate
Instagram Users**

By
Hongru Zhang

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
Department of Communication
Faculty of Arts
University of Ottawa
Spring/Summer 2023

Abstract

A gap, known as the privacy paradox, often exists between peoples' privacy concerns and the actions they take to protect their privacy. This thesis investigates how a small sample of undergraduate students perceive their online privacy, the measures they take to protect their online privacy, and the reasons for their action/inaction. In so doing, it seeks to ascertain whether the findings of Hinds et al.'s (2020) regarding Facebook users' perceptions of online privacy issues are replicable among a sample of undergraduate students who are regular users of Instagram. Interviews with 20 undergraduate students were conducted to gather information about their online privacy concerns, their attitudes toward social media platforms collecting their information, and the privacy protection strategies they employ. The findings suggest that in enacting protection strategies, the participants delineate between both social and institutional conceptions of privacy, and the notion of privacy as a right requiring protecting versus viewing privacy as a negotiable commodity. This, in turn, suggests a possible need to re-consider how privacy-related education is approached as well as privacy policy.

Acknowledgement

I would like to especially thank Daniel J. Paré, my supervisor, for all the precious help I received in the last 2 years; I couldn't even imagine how to get this done without you.

I would like to express my love to my family; it's your support that has carried me all along the way to where I am today. I would also like to mention my glamorous friend, Coco Wang; raise glass for all the songs we've sung together, for the dreams we are still dreaming, and for this journey that will still be going on.

Table of Contents

Chapter 1: Introduction	1
1.1 General Background	1
1.2 Surveillance Capitalism and Advertising	2
1.3 Privacy Paradox	4
1.4 Thesis Structure	5
Chapter 2: Literature Review	7
2.1 People's Daily Uses of the Internet Under the COVID-19 Pandemic	7
2.2 The Facebook-Cambridge Analytica Data Breach Scandal	9
2.3 Surveillance and Manipulation	14
2.4 Instagram's Data Policy	16
2.5 Theoretical Background of Online Privacy	19
2.6 Statement of Central Research Question	27
2.7 Conclusion	29
Chapter 3: Methodology and Findings	30
3.1 Methodology	30
3.2 Summary of Questionnaire	36
3.3 Perspectives on Instagram Connecting with Users' Personal Data	41
3.4 Participants' Knowledge of Data Collection	43
3.5 Data Breaches	46
3.6 Privacy Protection Strategies	50
3.7 Leaving Instagram or Not	52
3.8 Shifting Platform Preferences	56
3.9 Conclusion	56
Chapter 4 Analysis	58
4.1 Privacy Literacy, Privacy Concerns, and Privacy Protection Behaviours	58
4.2 To Leave or Not to Leave; That Is Not the Question	66
4.3 Naivety	68
4.4 Rights vs. Needs	72
4.5 Conclusion	75
Chapter 5: Conclusion	76
5.1 Privacy Cynicism or Privacy Apathy	77
5.2 Limitations	81
5.3 Directions for Future Research	83
5.4 A Few Tentative Suggestions About Privacy-Related Education	84

5.5 Concluding Remarks	86
------------------------------	----

List of Tables

Table 1	18
Table 2	38
Table 3	39
Table 4	40

List of Figures

Figure 1	37
Figure 2	37
Figure 3	40

Bibliography	88
---------------------------	-----------

Chapter 1: Introduction

1.1 General Background

At this historical juncture, social media is an integral part of modern daily life in many parts of the world. Throughout the period of the global COVID-19 pandemic social media transformed from being largely perceived as a means of pursuing leisure and entertainment interests online into a vital tool for maintaining employment, familial, and social connections with others (Dixon, 2022). The ever-growing reliance, and seeming entrenchment, of social media in every facet of people's daily lives gives rise to a host of concerns about the privacy and surveillance implications of platform companies. Central to these concerns is the fact that, the basic principle of social media operation is anchored in providing users with 'free' access to services in return for the ability to collect users' personal information; the stated objective of which is both to design more personalized service offerings, and to re-sell the captured information on it to third parties for advertising and other purposes (see, for example, Trottier, 2012; Zuboff, 2015; Zuboff, 2019; Pangrazio & Selwyn, 2018).

As Pangrazio & Selwyn (2018) put it, interactions between users and social media platforms have come to constitute a 'symbiotic relationship.' However, this 'symbiotic relationship' comes at a cost for social media users; much of which is not always clear to users. For example, in the lead-up to the 2016 United States Presidential Election, Cambridge Analytica, a voter-profiling company, harvested some 50 million Facebook raw user profiles without informing the affected parties that their data would be used for political purposes. This constituted one of the largest data leaks in the history of social media (Rosenberger et al., 2018). It also catalyzed, public concerns about online privacy, giving rise to the #DeleteFacebook Movement

which sought to promote a boycott of the company.¹ Despite ultimately fizzling out and having little noticeable impact on Facebook's user numbers, the movement did serve to foment awareness about online privacy issues and to inform changes in government policy in the United States (Guynn, 2018).

The failure of the #DeleteFacebook Movement to gain much traction suggests, among other things, that it likely is unrealistic to expect people, today, to cut their ties with social media platforms as a means of protecting their privacy. With this in mind, and averring that participating on the Internet is “a prerequisite for social media inclusion,” Lutz et al. (2020) point to the seeming paradox of “most Internet users report[ing] both high levels of privacy concerns and high levels of privacy information disclosure” (pp. 1168-1169). It is the desire to better understand this paradox – a privacy paradox – that is the driving motivation for this thesis.

1.2 Surveillance Capitalism and Advertising

Taking stock of the combined levels of automation and surveillance characterizing much of the contemporary global economy, Zuboff (2015) proposed the concept of surveillance capitalism. This term refers to a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales (Zuboff, 2019, p. 8). As she puts it, surveillance capitalism reflects the latest stage in the logic of accumulation throughout the history of capitalism and as with the earlier stages, it too is producing “its own social relations and with that its conceptions and use of power” (Zuboff, 2015, p. 77). According to Zuboff, we have entered into a new form of economic relations that is characterized by people trading, both willingly and unwillingly, their personal information for access to free services. She further contends that this new economic structure constitutes a clear threat to the foundations of

¹ For a concise overview of this initiative see: <https://moveme.berkeley.edu/project/deletefacebook/>

democracy because the transaction of personal data can be used to “predict and modify human behaviour” without people being aware that this is occurring (i.e., nudging) (p. 75). As she sees it, when it comes to social media platforms the real customers are not the users, but advertisers who purchase user information. To this end, and as Zuboff (2019) points out, the type of surveillance and unauthorized mass scale behavior modification at the heart of the Facebook-Cambridge Analytica scandal, “appropriated the means and methods that are now both standard and necessary operations in the surveillance capitalism arsenal (p. 17). The advertisers pay for the mass users’ data to target them with advertisements. As a result, social media users become instruments to be modified, predicted, monetized, and controlled by the power produced by the platforms (Zuboff, 2019). Put simply, this is not the audience as commodity; it is audience *data* as commodity with the potential to directly modify individuals’ behaviour in real ways without their awareness or consent.

Zuboff labels this process, instrumentarianism. It refers to the capacity of platform companies to take advantage of “unprecedented asymmetries of knowledge and power” (Zuboff, 2019, p. 25). This is achieved by users being largely unaware of when and how their data are collected and sold. Over time, as people's dependencies on the platform services grow, so do their needs. Today, people rely on any number of “daily logistics, social interaction, work, education, health care, [and] access to products and services” provided by the companies who surveil them (p. 25). In such contexts, it is all too easy to succumb to “resigned cynicism,” sheltering oneself “behind the defense mechanisms (‘I have nothing to hide’)... choosing ignorance out of frustration and helplessness” (p. 25) and eschew protecting one’s on- and off-line privacy.

Claxton (2021) also examines the links between the predictive power of the data held by platform companies and contemporary advertising. Echoing Zuboff, she argues that in purchasing

users' data from platform companies, advertisers can both reach consumers with "unprecedented precision," and "predict and influence [the consumers'] future behaviours" (p. 1202). This process, she further notes, tends to be coupled with the propensity for platform companies to provide the users with personalized content that, in turn, serves to "to create dopamine reactions and keep users glued on the screens" (p. 1205).

The functioning of surveillance capitalism is contingent upon fostering a sense of dependency among consumers. Specifically, the sense that they cannot live without the services provided by platform companies. In turn, the decision to stay results in the platforms being able to collect ever growing quantities of user data; a not-so-virtuous cycle of sorts.

1.3 Privacy Paradox

According to Sindermann et al. (2021), the privacy paradox is defined as the "gap between privacy concerns and privacy behaviours" (p. 1456). Several studies of online privacy link the privacy paradox to privacy fatigue and/or privacy cynicism (see, for example, Taddicken, 2014; Aguirre et al., 2016; Barth & de Jong, 2017; Zeng et al., 2021). According to Choi et al., (2018), "privacy fatigue reflects a sense of weariness toward privacy issues," that can lead users to "'do nothing' in response to the misuse of their personal information" (pp. 42 & 48). Hargittai & Marwick (2016) have suggested that the existence of privacy fatigue, the simultaneous presence of privacy concerns, and people's widespread self-disclosure are not necessarily paradoxical, "but rather a pragmatic response to the contemporary networked social environment" (p. 3752).

Another factor at play in this context is privacy cynicism. It is widely considered to be a core component of privacy fatigue (see, for example, Choi et al, 2018; Lutz et al., 2020; Zhu et al., 2021). According to Hoffmann et al., privacy cynicism is defined as "an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering

privacy protection behaviour subjectively futile... [that] moderate[s] (i.e. weaken) the effect of privacy concerns on protection behaviour” (p. 2 and p. 7).

In the wake of the Facebook-Cambridge Analytica scandal Hinds et al. (2020) investigated issues of privacy fatigue and privacy cynicism among 30 Facebook users. Their findings suggested that the participants appeared to have contradictory beliefs and concerns about their online privacy as well as mixed emotions regarding their privacy protection strategies. Inspired by the latter study, this thesis investigates privacy fatigue and privacy among a small sample of undergraduate students from the University of Ottawa who are all regular users of Instagram, as one of the most popular apps among young adults. The objective of my project is to ascertain whether Hinds’ et al.’s findings are replicable among regular Instagram users. With this in mind, the central research question leading this exploratory project is:

Are Hinds et al.’s (2020) findings regarding people’s perceptions of online privacy issues replicable among a sample of undergraduate students who are regular users of Instagram?

In the pages that follow, this question is addressed by examining two aspects of the privacy paradox.

- *What concerns do undergraduate students in my sample have about Instagram’s use of data to facilitate the targeting of advertising to their screens?*
- *What strategies do the undergraduate students in my sample use to protect their online privacy? And, do they view these strategies as effective?*

1.4 Thesis Structure

This thesis is divided into five chapters. This first chapter has provided a brief introduction to the background of the research topic and the research objectives. Chapter 2 starts by providing an overview of the Facebook-Cambridge Analytica scandal. This is followed with a review of Instagram’s Data Policy and a detailed discussion of the core theoretical concepts at the heart of this project. Chapter 3 presents the research design and methodology used to guide this

undertaking. In Chapter 4 I present an analysis of the research findings in the light of the relevant theory and in comparison, with the findings of Hinds et al. (2020). Chapter 5 wraps up this thesis by setting out the key findings and implications emerging from my project.

Chapter 2: Literature Review

The discussion presented in this chapter centers on the role social media platforms play in people's daily lives and issues of security of personal information in the online environment. In the first section, the discussion examines how the changing of the role of the Internet and social media in people's lives during the global COVID-19 pandemic has increased the level of urgency of discussion about online privacy issues. In Section 2, the discussion turns its attention to the Facebook-Cambridge Analytica scandal and some of its repercussions. Section 3 examines why users' personal information is easily breached on social media and the potential harm this bring. In Section 4, the discussion shifts focus to Instagram's Data Policy Section 5 offers a concise review of some of the key privacy-related concepts that are central to my project. This chapter concludes with a brief overview of the broader research context for this thesis and a presentation of the central research question guiding the study.

2.1 People's Daily Uses of the Internet Under the COVID-19 Pandemic

With the outbreak of COVID-19 in Wuhan, China at the end of 2019 and the World Health Organization's subsequent declaration of a global pandemic on March 11, 2020, people's daily lives were fundamentally transformed as everyday activities ground to a halt and people found themselves in lockdowns. One consequence of being stuck in one's home was that people began spending even more of their daily time online and engaging with social media platforms for work, study, and leisure (see, for example, Koeze & Popper, 2020; Molla, 2020; Wold, 2020).

For example, Saud et al.'s (2020) investigation of the role that social media played in the daily lives of 348 Indonesians of varying age groups during the period of the COVID-19 pandemic found that social media served as an important "social support parameter with family, online and offline friends, relative, general public, and colleagues" and as an important to tool "to learn and

collect information about the illness” (p. 4) during periods for which people were required to stay at home (p. 7).

The pandemic also brought to the fore the importance of the types of information people were accessing online and, specifically, the damaging roles of mis- and dis-information. In their investigation of the spread of misinformation² on Twitter, Wang et al. (2021) found that misinformation about different topics has different effects on their spread, with conspiracy theories being retweeted most frequently. In addition, their examination of some 39 million tweets suggest that “when users were more active in talking about COVID-19 in general, misinformation also got more attention” (p. 731).

Mehta (2020) focused on the people who were working from home during the pandemic “to identify and highlight the relevant factor that influences WFH [work from home] work engagement and to investigate the relationship between WFH, work engagement, and happiness” (p. 4). In order to achieve these objectives, Mehta (2020) conducted a survey of some 440 employees of IT sector companies who were working from home. The results suggested that “employees feel more engaged with their work because working from home affords them autonomy, safety, and convenience during COVID-19 pandemic, and that this work engagement leads to happiness” (Mehta, 2020, p. 9). In other words, WFH was significant in employees’ positive mentality during the pandemic lockdown period.

During the COVID-19 pandemic, Nur-A Yazdani et al. (2022) conducted a sequential cross-section survey of some 2926 Bangladeshi Internet users between the ages of 25 and 45 to

² Misinformation refers to “false or misleading information, unintentionally, presented as fact – when one believes something is accurate, but in reality, it is not” whereas disinformation refers to “false or misleading information purposefully distributed – when one knows something to be untrue but shares it anyway.” See, What is Misinformation/Disinformation?, <https://www.lib.purdue.edu/misinformation-training/training-module/what-is-misinformation>

investigate “psychological and physical issues related to social media.” The authors collected data from users across a six-week period that coincided with a period of national lockdown in Bangladesh; early September to mid-and October, 2020. Echoing Saud et al.’s (2020) observation that using social media use was providing people with varying types of psychological support during the pandemic period, Nur-A Yazdani et al. (2022) suggest that “social media addiction decreases users’ fear level, and fear level decreases with longer social media hours over the period of six weeks” (p. 11).

People’s use of and reliance upon social media platforms increased throughout the pandemic. The services offered by these platforms served as, among other things, important tools for people working and studying from home, venues for obtaining information, misinformation and disinformation about the pandemic, and a means of keeping in touch with friends and family. The heightened sense of reliance, and indeed dependency, upon these platforms point to a need to better understand people’s online privacy concerns and the strategies they employ to protect their interests. This is especially so for young adults given that they constitute the most prolific demographic of active social media users. As reported by Schaffer (2023), 18 to 29-year olds account for 88% of the usage of the main social media platforms.³ With this in mind, the discussion in the next section turns its attention to what is widely recognized as perhaps the most infamous breakdown in privacy; the Facebook-Cambridge Analytica scandal.

2.2 The Facebook-Cambridge Analytica Data Breach Scandal

As people spend more and more time engaging with social media platforms, they inevitably leave behind ever more personal information about themselves. Hence, the widespread concerns about

³ See, <https://nealschaffer.com/social-media-demographics/#:~:text=Which%20demographic%20uses%20social%20media,Facebook%2C%20Instagram%2C%20and%20Twitter.>

people's online information security (Isaak & Hanna, 2018; Kaiser, 2019; Laterza, 2021). In 2018, the release of details about Cambridge Analytica's gathering of the personal information of millions of Facebook users without their consent throughout the 2010s sparked a heated public discussion about online privacy, security, and surveillance capitalism (Meredith, 2018; Leetaru, 2019; Rosenberger et al., 2018).

The reader may recall that this scandal involved a 2015 collaboration between the U.K.-based Cambridge Analytica and Aleksandr Kogan, a Cambridge researcher, in developing an app called *thisisyourdigitallife* at the core of which was a personality quiz (ur Rehman 2019). In the period coinciding with the lead-up to Donald Trump's 2016 United States Presidential election campaign, this app harvested, without the quiz-takers' consent, data from their Facebook accounts and that of their Facebook friends. Elaborating on this matter, ur Rheman (2019, p. 6) points out that, the quiz-takers,

agreed to share their data, and Facebook's default terms allowed their friends' data to be collected by an app... but none of them agreed to sell their data to firms such as Cambridge Analytica that turned their data into a lucrative political tool.

When Facebook learned about this situation in 2015, it banned the app and demanded Cambridge Analytica deleted all the data gathered (Meredith, 2018). However, three years later, in 2018, Facebook learned that Cambridge Analytica had failed to heed its demand (Meredith, 2018).

When the story of this data breach broke on March 20, 2018, the U.S. Federal Trade Commission (FTC) opened an investigation into whether Facebook had violated a previous settlement it had reached with the regulator regarding users' privacy protections (Meredith, 2018). One day after the FTC announced it was launching the investigation, Mark Zuckerberg, the CEO of Facebook, admitted that "it was... a breach of trust between Facebook and the people who share their data with us and expect us to protect it." In the same announcement he pledged to make

changes in Facebook policies to prevent similar breaches happening (Lee, 2018). In July 2019, the FTC fined Facebook \$5 billion as a result of the investigation into this data breach. At the time of writing this thesis, the fine remains the largest penalty assessed by the US government against a technology company (Wong, 2019).

Within days of this story breaking, the #DeleteFacebook Movement was initiated on Twitter. The hashtag was tweeted more than 400,000 times within 30 days of the Facebook-Cambridge Analytica scandal being exposed (Zeitlin, 2018). However, the findings of a survey conducted by the investment firm Raymond James found that despite 84% of users being concerned about this data breach issue, nearly half of the participants, 48%, indicated that they would not cut themselves off from Facebook (Guynn, 2018). Nonetheless, Brown (2020) maintains that in the aftermath of the Facebook-Cambridge Analytica scandal, people became more concerned about their online privacy as was evidenced, in part, by the numbers of those who joined the #DeleteFacebook Twitter campaign. However, Brown (2020) also found evidence of a “privacy paradox” in social media use (p. 2) insofar as “the people who are most concerned about privacy do not always utilize the privacy settings available on social media” (p. 2).

Starting from the premise that the online privacy concerns perpetuated by the Facebook-Cambridge Analytica scandal are multicultural and global in scope, Gonz’alez-Pizarro et al. (2021) sought to identify the types of information privacy concerns people were tweeting about in relation to the scandal and whether these concerns differed by language and world region. In so doing, they analyzed tweets some 74,644 Spanish language tweets and 975,678 English language tweets relating to the Facebook Cambridge Analytica scandal that were sent from 36,056 human-owned accounts in the period spanning April 1 to July 10, 2018.

The sampled tweets were analyzed in relation to two types of privacy concerns: control or “the perceived fairness of the procedures that maintain personal data” (p. 37) and awareness or on “issues of transparency of the procedures and specificity of information to be used” (p. 37). Gonz’alez-Pizarro et al.’s (2021) findings suggest that English-language tweets illustrated “a broader emphasis on data collection” than their Spanish counterparts, and those tweets emanating from North America showing the least emphasis on awareness. As Gonz’alez-Pizarro et al. point out the noteworthiness of their findings is twofold. First, it serves to highlight the need for more diverse sources of data about privacy. Second, and perhaps most importantly, it highlights the need for more nuanced analyses of online privacy concerns around the world.

To gain an understanding of peoples’ thinking regarding the scandal and the factors subsequently influencing their decision to stay with or leave Facebook, Brown (2020) interviewed ten undergraduate and graduate students. She found that despite all the participants knowing about the Cambridge Analytica scandal prior to the interviews, only one had deactivated their account in response to this misuse of data. None of the participants, however, left Facebook permanently. In other words, despite the participants' concerns about privacy issues, most “resigned themselves to this as the status quo” (p. 6), due, in part, to fears of “losing touch with friends, family, professional, and the other contacts” and “the cross-platform use of Facebook logins to access other online services” (p. 6). Given the small size of Brown’s research sample, one clearly cannot generalize from these findings, but are illustrative of a privacy paradox and may nonetheless be illustrative of Facebook having, for many, become a necessity in their daily lives.

Afriat et al. (2021) also investigated the views of young adults who continued engaging with Facebook after the Cambridge Analytica scandal had become public. They conducted in-depth semi-structured interviews with 26 young adults prior to news of the scandal breaking

(December 2017) and with another 24 while it was unfolding (April 2018). Afriat et al. identified “a marked shift away from the understanding of privacy as a right” in the aftermath of the scandal (p. 123). Indeed, these authors note that the participants seemed to understand “the idea of privacy as a negotiable commodity” that is used to pay for free online services (p. 122), with some even considering “surveillance an advantage in itself” (p. 120). For example, some interviewees reportedly found the targeted advertisements on their Facebook pages very helpful. Also, in their research, Afriat et al. (2021) discussed the concept of ‘social privacy’⁴ and ‘institutional privacy’⁵ and found that “even at the outbreak of an institutional privacy scandal, young adults were still preoccupied with dangers presented by other users” (p. 119). Moreover, just like Brown’s (2020) research results, Afriat et al (2021) found that even with the Facebook-Cambridge Analytica scandal, most participants did not consider “leaving Facebook to be a valid option” (p. 122). There were three main reasons given by the participants. First, they needed the information provided by the platform in order to “be kept up to date” on developments of interest to them (p. 122); second, “they consider themselves ‘addicts’” (p. 122); third, the participants associated people without Facebook accounts with being considered weird, a behaviour of “a desire to be unique, [and] to go against the stream” (p. 122).

The conclusion to be drawn from the studies reviewed above is although expressed concerns about their online privacy in the wake of Facebook-Cambridge Analytica scandal, and while these concerns were far from uniform around the globe a privacy paradox appeared to be manifest. That is people’s concerns about their online privacy and personal information security were the lengths

⁴ Social privacy refers to “the control of information flow about how and when personal information is shared with other people” (Raynes-Goldie, 2010).

⁵ Institutional privacy refers to “how institutions such as governments, banks, and business, use or misuse the personal information” (Raynes-Goldie, 2010).

people are willing to go to protect their privacy is bounded by a sense of pragmatism that largely precludes the possibility of cutting one's ties with social media platforms.

Moreover, this pragmatism also appears to be connected toward an understanding and acceptance of privacy as a 'negotiable commodity' to be traded for free services provided social media platform companies. This 'trading' of personal information for access to desired products and services is the basis of what Shoshna Zuboff labels surveillance capitalism. This economic model is the focus of discussion in the next section.

2.3 Surveillance and Manipulation

In 2015, Zuboff proposed the concept of 'surveillance capitalism' to describe the contemporary form of economy in which people trade their personal data for access to 'free' social network services. She discussed four uses of data in the computer-mediated transactions that are central to surveillance capitalism: data extraction and analysis, new contractual forms due to better monitoring, personalization and customization, and continuous experiments.

For data extraction and analysis, the trade for free services is done by users' personal information being extracted and analyzed by platforms companies. This information is not just comprised of names and emails. It includes all aspects of the users' everydayness. These extractions and analyzes "typically occur in the absence of 'the individual's consent' (p. 79) and, yet, rather than being "regarded as a violation, invasion, or erosion of privacy rights," tend to be taken as a new contractual form that takes effect as users click the tick at the end of the User Agreement (p. 82).

Next, personalization and customization come into play. As Zuboff (2015) puts it, platform companies pretty much always "know what you want and tell you before you ask the question" (p. 83). She further contends that this state of affairs goes hand-in-hand continuous experiments

insofar as, even reality itself seems to be fictional and artificially created by being “subjugated to commodification and monetization” in the continuous experiments of users’ data being capture and analyzed every day (p. 85). This capacity reflects asymmetries of knowledge that are sustained by asymmetries of power between the platforms and the users. This asymmetry rests in no small measure in how difficult it is for users to fully recognize what information is collected from them and the purposes for which it is being used whether commercial or, as in the case of Cambridge Analytical, political. Moreover, as Zuboff sees it, with these processes constitute an anti-democratic threat because with the continuous capturing of the data of everydayness “what is accumulated... is not only surveillance assets and capital, but also rights” and a reality in which future behaviours and decisions are decided in the absence of mutual dialogue.

Paralleling the arguments advanced by Zuboff (2015), Manokha (2018) posits the commodification of personal data by social media platforms “is a major threat to the right to individual privacy” that “threatens the very existence of democratic politics” (p. 11). Manohka (2018) describes platforms as “digital infrastructures that connect producers, consumers, service providers, advertisers, and other groups in an interactive ecosystem and enable the exchange of goods, services or information” (p. 4). In his view, platforms are places to make all these activities happen in accord with capitalist principles and values.

Surveillance, he maintains, “necessitates constant profiling and sorting, evaluation and ranking, notation and monitoring,” and is the essential logic that guarantees platforms operate effectively (p. 4). Through surveillance, users’ personal data are gathered and transformed into a ‘fictitious commodity’ that is transacted between the platforms and the advertisers. Echoing the lack of user consent and *a priori* awareness in the Facebook-Cambridge Analytica scandal, today, users whose data constitutes the commodity, are not part of the transaction. According to Manohka

(2018), if people want to maintain their privacy rights, it is not the individual actors, like Cambridge Analytica, that need to be challenged, but the “platform capital as a whole” (p. 11).

Susser et al. (2019) examined the threat of surveillance capitalism to democracy by focusing on the concept of online manipulation. For them, online manipulation involves “the use of information technology to covertly influence another person’s decision-making, by targeting and exploiting decision-making vulnerabilities” (p. 6). Digital surveillance, they argue, aims to let third parties who maintain business relationships with platform companies engage in behavioural targeting aimed at detecting “when and how to intervene in order to most effectively influence” users’ decision-making (Susser et al., 2019, p. 6). Susser et al. further point out that even the language used in the terms like ‘users’, ‘user interfaces’, or ‘human-computer interaction’ also is a part of this manipulation (p. 7). These terms, they argue, contribute to making people believe that,

they have a mutual relationship with the digital services, so it is hard for them to recognize that they are one-way manipulated by the digital platforms. Upon the fact that digital surveillance affects the users’ independent decision-making, this online manipulation clearly “violates its target’s autonomy. (Susser et al., 2019, p. 8).

Put simply, although users may believe or otherwise feel that they are exercising autonomy by deciding to ‘trade’ personal information in exchange for access to free services that align with their preferences, this autonomy is only an illusion because their preferences are already manipulated by the platforms. With this in mind, the discussion in the next section looks at the contractual form to which Instagram users are subjected.

2.4 Instagram’s Data Policy

Instagram <<https://www.instagram.com>> is a popular social media platform among the 18-24 age

demographic (Lin, 2023) and, like Facebook, is owned by Meta Platforms Inc.⁶ Instagram is a photo- and video-sharing social networking mobile app founded in 2010⁷ that was acquired by Facebook Inc., in 2012 (Protalinski, 2012). In an effort to distance the company from a number of controversies with which it found itself having to contend, including how it was being used to spread hate speech, misinformation, and disinformation, in late 2021 Facebook changed its name and rebranded itself to Meta (Isaac, 2021).

Instagram users can create social networks by sharing photos and videos with their followers or with a preselected group of friends. Instagram's Data Policy clarifies the types of information collected from users and how this information is used (see Table 1). Even just a quick glance at the information presented in Table 1 makes clear that the information collected by Instagram, or Meta, is very comprehensive. It is illustrative of what Zuboff (2015) describes as the information of everydayness.

Instagram's Data Policy is very lengthy and hardly an enthralling read. Using this simple observation as a launch pad, Soumelidou and Tsohou (2019) investigated how to improve the format of Instagram's data policy to increase users' information privacy awareness levels. They define information privacy awareness as "one's knowledge of possible threats related to the disclosure of their personal information" (p. 503), "the knowledge of the content of privacy statements" (p. 504), and "one's ability to recall the elements or a privacy policy" (p. 504). To achieve their research objective, Soumelidou and Tsohou (2019) sought to identify document visualization techniques that might contribute to presenting Instagram's privacy policy in a more effective manner. They chose the 'Cards' and the 'Clouds' formats. The former is a technique

⁶ See, https://about.facebook.com/?sk=h_chr

⁷ For a brief history of Instagram see, <https://www.investopedia.com/articles/investing/102615/story-instagram-rise-1-photo0sharing-app.asp>

Table 1: Information Collected by Instagram and What It Is Used For⁸

Types of Information Collected	How Information is Used
➤ Things users do and provide (e.g., when registered for an account, create or share content and message or communicate with others; networks and connections; usage of Meta products; information about transactions made using Meta products; things others do and information they provide about users). ➤ Device information (e.g., device attributes, device operations, identifiers, device signals, data from device settings, network and connections, cookie data) ➤ Information from partners (e.g., information about the activities of Instagram users when they are not using Instagram)	➤ To personalize, and improve product offerings. This includes: information gathered across Meta products and devices and location-related information ➤ For product research and development ➤ For tailing ads and sponsored content ➤ Provide measurement, analytics, and other business services ➤ Promote safety, integrity, and security ➤ To communicate with users ➤ Research and innovation ➤ How information is shared and with whom: ➤ People and accounts users share and communicate with ➤ Content others share or reshare about individuals' users ➤ Information about active status or presence on Meta products ➤ Apps, web sites, and third-party integrations on or using Meta products ➤ Third-party partners ➤ Partners using Meta analytics services ➤ Advertisers ➤ Measurement partners ➤ Vendors and services partners ➤ Researchers and academics ➤ Law enforcement or legal requests

That builds on the concept of top trumps game cards.⁹ In so doing, this approach offers a meaningful concise overview of Instagram's privacy policy by combining important key terms and images. The Clouds format, by contrast, involves tag clouds consisting of "representative

⁸ See, Instagram Data Policy at: https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

⁹ Top Trumps is a card game that contains "expressive pictures and facts provide a combined overview of an object" (Strobelt et al., 2009).

keywords that either are extracted from the privacy policy or have the same meaning with the words of interest that are highlighted by font size and weight” (Soumelidou & Tsohou, 2019, p. 508).

They, then, recruited 60 undergraduate students from the Department of Informatics at Ionian University¹⁰ who possessed technical backgrounds and 60 others from the university who were familiar with Instagram but lacked technical backgrounds. The participants were randomly assigned to three groups. Members of the first, or control group, were tasked with reading Instagram’s conventional privacy policy. Those assigned to the other two groups were exposed to presentations of the privacy policy in the cards and clouds formats, respectively. The participants were then asked to complete a questionnaire that tested their awareness levels of Instagram’s privacy policy.

Soumelidou and Tsohou (2019) found that the conventional privacy policy was “verbose and difficult to understand” (p. 516) whereas “a visualized privacy policy can contribute to users’ privacy awareness on Instagram than the conventional privacy policy more effectively” (p. 515). This led them to call “for the conversion of the traditional text-based format to a more attractive one” (p. 516). Nonetheless, some three years after this study was published, Instagram’s Data Policy remains lengthy and verbose which, in turn, calls into question its efficacy as a tool for making users aware of the privacy issues they might encounter once registered with the platform.

2.5 Theoretical Background of Online Privacy

Despite ever-present concerns about online privacy, such worries do not always lead to the taking of protective measures to ensure the security of one’s information. As was noted earlier, this phenomenon – “users claim[ing] to be very concerned about their privacy but do[ing] very little to

¹⁰ See, <https://di.ionio.gr/en/>

protect their personal data” (Barth et de Jong, 2017, p. 139) – is known as the privacy paradox and has garnered growing amounts of scholarly attention in recent years (Aguirre, 2016; Guo et al., 2016; Karwatzki et al, 2017; Cloarec, 2020; Martin, 2020; Chhabra, 2021).

Petronio (2002) introduced the Communication Privacy Management (CPM) theory to argue that “privacy disclosures are dialectical” with “choices about revealing or concealing based on criteria and conditions they [individuals] perceive as salient” (pp. 2-3). To this end, she uses the metaphor of boundaries to illustrate that the parameters of privacy are not fixed but, rather, a negotiation between accessibility and retreat. For example, in some instances, one may opt to set their Instagram account to private, thereby preventing anyone else from viewing one’s posts, while nonetheless continuing to enjoy the other services provided by Instagram. However, to share select aspects of one’s life with friends and family or even to get more attention from strangers, many people choose to approve any and all ‘follow’ requests or to make their accounts fully public.

It merits noting that neither option – privacy or approve all – prevents Meta from gathering data and retaining the rights over the material posted.¹¹ If one wants to stop Meta from gathering one’s data, they must delete their Facebook and/or Instagram accounts and any other Meta products they may use, as well as find a means to ensure no third parties share their data with Meta. In other words, one ostensibly needs to give up their ability to participate in a wide range of platform mediated online activities that have come to be embedded in many peoples’ everyday lives. Faced with such a heavy cost, when it comes to negotiating privacy, many people opt to disclose personal information to Meta despite any privacy-related reservations they may hold.

In order to investigate “the relationship between online privacy concerns, privacy literacy,

¹¹ Instagram’s Data Policy, specifies, “we collect information about how you use our Products, such as the types of content that you view or engage with, the features you use, the actions you take, the people or accounts you interact with and the time, frequency and duration of your activities” (See, <https://help.instagram.com/155833707900388>).

and behavioural intentions and behaviours” Baruh et al. (2017, p. 27) conducted a systematic literature review and meta-analysis of 6,427 articles whose titles and/or abstracts contained “derivates of *privacy concern*, *privacy knowledge*, and *privacy protection*” (p. 31) [emphasis in original]. Privacy literacy here can be understood as “declarative knowledge of privacy risks” and “procedural knowledge about how to protect one’s privacy” (p. 29). Baruh et al.’s (2017) findings suggest that higher privacy concerns tend to be associated with lower intentions to use online services but not so much with the intention to use social networking sites. In other words, although some people may express apprehensions about using online services when it comes to their online privacy, such concerns seldom are strong enough to induce them to refrain from using social media platforms. Baruh et al. (2017) also found that “users with higher privacy literacy reported higher concern from privacy” but “in terms of privacy-management behaviours, privacy literacy was not significantly associated with information-sharing behaviour” (p. 39). This finding appears to support Petronio’s (2002) assertion about the boundaries of privacy being context-dependent and subject to the internalized negotiation with oneself.

A second approach used to frame the study of people’s online privacy-related behaviours is rooted in the theories of planned behaviour (TPB). Proponents of this view posit that “behavioural dispositions, such as social attitude and personality trait, have played an important role in these attempts to predict and explain human behaviour” (Ajzen, 1991, p. 179). Drawing from this perspective, Saeri et al. (2014) investigated “the role of perceived risk and trust in online privacy protection” (p. 363) by conducting two surveys, two weeks apart, with 119 first-year Australian undergraduate students. Their objective was to ascertain if the participants changed the privacy settings of their Facebook accounts after learning “online privacy protection... perceived risk and trust, [and] the theory of planned behaviour variables” (p. 357).

Overall, their participants reported “positive attitudes, high perceived behavioural control, and high intention to protect their privacy on Facebook” (p. 359). Further, their results showed that “when participants perceived greater risk, they reported more positive intentions to protect their privacy online” (p. 361), but that there was no association “between perceived risk and *actual* privacy protection behaviour” (p. 363). This led Saeri et al. (2014) to conclude that the inconsistencies demonstrated by their findings point to behavioural dispositions perhaps informing privacy protection intentions but not necessarily real privacy protection behaviours. This conclusion parallels the more recently advanced observations of González-Bailón & Gorham (2018) who, as previously mentioned, found that within the span of a few short months both the Facebook Cambridge Analytica scandal and the #DeleteFacebook Movement had run their course without any notable impact on Facebook user numbers.

Bartsch and Dienlin (2015) examined factors that might increase online privacy literacy and how such literacy might alter both online behaviour and perceived safety. They surveyed 630 Germany-based participants between the ages of 18 and 63, 74% of which identified as female, who responded to an online questionnaire that was administered between October and November of 2012. They identified a positive relationship between privacy literacy and both the amount of time spent on social networking and the frequency of changing privacy settings. They also found that “respondents with higher levels of social privacy literacy... showed more social privacy regulation behaviours... [and] felt safer when using SNSs” (p. 152). These findings seem to contradict Baruh et al.’s (2017) observation that “in terms of privacy-management behaviours, privacy literacy was not significantly associated with information-sharing behaviour” (p. 39). There are several viable explanations for this discrepancy, including the methods used by the

different researchers, different research frameworks and strategies, and differences between research samples.

A related concept that contributes to the privacy paradox is privacy fatigue. Choi et al., (2018) defines privacy fatigue as “a sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet” (p. 42). Privacy fatigue is hardly a new phenomenon. Writing some 16+ years ago, Acquisti et al. (2006) observed that when it comes to privacy fatigue, frequent incidences of data breaches and the complexity of the online privacy problems “may have started generating audience fatigue and reduced attention” to the online privacy issues (p. 2).

Choi et al. (2018) contend that “privacy concern... does not account for the range of users’ responses to privacy risk,” as “frequent data breaches may make people feel as though they have no control over personal information, and ultimately drive them into a state of resignation about online privacy” (p. 42). To test this argument, they investigated the impact of privacy concerns and privacy fatigue on privacy protection behaviours. Their findings are based on data gathered from an online survey conducted in South Korea in 2016. The survey included 324 respondents (163 males and 161 females). The results of the survey supported their hypotheses that,

a higher level of privacy concern will result in less intention to disclose personal information [and] less disengagement [in privacy protection. And] a higher level of privacy fatigue will result in higher intention to provide personal information [and] higher disengagement [in privacy protection] (Choi et al. 2018, pp. 44-45).

This observation implies that privacy fatigue lessens the impact of privacy concerns on privacy protection behaviours. Choi et al. (2018) also found that “privacy fatigue had more significant and intense impacts on users’ disclosure intention and users’ disengagement than privacy concern” (p. 48). This, they posit, could help to explain the general phenomenon of the privacy paradox.

In their study of peoples' intention to disclose personal information, Tang et al. (2020) focused on the role that privacy fatigue and privacy concerns play in App users' privacy protection behaviours. The analyzed data gathered from an online questionnaire that was completed by some 426 China-based WeChat¹² and QQ¹³ users between the ages of 20 and 40, 52.6% of which identified as female. Their findings suggest that "privacy fatigue is positively related to App users' intention of disclosing personal information [and] privacy concerns is negatively related to App users' intention to disclose personal information" (pp. 1103-1104). If applicable to the Facebook and/or Instagram context, this would mean that users who experience privacy fatigue are less likely to consider making use of the minimal privacy protections these platforms afford than those who have privacy concerns(s). Thus, according to Tang et al., levels of privacy fatigue can contribute to the gap between people's privacy concerns and people's intention of sharing their personal information online. This result seemingly supports Choi et al.'s (2018) observation that "users with more privacy fatigue tend to put less effort into making privacy decisions" (p. 48). However, it merits noting that the gap identified by Tang et al.'s (2020) cannot be accurately described as a privacy paradox because these researchers focused only on intentions, not actual behaviours.

Related to the notion of privacy fatigue, is the concept of privacy cynicism which, according to Lutz et al., (2020), is "a core component of privacy fatigue" (p. 1173). Hoffmann et al. (2016) define privacy cynicism "as an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behaviour subjectively futile" (p. 2). In their study of the association between privacy cynicism and privacy protection behaviour, Hoffmann et al. (2016) conducted online group discussions and focus groups

¹² WeChat is a Chinese instant messaging, social media, and mobile payment app developed by Tencent with one billion monthly active users. See, <https://www.wechat.com/>

¹³ QQ is an instant messaging software service and web portal developed by Tencent with 597 million monthly active accounts. See, <https://im.qq.com/index/>

with 96 German Internet users, 37% of which identified as digital outsiders,¹⁴ 19% as digital immigrants,¹⁵ and 44% as digital natives.¹⁶ These authors identified uncertainty and insecurity, loss of control/powerlessness, mistrust, and resignation as four recurring themes associated with privacy cynicism. As Hoffmann et al., (2016, p. 6) put it, with the sense of uncertainty and insecurity, and powerlessness, “many participants reported a lack of understanding [of online privacy concerns]... and a lack of efficacy [with regard to their privacy protection behaviours].” However, the authors did not find privacy literacy to necessarily relate to the sense of mistrust, insofar as both high- and low-skilled participants were observed to “speculate about selfish and sinister motives” of service providers (p. 6). Moreover, skilled users were found to “more readily resort to resignation,” as they tended to observe that “control, for a regular citizen, is hypocrisy” (p. 6). Overall, Hoffmann et al. (2016) propose that “privacy cynicism moderates (i.e., weakens) the effect of privacy concerns on protection behaviour” (p. 7), which leads them to call for future research examining “the relationship between privacy skills... and cynicism” (p. 8).

Some four years later, a number of the researchers who had been involved in the Hoffmann et al.’s (2016) study further investigated factors contributing to privacy cynicism by conducting another survey. The ‘new’ survey received 1008 responses from participants based in Germany, 51% of which identified as female. Drawing from a quantitative analysis of the survey data, Lutz et al. (2020) found that “Internet skills have a significant negative effect on uncertainty, powerlessness, and resignation... [but] do not counteract mistrust in Internet companies” (p. 1178).

¹⁴ In the context of this particular study, the term digital outsiders refers to “elderly people who hardly use the Internet and are cautious and inexperienced in using Internet applications.” See, Hoffmann et al., (2016, p. 5).

¹⁵ In the context of this particular study, the term digital immigrants refers to Internet users who have “intermediate technology enthusiasm, rather high Internet use intensity, rather broad spectrum of uses, rather high level of computer and Internet skills.” See, Hoffmann et al., (2016, p. 14).

¹⁶ In the context of this particular study, the term digital natives refers to Internet users who have “high technology enthusiasm, high Internet use intensity, broad spectrum of online activities, high level of computer and Internet skills.” See, Hoffmann et al., (2016, p. 14).

In other words, an Instagram user with advanced Internet skills is likely to know more about how to protect their online privacy and to be confident in that knowledge than users with a lower level of Internet skills. However, this same knowledge is just as likely to make these higher skilled individuals dubious of Instagram and/or any other social media platform.

Lutz et al. (2020) suggest that when it comes to privacy protection behaviours, privacy cynicism is negatively associated with resignation, positively associated with mistrust, and not associated with a sense of insecurity and uncertainty, and powerlessness (p. 1180). Moreover, they also maintain that privacy cynicism and privacy concern are positively associated “in the form of mistrust, uncertainty, and powerlessness,” but negatively associated with “resignation” (p. 1178). In other words, with their higher mistrust towards platform companies, the high-skilled users are less likely to acquiesce to disclosing their personal information.

Thus, there appear to be two points of divergence between the findings of Hoffmann et al. (2016) and Lutz et al. (2020). First, Lutz et al. (2020) conducted a quantitative study whereas its earlier counterpart mainly used qualitative research methods. As such, Lutz et al.’s (2020) study lacks descriptive detail about the respondents’ specific experiences and perspectives. For the second divergence, Hoffmann et al. (2016) found a tendency that higher Internet-skill levels may lead to a stronger sense of resignation (e.g., high-skilled users who know how powerful and ubiquitous the means by which platform companies collect users’ personal information are just as likely as their less-skilled counterparts to acquiesce and disclose their personal data online because they tend to believe no existing privacy protection behaviours are actually effective). However, and as noted above, Lutz et al. (2020) found a statistically significant negative association between these two factors. This divergence might not be only due to the difference in the research methodologies used.

Reflecting back to Baruh et al.'s (2017) study, which also used a quantitative research methodology, we recall that these scholars found no statistically significant association between privacy literacy and the behaviours of disclosing personal information. Given that the Internet skills considered in Hoffmann et al. (2016) and Lutz et al. (2020) include one's knowledge of how to protect online privacy, Baruh et al.'s (2017) research result provides another possibility of how one's Internet skills affects the sense of resignation. On the other hand, Baruh et al.'s (2017) conclusion is rooted in the notion that the boundaries of privacy disclosure are context-dependent which, in turn, suggests that one's level of privacy literacy is hardly a determinant of one's behaviours when it comes to decisions about disclosing personal information.

2.6 Statement of Central Research Question

Relying on CPM theory to frame their study, Hinds et al. (2020) investigated the level of people's online privacy concerns and their behaviours to protect their privacy online right after the Facebook-Cambridge Analytica scandal had been exposed. Their project involved interviewing 30 Facebook users (20 females and 10 males), between the ages of 18-46, to examine the participants' understanding and knowledge of online privacy and their level of awareness of the scandal.

In presenting their work, these authors introduce the concept of 'privacy calculus' in reference to the process through which "individuals make privacy decisions by evaluating the potential risks and benefits of disclosing information" (Hinds, et al., 2020, p. 3). However, in the context of the Facebook-Cambridge Analytica Scandal, the concept of 'privacy calculus' is not applicable because the covert nature of Cambridge Analytica's operations meant that users "had no way of knowing that their data would be used, how it would be used, and therefore had no means to evaluate the costs/benefits of their interactions" (p. 3). Additionally, Hinds et al. (2020) discussed the potential role of privacy fatigue in people's attitude towards the online privacy

issues, as “people [might have felt] exhausted from hearing about (seemingly) endless data breaches in the news, and as a result feel that attempts to do anything to protect their data are pointless” (p. 3). To this end, Hinds et al. (2020) suggest that privacy fatigue can help to account for the gap observed between people’s privacy concerns and people’s privacy protection behaviours.

‘Networked privacy’ is another concept discussed by Hinds et al. (2020) that is applicable to both Instagram’s Data Policy and the Facebook-Cambridge Analytica scandal. It describes the “interconnection between a user’s privacy settings and those of other people” (p. 3). As indicated in Instagram’s Data Policy, Meta collects the information from one’s “networks and connections,” which includes the information from the accounts of one’s friends’. Also, in the Facebook-Cambridge Analytica scandal, most of the breached data were not provided by the Facebook users directly but indirectly via their friends who participated in the quizzes on *thisisyourdigitallife* and whose personal information also was breached.

There are several notable findings emerging from Hinds et al.’s (2020) study. The first is their observation of people’s propensity for a type of naivety that is characterized by a propensity “view online privacy simplistically” (p. 6). This naivety, the authors claim, often is couched in notions of ‘having nothing to hide’ and professing to find targeted advertisements useful. The pertains to the sense of powerlessness experienced by the participants in the wake of the scandal, which both Hoffmann et al. (2016) and Lutz et al.’s (2020) suggest is a typical of the mentality that feeds into privacy cynicism. The third notable finding to emerge from Hinds et al.’s is the observation that when it comes to actual privacy protection actions people acknowledge that they should check their privacy settings, but also express lethargy when it comes to regularly responding to a constant flow of over constantly changing security policies and data breaches.

Fourth is the pervasive antipathy associated with the idea of relinquishing one's social media accounts. At play here are the mixed emotions at play in tension between feeling "some form of anger or feeling of being 'fed-up' with Facebook" and a perceived need to maintain connections with others that keeps one locked into the platform.

My project aims to replicate Hinds et al.'s (2020) study within the context of Instagram. At the time of conducting my research, the Instagram platform is far more popular among young adults than its Meta counterpart Facebook.

With this in mind, the central research question guiding this project is:

Are Hinds et al.'s (2020) findings regarding people's perceptions of online privacy issues replicable among a sample of undergraduate students who are regular users of Instagram?

In seeking to address this question, this project investigates the two aspects of the privacy paradox:

- *What concerns do undergraduate students in my sample have about data breaches and Instagram's use of data to facilitate the targeting of advertising to their screens?*
- *What strategies do the undergraduate students in my sample use to protect their online privacy? And, do they view these strategies as effective?*

2.7 Conclusion

The global COVID-19 pandemic has changed peoples' relationship with social media platforms in many notable ways. Coinciding with this shift, and with concerns about what was learned from the Facebook-Cambridge Analytica scandal still relatively fresh, is a resurgence of interest in online privacy issues. As the discussion in this chapter has made clear, there is an ever present a gap between people's online privacy concerns and their actual privacy protection behaviours. My project seeks to contribute to this discussion by bringing to bear to the views of a sample of adults who are regular users of Instagram. In the next chapter I set out the methodology I used to conduct this investigation and present the findings that emerged.

Chapter 3: Methodology and Findings

This chapter sets out the methodology used to address the central research question, and the findings that emerged. The discussion opens with an outline of the research design for my project. This is followed, in Section 2, with a presentation of the results from the short questionnaire participants were asked to complete prior to being interviewed. Section 3 focuses on the participants' views about how Instagram connects to their personal data. The fourth section looks at the participants' knowledge about and perceptions of Instagram's data collection, as well as their understanding and attitude towards the ads that appear on their screens. The fifth section zeroes in on what the participants had to say about data breaches. Sections 6 and 7 deals with the strategies the participants reportedly use to protect their personal information while using Instagram and self-evaluations on the effectiveness of these strategies.

3.1 Methodology

3.1.1 Research Design

The objective of this research project was to conduct an exploratory investigation of attitudes of young adults who are regular Instagram users toward online privacy and the privacy strategies they use when engaging with this platform. Guided by my interest in the privacy paradox, I wanted to find out whether and how privacy naivety and feelings powerlessness identified by Hinds et al. (2020) in relation to Facebook users recruited from a university population might be manifest among a similar demographic of Instagram users. Given my desire to see if Hinds et al.'s findings were replicable in relation to a different social media platform and in the absence of any recent prominent media coverage of anything akin to the Cambridge Analytica scandal, I opted to use the same method as that which they reported using for their study. This approach entailed having

participants complete a short questionnaire about their Instagram usage and engage in a semi-structured interview within one meeting.

In seeking to replicate the approach used by Hinds et. al., I began by reaching out to the study's lead author, Joanne Hinds, Senior Lecturer, University of Bath, to ask if she and her co-authors would be willing to share with me the survey and questionnaire they had used. Unfortunately, she declined. This said, in their study, Hinds et. al., noted that they had relied upon on a modified version of the questionnaire Ross et al., (2009) had designed to examine Facebook usage, and I turned my attention to the same questionnaire. The Ross et. al., questionnaire asks about such things as time spent online, the use specific communication functions offered by the Facebook platform, membership in Facebook groups, attitudes toward Facebook, and considerations in posting personally identifying information to Facebook. In adapting the questionnaire for my study, I selected ten questions from the original questionnaire that were most salient for my purposes and revised them into the Instagram-specific context. Upon completing this exercise, I arrived at a questionnaire comprised of 16 questions (i.e., ten questions from Ross et al., and six 'new' questions I developed) that was divided into three sections (See Appendix 2).

Ross et al.,'s (2009) questionnaire is comprised of 28 questions. The questionnaire itself is divided into four sections examining respondents':

1. Basic use and attitudes toward Facebook – 7 questions;
2. Settings for specific security functions of Facebook – 5 questions;
3. Use of the basis Facebook functions and applications – 11 questions; and
4. General attitudes toward Facebook – 3 questions.

The four questions comprising the first part of my questionnaire were taken directly from the Ross et al., questionnaire. For these, I simply substituted the term 'Instagram' for 'Facebook.' The

second part of my questionnaire is comprised of nine questions that seek to gather information about respondents' Instagram privacy settings and their use of Instagram. The first four questions in this section are simplified and modified (so as to be Instagram-centric) versions of four questions from the second and third sections of the Ross et al., questionnaire. The remaining five questions focus on Instagram's 'Story' feature. One simply cannot examine Instagram use patterns without examining engagement with this iconic feature. Although the questions I developed around the Story feature are new, they were inspired by the types of questions Ross et al., developed regarding Facebook functions and applications. The last section of my questionnaire consisted of three questions, two of which were taken directly from the Ross et al., questionnaire and wherein I once again substituted the term 'Instagram' for 'Facebook.' The third question in the concluding section, which focuses on targeted ads, was novel. It was motivated by the fact that targeted advertising was a matter of consideration in Hinds et al.'s (2020) study. I opted to add this question so as to gain a general sense of the respondents' perceptions of the ads that appeared on their screens which would, in turn, allow me to draw comparisons with Hinds et al.'s findings.

The sample for my study was comprised of 20 undergraduate students from the University of Ottawa (12 females, 8 males) who were recruited through the university's Integrated System of Participation in Research (ISPR) program.¹⁷ My rationale for this targeted sample was purely instrumental in nature and centered on the ease of recruiting participants in a timely manner. The ISPR program is managed through the School of Psychology of the University of Ottawa and is a mandatory component of some introductory Psychology courses. It aims to encourage undergraduate students to participate in academic research in the Department of Psychology and other partner programs (e.g., Communication), and to provide university researchers with a steady

¹⁷ See, <https://www.uottawa.ca/research-innovation/inspire/discover-lab/ispr-student-pool>

pool of research participants. By registering to be research subjects and/or by viewing films on research methods in human behaviour, participating students can earn a four-percent course grade based on a total of four participation points. As per the ISPR guidelines, individuals who participated in my study each gained one course credit point towards one of their final grades. Aside from needing to be registered in the ISPR program the only other criterion for participation in my project was that participants needed to self-identify as Instagram users and between 18-25 years old (See Appendix 1).

Here, there are two important points that must be noted. First, my reliance on the ISPR program as a source for recruiting participants necessitated my targeting of only undergraduate students. To this end, my focus on participants in the 18-25 age range was a deviation away from Hinds et. al.,’ s recruitment parameters insofar as age was not one of their participant selection criteria.¹⁸ Indeed, the ages in their sample of 30 participants ranged from 18-46. The second issue of note is that, in following Hinds et. al.’s lead, I too elected not to look at differences in privacy concerns and perspectives on the basis of either biological sex or gender. However, I did not make this decision until my sample pool had materialized. Although I had initially toyed with the idea of incorporating this into my analysis, when it became clear that my sample would not exceed 20 participants, I decided there was little merit in further sub-dividing an already small sample into even smaller groupings as any differences identified would have no merit in terms of generalizability.

Prior to administering my questionnaire, I piloted early iterations of it on three separate occasions wherein I asked the same three friends to complete and comment on whether the questions – both the modified Ross et al. questions and my new questions – were clearly phrased.

¹⁸ Hinds et. al., had two selection criteria. Participants had to: (i) log into Facebook once a day, and (ii) be willing to discuss their Facebook-related activities and opinions.

This also enabled me to ensure that my friends were interpreting the questions in the manner I intended. The feedback from the first meeting indicated that some of the questions I was asking about Instagram's 'Story' feature were not clear, especially those pertaining to specific 'Story' functions. Based on the feedback received, I revised these particular questions. In the second piloting session, my friends suggested I add more options for the question asking about reasons for blocking/restricting/muting other Instagram accounts. Based on their feedback and the variety of answers they provided to this question, I opted make this question open-ended. At the third piloting session, my friends indicated that they now found all the questions easy to understand, and that the questionnaire could be completed within 15 minutes. The discussions in this third meeting also enabled me to ascertain that the revised questions in questionnaire elicited the types of responses I was looking for.

To ensure the appropriateness of the questions in my interview protocol, I submitted the questions I planned to ask to two informal pilot sessions with friends who use Instagram regularly. In these mock interviews, I asked my friends both to answer to the questions I was asking and to let me know whether the questions were clearly phrased. This enabled me to ensure my friends were interpreting the questions in the manner I intended. The reactions and responses of my friends during the first session indicated that they were able to understand all the questions as I intended. However, I felt some of their responses were overly vague. With this in mind, I developed some 'nudges' to the questions that I employed at the second pilot session. These nudges enabled me to gently prod my friends for clarifications about the details of the perspectives they expressed. In this way, I was able to ascertain that the interviews allowed to me to gather the types of research data I was looking for. In the end, the interview protocol I arrived at consisted of 10 questions (see, Appendix 3).

3.1.2 The Interviews

Students registered to participate in my project via the ISPR portal. Forty timeslots were opened for inscriptions, with spots allocated on a first come, first serve basis. Some 30 students registered. However, ten students failed to attend their scheduled meeting.¹⁹ Hence, the final total sample size for my project was 20. All 20 meetings were conducted during a three-week period spanning from November 17th and December 7th 2022 (see Appendix4). In keeping with the public health guidelines in place at the time, all interviews took place virtually via the Zoom video conference platform. The use of Zoom had the added benefit for facilitating the video and audio recording of the meetings.

Prior to the start of each meeting, the participants were asked to read the informed consent form I shared with them and to return a signed copy to me. Once I received the signed copy, the meeting officially began. The first stage of the meeting involved giving every participant 10 to 15 minutes to complete the questionnaire before moving on to the interview portion of the meeting. The total duration of each meeting was 45 to 60 minutes. Upon completion of the meetings, the audio recordings were transcribed automatically using Zoom's 'Transcription' feature. To ensure the transcripts were precise and correct, I listened to the recording again against the generated transcripts and corrected any errors.

The analysis of the transcripts was rooted in an 'open coding' approach. This is a technique that involves breaking "data apart to delineate concepts or categories to present chunks of data (themes)" (Croucher & Cronn-Mills, 2019, p. 164). First, I carefully read through each transcript.

¹⁹ As part of the ISPR operational protocols, after each meeting, I was required to log attendance at the ISPR portal. Students who had registered to participate but who failed to attend without having advised me ahead of time were logged as 'unexcused no-show,' which meant they did not receive the 1% credit. Those who advised me in advance of their inability to attend were logged as 'excused no-show' and received the 1% credit despite their absence.

In accord with the interview questions, I sought to categorize the contents of the interviews into six themes:

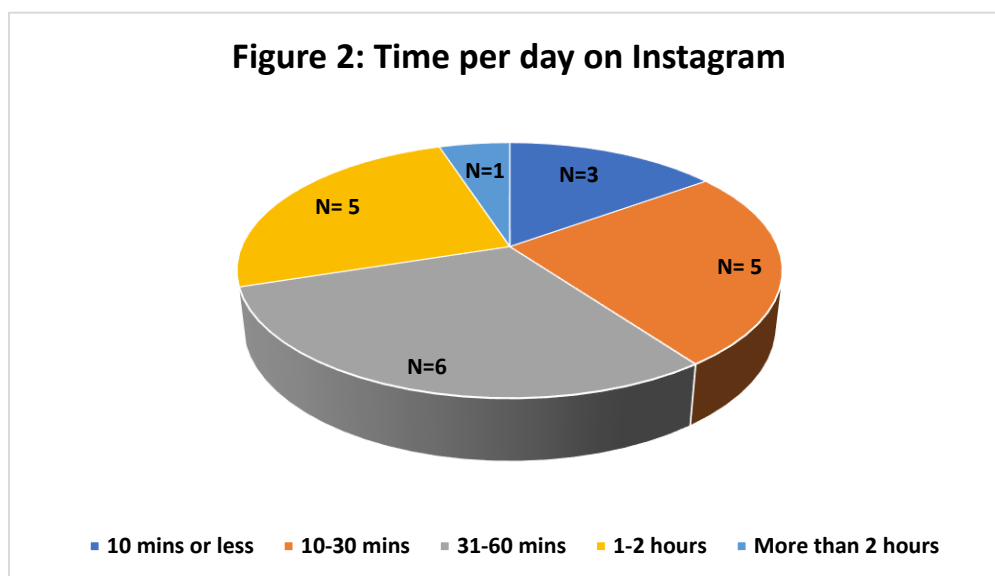
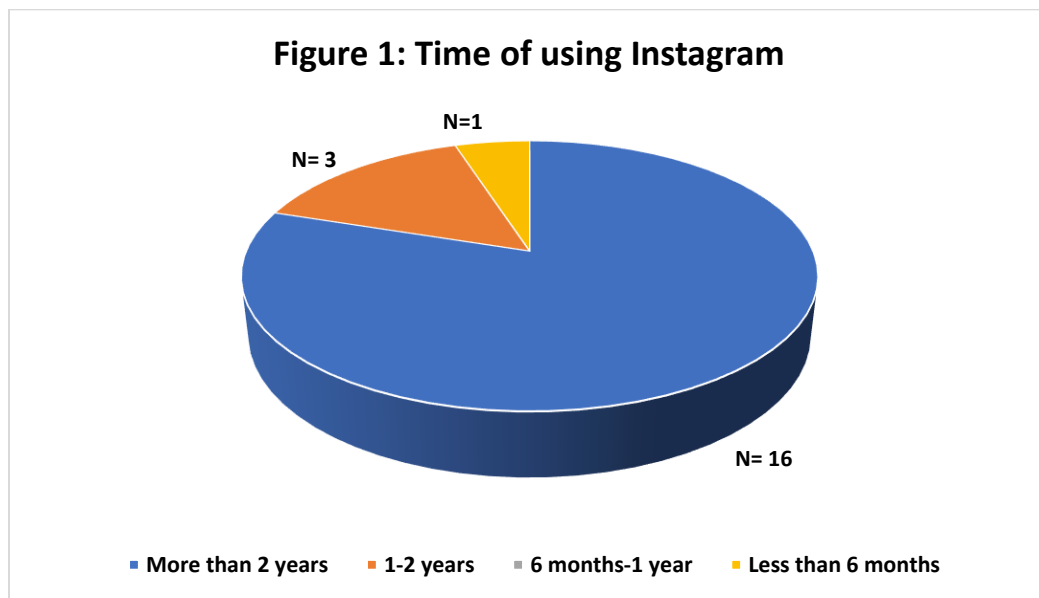
1. concerns about Instagram connecting to users' personal information;
2. knowledge about Instagram's data collection;
3. knowledge and concerns about data breaches;
4. privacy protection strategies;
5. intention to leave Instagram; and
6. shifting platform preferences.

Next, I re-read each interview transcript file looking for common/shared ideas that emerged from the responses to each of the above six themes. For example, to analyze responses pertaining to the first theme, concerns about Instagram connecting to users' personal information, as I read each interview transcript I highlighted all references to unawareness of Instagram connecting to users' personal information in blue, references to not having any concerns about this issue in violet, the mentality of 'nothing to hide' in green, and finding Instagram connecting to users' personal information helpful in red. Once I had read through and colour-coded all the responses for this theme, I then created a spreadsheet to collate all the sentences/phrases into groups in accord to the latter categories. This was the process I followed for each of the above six themes. In so doing, I was able to uncover similarities and differences between participant responses both within and across themes.

I then re-analyzed the transcripts using the same process as above but this time reorganizing the responses into a new spread sheet in accord with six categories of direct interest for my project: privacy literacy, privacy concerns, social privacy vs. institutional privacy, privacy protection strategies, naivety, negotiable commodity rather than basic right.

3.2 Summary of Questionnaire

Prior to each interview, the participants were asked to complete a short questionnaire comprised of 16 questions that explored various aspect of their Instagram use. The majority of participants indicated that they had been using the platform for two or more years (see, Figure 1). Likewise, a majority of participants claimed to spend between ten minutes to two hours per day engaging with Instagram (see Figure 2).



The information provided in Table 2 sets out the participants responses to questions dealing with their emotional engagement with Instagram. A majority of respondents agreed or strongly agreed with the statement “Instagram is a part of my everyday life” and “I would be sad if Instagram is shut down.” The sample was more or less equally divided about whether they felt out of touch when they had not logged into Instagram for some time.

Table 2. Participants’ Emotional Engagement with Instagram (N=20)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Instagram is a part of my everyday activity	2 (10%)	2 (10%)	5 (25%)	9 (45%)	3 (15%)
I feel out of touch when I have not logged on to Instagram for a while.	3 (15%)	7 (35%)	2 (10%)	8 (40%)	0
I would be sad if Instagram is shut down.	2 (10%)	2 (10%)	4 (20%)	11 (55%)	0

The next three questions dealt with the privacy settings the participants used when engaging with Instagram (see, Table 3). Seventy percent (n=14) of respondents reported setting their accounts as private, with the other 30% (n=6) reporting having their accounts set as public. The participants were also asked whether they allow others to comment on their posts and/or if they allow themselves to be mentioned or tagged by other Instagram users. As the information in Table 2 shows, the majority of participants reported allowing anyone to comment on their posts and to mention or tag them.

Table 3. Participants’ Privacy Setting on Instagram (N=20)

	Everyone	Both people you follow and your followers	Only people you follow	Only your followers	No one
Who do you allow to comment on your posts?	9 (45%)	8 (40%)	1 (5%)	0	2 (10%)
Who do you allow yourself to be mentioned by?	13 (65%)	5 (25%)	0	0	2 (10%)

Who do you allow yourself to be tagged by?	12 (60%)	6 (30%)	1 (5%)	0	1 (5%)
---	----------	---------	--------	---	--------

The third section of the questionnaire queried the participants' use of Instagram Story.²⁰ Some 75% (n=15) of participants reported using this feature. Of these 15, seven (n=7) reported allowing everyone to see their Stories, five (n=5) claimed to only allow Close Friends²¹ to see their Stories, and three (n=3) indicated they allow everyone except for the selected accounts to see their Stories.

In terms of who the participants allowed to reply to their Stories, eight (n=8) reported giving everyone permission to do so, five (n=5) indicated only giving people they follow this permission, and two (n=2) claimed to not have any idea who has access to reply to their Stories. As shown in Table 4 most of the participants who use the Instagram Story feature allow their Stories to be shared in others' Stories and messages but do not automatically share their Instagram Stories to their own Facebook Stories.

Table 4. Participants' Instagram Story Settings (n=15)

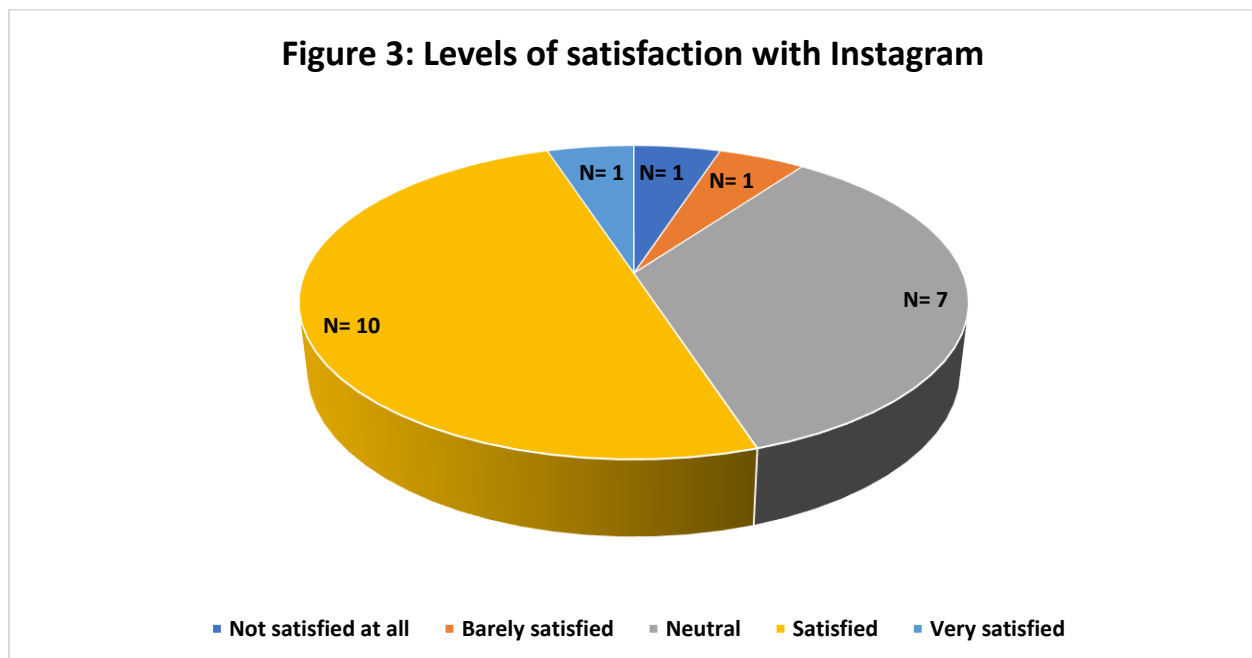
	Yes	No
Do you allow people to share your Stories to their Stories?	14	1
Do you allow people to share your Stories in their Messages?	14	1
Do you automatically share your Instagram Stories to your Facebook Stories?	1	14

The questionnaire also asked whether the respondents have ever restricted/blocked/muted the accounts of others. Nineteen participants (95%) answered yes, with 12 indicating they had restricted/blocked/muted 1-10 accounts, five (n=5) noting they had done so for more than ten

²⁰ 'Story' is a feature of Instagram that "allows users to post photos or videos that automatically disappear within 24 hours" (Read, 2022).

²¹ An Instagram feature that allows the users "to grant a subsection of followers special permission to view private Stories" (Oladipo, 2022).

accounts, and three (n=3) specifying they had no idea how many accounts they had restricted/blocked/muted. These 19 participants were also asked to provide the three main reasons for which they had restricted/blocked/muted accounts. The most frequent responses (n=14) were associated claims of “people I don’t like” or variations thereof. The second most frequent reason given (n=9) had to do with taking action against “fake/spam accounts,” followed by (n=8) actions taken against harassment messages.



The fifth section of the questionnaire had to do with the advertisements the participants see on their screens when using Instagram. From the results of the questionnaire, 11 participants were not bothered by the ads on their screens while nine (n=9) felt bothered by them. Sixteen (n=16) participants did not think these ads are helpful, while four (n=4) participants found these ads helpful.

The last question asked respondents about their levels of satisfaction with Instagram. The results are shown in Figure 3. More than half (n=11) of respondents reported being either satisfied or very satisfied with the platform, with 35% (n=7) reporting being neutral about it.

3.3 Perspectives on Instagram Connecting with Users' Personal Data

Only one of 20 participants, (P14), reported being unaware that Instagram connects to their personal information when they access their account. Of the 19 other participants, seven (n=7) (P1, P3, P4, P5, P9, P10, P16) claimed to have no concerns about this practice, of which five (n=5) (P1, P3, P9, P14, P16) indicated that their lack of concern hinged on them not being important people and, as such, having nothing to hide. Some of the views expressed in this regard included:

P3: "I think my personal data is not worth being stolen or being watched;" and

P9: "[I] don't believe that some companies will use my personal information to do something."

One member of this group, P10, went a bit further stating, "I don't see it as a problem because that's how it helps me to want to go on Instagram," because they believed that they received more personalized feed content due to this connection between their personal information and Instagram. The two others within this group – P4, P5 – did not provide any reason for their lack of concern when asked about their position.

Of the ten remaining participants who expresses awareness of Instagram connecting to their personal information, eight (n=8) (P2, P8, P11, P12, P13, P17, P18, P19) expressed concerns about this matter. However, six (n=6) (P2, P8, P11, P12, P13, P17) did not provide any details as to what underpinned their unease, or offered only vague ideas, like "when sometimes I post, I don't want random people to see" (P2), "algorithm can get to know your personality" (P12), "If you stop on one page, it gives more ads and never stops" (P13). Only two participants offered clear relations for their belief that Instagram connecting with their personal information was a cause for concern.

According to these Individuals:

P 18: "Privacy should be a guaranteed right on the Internet, allows open expression of views... and it's not guaranteed now."

P 19: "I think the world we live in today like everybody sees your data. We have lives manipulated by data."

The views of these two individuals suggest that they think their personal information has meanings beyond their personal level.

The three (n=3) remaining participants (P6, P7, P15) indicated that although Instagram's collection of personal data *should* be a source of concern, they did not have any personal concerns about the matter and, as such, did not pay much attention to it. Echoing the dominant view expressed among those who expressed no concern, P6 and P7 reported that they, as common users, would never be special enough to be the ones whose data is likely to make any difference. In the words of P6, "they know a lot about so many people and so many accounts, so ultimately what makes me special if they know all this information?" The third participant in this group, P15, pointed out,

"I kind of try not to think about it... I just feel you cannot do anything about it. I feel it's going to happen anyway."

Interestingly, there was one participant who seemed indecisive about this matter. P11 began by stating "that's why I don't use social media a lot [Instagram connecting to their personal information], but that's how you stay in contact with your friends." They, then seemingly contradicted themselves by adding "Personally, I don't care because I don't have any secret information, I'm not a famous person or anything."

It merits noting that among the ten participants who found Instagram connecting to their personal information to be either a source for concern or who indicated they should be concerned, the unease they expressed varied from P15's observation that Instagram's actions were "scary," to P13 "have[ing] a few concerns about that, but not too crazy." There were four (n=4) participants (P7, P8, P11, P19) who revealed that their levels of concerns had reduced since they had stopped posting pictures to, or stopped, using Instagram. For example:

P8: "I don't post very often, so I don't think there are many things I need to worry about."

P19: “I don’t like people to know my data, but I don’t think they know much, because I don’t use it much.”

This said, facing the fact of Instagram connecting to users’ data, most of the participants either showed privacy indifference or lacked awareness of what is really concerning in this issue.

3.4 Participants’ Knowledge of Data Collection

When asked about the type(s) of data Instagram collects from its users and why it collects this data, the responses provided by most participants suggested they possessed only a broad general sense of Instagram’s data collection practices. Put simply, none of the responses conveyed in-depth knowledge and understanding.

In terms of awareness levels about the type(s) of data gathered, fourteen (n=14) participants indicated being aware that their data was being collected. In this group, ten (n=10) expressed that they were not sure what information Instagram is collecting but gave two to three examples of types of information they believed Instagram gathers. The remaining four (n=4) appeared to be more certain when answering this question. Further, within this group of 14 participants, ten (n=10) (P1, P5, P6, P8, P10, P11, P12, P13, P15, P18) mentioned Instagram collects content-related information such as browsing histories, search histories, likes and dislikes, comments, and interests. Seven (n=7) participants (P2, P6, P7, P13, P17, P18, P20) indicated awareness of Instagram collecting users’ basic information including names, phone numbers, email addresses, dates of birth, and locations. The responses of three (n=3) participants (P1, P13, P18) focused on use-related considerations. Specifically, the amount of time that users spend online, the frequency with which users log into their accounts, and the times of day during which they do so. P18 further

mentioned the concept of metadata,²² stating “essentially, they are collecting the metadata of what you are accessing.” This individual was the only participant who was aware that Instagram is not just selectively collecting certain types of users' data but instead collecting all traces users leave on Instagram as well as their activities at other locations across the Web including other platforms.

Four (n=4) participants (P4, P9, P16, P19), indicated being aware their data was being collected, but not knowing what specific data Instagram gathers. Two (n=2) participants (P3, P14) reported not knowing that Instagram collects user data.

The participants' understanding of the reasons for Instagram collecting their information fell into three categories. Eight (n=8) participants (P1, P2, P3, P8, P9, P14, P15, P20) reported not knowing why Instagram collects user data. Another eight (n=8) (P6, P10, P11, P12, P13, P16, P18, P19) indicated it was for advertising purposes. Four (n=4) participants (P4, P5, P7, P17) specified that Instagram collects user data in order to provide users with more personalized content and, thereby, encourage them to engage heavily with the platform. As an interesting aside, it merits noting that none of the participants offered more than one reason for Instagram's data collection practices.

A noteworthy feature of the responses to the above queries was the personalized nature of the views expressed by some participants. For instance, two (n=2) participants expressed that they did not care about Instagram's data collection activities because they had nothing to hide:

P3: “I feel everything they know is just what kind of person I am. I don't care if they know. I won't feel unsafe.”

P12: “There's nothing that I have to hide.”

Two (n=2) other participants expressed their sense of powerlessness toward this issue:

²² According to Greenberg (2017, p. 21), “Metadata has been loosely defined and popularized as data about data, information about information. More comprehensive definitions address metadata as structured data supporting functions associated with an object, an object being any ‘entity, form, or mode.’”

P4: “It is concerning because you don’t have any privacy... but so long I can’t change it.”

P11: “That’s scary, but there’s nothing we can do about it.”

P17 suggested this was an issue of concern but that they nonetheless felt safe as a user. As they put it, “I am concerned, but I don’t think the company itself is a danger to the users, but if this information gets leaked to other users, then that’s when it becomes a problem.” Echoing this view, P5 saw this issue in terms of pros and cons,

“they’re [Instagram] not giving you personal space to your personal affairs, but the pros are that... they know the things that you like to do, things that you like to see, and things that you’d like to post, so the moment that starts changing may alert them in a certain way that something is going wrong, and if you’re in a problem or something they could help you.”

P7, likewise, suggested feeling like their privacy was being breached, but thought this breach was reasonable because “it’s part of the agreement that you sign once you start up on Instagram; so, it’s kind of what you are signing up for.”

Following the discussions of the reasons for Instagram collecting users’ data, the participants were further asked about their knowledge of, and attitudes toward, targeted advertisements. This was a follow-up to responses each participant had provided to the questionnaire they had completed prior to the interview.

During the interviews, eleven (n=11) participants (P1, P4, P6, P7, P10, P11, P12, P13, P17, P18, P19) reported being aware that the targeted ads emerging on their Instagram pages are a product of the information Instagram data collects about them and the algorithms it uses. Nine (n=9) participants (P2, P3, P5, P8, P9, P14, P15, P16, P20) reported having no idea of how the targeted ads work. One individual in this group, (P20), claimed they had never seen any ads on their screen. Others within this group seemed surprised to learn about the connection between

Instagram's data collection practices and the ads users see. P15, for instance, said "that's kind of gone scary." P2 went a bit further, stating

"It's kind of invading people's privacy. I feel it's not talked about enough," and further commented "technically, no one wants to read the policies, right? I think they should add another way to show..."

This said, not everyone in this group held a negative perception of how Instagram promotes ads. P9, for instance, was ambivalent about the matter, stating, "I never pay attention to them, so I don't care." P5 seemed equally unphased about how the ads appear on their screen, not least because they reported finding the ads helpful. As they put it, "It's like you are helping me but also helping yourself, but you don't tell me what you are doing."

As should be clear from the preceding discussion, with the exception of one individual, P18, by and large participants lacked knowledge and understanding of both the information Instagram gathers from users, and the connection between the data collected and the advertisements to which one is exposed on the platform. When reasons were provided, they were by and large anchored in folk theory understandings.

3.5 Data Breaches

When exploring the participants' perceptions and concerns regarding breaches, most provided responses that suggested a lack of familiarity with this topic. When asked whether they recalled hearing of any data breaches, nine (n=9) answered, never (P1, P3, P4, P5, P9, P10, P13, P14, P20). Four (n=4) participants (P2, P7, P12, P19) confirmed they had heard of some incidents related to data breaches from the news but could not recall any specific details about what had happened or who what involved. To these 13 participants, I subsequently mentioned the 2018 Facebook-Cambridge Analytica scandal as an example of a well-known data breach. Even with this gentle

refresher, only one (n=1) participant, P13, indicated having any recollection of, perhaps, one of the best-known data breach incidents in recent history.²³

Having been provided with a brief overview of the Facebook-Cambridge Analytica scandal and the types of concerns to which it gave rise, three (n=3) participants indicated that they failed to see why this incident should be of any concern to them:

P1: “If it doesn’t affect me directly, I don’t think I have an issue with that.”

P3: “Maybe they can get money from the US presidential election, but it doesn’t mean they can do that in other countries... I still don’t get how this affects the election result. People should know what they will vote for, so they should not be affected by the ads.”

P20: “I don’t get it that nothing happened to me.”

The first reaction of two (n=2) other participants was to question the legitimacy of Facebook’s behaviour in this incident:

P5: “I think it’s kind of a crime.”

P7: “It sounds very illegal, and it’s very unethical.”

Another two (n=2) individuals did express tempered concerns:

P4: “If they really try to use the data to win the election, it is not right.”

P10: “Cuz you can end up being in stuff you don’t wanna be in. I think it’s an issue.”

The remaining six (n=6) individuals in this group (P2, P9, P12, P13, P14, P19) of thirteen offered no comments about the scandal.

Among the seven (n=7) participants who did express an awareness of data breaches, five (n=5) provided examples of incidents of hacking. P15, for example, shared a story of a bank system

²³ See, “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far” from The New York Times (April 4, 2018), <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>; “Facebook Pays \$643,000 Fine For Role In Cambridge Analytica Scandal” from NPR (October 30, 2019), <https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal>; “Facebook data misuse and voter manipulation back in the frame with latest Cambridge Analytica leaks” from TechCrunch (January 6, 2020), <https://techcrunch.com/2020/01/06/facebook-data-misuse-and-voter-manipulation-back-in-the-frame-with-latest-cambridge-analytica-leaks/>

getting hacked and everyone's account information being posted online. P11, likewise, shared a story of an incident wherein someone had hacked the iCloud account of a social media influencer, obtained intimate pictures of the influencer in question, and blackmailed them to pay a ransom lest the photos be made public. The three others all shared stories about their friends' Instagram accounts getting hacked (P6, P8, P17).

The two (n=2) other individuals in this group spoke of instances wherein the users' information was leaked by the platforms. In both instances, the examples provided had to do with the leaking of health-related information. P16 related a generic story they had heard from the news about a healthcare service provider accidentally leaking the passwords to the accounts of all its patients. P18 offered a similar tale of a health app that had allowed its users' information to leak out.

When asked about the Facebook-Cambridge Analytica scandal, three (n=3) participants in this group made no comment (P15, P16, P17). The other four (n=4) offered different perspectives about this case. P11, for instance, suggested it was Facebook users, themselves, who were at fault. As they put it:

“It's our own responsibility. Some people just don't use social media because they are against all that collecting data stuff. So it sucks, but at the same time, I feel we are grown enough and responsible for our actions.”

By contrast, P8, who took issue with social media platforms employing their users' information for political purposes, had no qualms about the same information being used for advertising purposes.

“I think it's unfair... because it's not relevant [employing user information for political purposes]. Maybe selling the users' information for ads, that are still relevant. But I don't know why our personal information should be used in that kind of context [political].”

P6 indicated they had learned about the Facebook-Cambridge Analytica scandal in a course they had previously taken. For them, the details of this case were highly concerning. As they put it:

“Some people would think [the data breach happened in another country or the political ads are] not going to affect me, but no... the ads you are seeing have been chosen for you because the company has paid for your demographic to see it. It’s going to affect you... It’s so easy to affect people.”

P18 sought to draw a comparison between the Facebook-Cambridge Analytica scandal and political ads about the NDP they had seen on their Facebook newsfeed during the 2021 Canadian federal election period. They queried why so many NDP ads turned up on their feed despite their never having actively searched online for NDP-related information. From there, they went on to express deep concerns about online political ads. In their words:

“Your view can be affected by those [online political ads]. It’s a really powerful thing... There is a possibility that these people can do anything they want. They’ll do anything because they can do it. So it matters. It’s not something tied to any personal values, it’s something carried by everyone.”

In sum, most of the participants were not able to provide much in the way of specific information about incidents of user data gathered by platform companies having been breached. Even among the few who did recall at least one data breach that they had heard about, most only recalled individual instances of users’ information being hacked and leaked by other people.

3.6 Privacy Protection Strategies

When exploring the participants' privacy protection behaviours, 15 of 20 participants confirmed that they took actions to protect their personal information when using Instagram. Of the five (n=5) who did not (P1, P2, P3, P10, P16), one (n=1), P1, indicated that despite their doing nothing to protect their personal information when using Instagram, they always removed cookies²⁴ when using Google Chrome web browser.

When asked about the types of measures the participants used to protect their privacy when using Instagram, a number of practices were revealed. The most frequently cited strategy was the setting of one's Instagram account(s) as private. This approach was cited by nine (n=9) participants (P4, P6, P8, P11, P13, P14, P15, P17, P20) as their main privacy protection strategy. Another privacy protection strategy that was mentioned more than once was the setting of authentication which requires face ID approved for logging into Instagram. Two (n=2) participants (P7, P12) reported using this technique. Other privacy protection behaviours mentioned included receiving alerts on one's phone if something unusual was happening with one's Instagram account (P5), not letting random people follow or message them (P8), never clicking on the ads on the screen (P9), never posting on Instagram (P11), deleting browsing history (P15), using burner numbers and fake emails (P18), using VPNs (P19), trying to stay away from social media (P19), and only giving the platform email but not phone number (P20).

Among the 15 participants who indicated they used privacy protection measures when using Instagram, six (n=6) (P8, P11, P15, P18, P19, P20) specified that they employed more than one action to do so. Some of the reported combinations included setting one's Instagram account as private and receiving alerts on one's phone if any unusual activity was associated with one's

²⁴ Stouffer (2022) defines cookies as "small files used by web servers to save browsing information, allowing websites to remember your device, browser preferences, and associated online activity."

account (P3), setting one's account as private and never posting on Instagram (P11), setting one's account as private and deleting one's browsing histories (P15).

When these 15 participants, along with the individual who claimed to always remove cookies when using the Google Chrome web browser, were asked to self-evaluate their privacy protection strategies, six (n=6) maintained their actions were effective, with two (n=2) advancing the following claims:

P1 [in relation to removing Cookies while using Google Chrome]: "Most of the time when I take time to remove the cookies, I don't want that on my history or something like that. So, if I don't see that anywhere else on my computer or on my phone, or on anything like that, at that point, I'm kind of safe."

P7 [in relation to setting a two-step authentication for logging in to Instagram]: "Yeah, it's preventing hackers."

The other four (n=4) individuals in this group indicated that their information could never be completely safe, but that their actions effectively lowered the risk of their information leaking. The views expressed by these individuals included:

P8 [in relation to their having a private Instagram account and not allowing random people to follow or message them]: "I know even for a private account, people can still do many things, but the chances of that happening would definitely be lower."

P12 [in relation to their using authentication for logging in to Instagram]: "It's probably not that effective, but it's more effective than nothing."

P14 [in relation to their having a private Instagram account]: "Not [effectively protecting] all of it [personal information], but some of it."

P20 [in relation to their having a private Instagram account and only giving the platform their email but not their phone number]: "Yeah, some of them. I don't think all of them, but some of them."

Three (n=3) other participants among the 16 pointed out that despite their actions protecting their information from other people, they offered no protection from the platform:

P5 [in relation to their receiving alerts on their phone about unusual happenings on their Instagram account]: "For humans, they are effective. But

against the people that actually made it, I don't think there's anything effective because they have access to everything.”

P11 [in relation to their having a private Instagram account and never posting on Instagram]: “I think it allows you to protect yourself from other users, just like preventing people you don't know from seeing you. But I don't think it protects you from the big, the social media, like Instagram has our passwords and everything.”

P15 [in relation to their having a private account and deleting browsing history]: “It only protects from people, but not from Instagram.”

One (n=1) participant was not sure if their privacy protection actions are effective or not:

P19 [in relation to their using VPNs and trying to stay away from social media]: “I don't know, maybe a little bit... Even using VPNs or staying away, it's like, okay, I'm not giving you that much to use against me, but I think... I still use Instagram, you know, even just 10 minutes, I'm still using it.”

The remaining six (n=6) participants (P4, P6, P9, P13, P17, P18) in this group of 16 did not believe their privacy protection actions were effective. Two of these individuals stated:

P4 [in relation to their having a private Instagram account]: “The biggest issue is the people who own Instagram... some people would think it's effective, but truthfully, it's just for them to make them believe it's being effective. But it's really not because they could still have access to it. So, it's just to make people feel safer, so they continue using the platform.”

P6 [in relation to having a private account]: “It's so easy that your pictures go everywhere.”

The other four (n=4) did not elaborate on the reasons for their views.

In sum, most participants' reported privacy protection strategies consisted of basic measures such as setting their Instagram accounts as private. Furthermore, the strategies employed were oriented foremost to protecting their online privacy from other users rather than from the Instagram platform.

3.7 Leaving Instagram or Not

When asked if they ever thought about leaving Instagram to protect their personal information, all

the participants' responses showed that privacy security was not a notable factor of consideration in their decision making.

Among 20 participants, ten (n=10) affirmed that they have never thought of leaving Instagram (P3, P5, P6, P8, P9, P10, P13, P15, P16, P20). The most common reason given (n=7) was the need to maintain connections with friends and family. For example, P5 mentioned that they had more than 4000 friends on Instagram who were all from different countries, so they needed to stay on the platform to keep in touch with these friends. P5 also added,

“And family, you know, a lot of people use social media too. They are posting on social media. You need it for communicating with your family in order to know about things that are happening”

With regard to the other three (n=3) participants who reported not having thought about leaving Instagram, they did not provide any reason other than to note that they simply had not ever thought of leaving.

Six (n=6) of the 20 participants (P1, P2, P7, P11, P14, P17) reported thinking about leaving Instagram without ever following through such thoughts. However, all six emphasized that despite these thoughts, they did not want to leave Instagram permanently and that privacy and security considerations did not play into their periodical desire to leave the platform. Indeed, the most common reason (n=4) given for considering walking away from Instagram was a sense of it being an overwhelming distraction. Views expressed about this included:

P1: “Not permanently, but taking breaks”

P7: “Never for the security, but sometimes I think about it because of the usage, like I spend an hour on it, but it could be spent somewhere else, like doing my homework.”

P11: “The reason why I’ve thought about it is because of the pressure of social. I just wanted to focus on myself, and I felt like social media was like a distraction.”

P17: “Because sometimes being too stuck into the social media world can go a little overwhelming. It stops you from having a lot of real-life

interactions or just focusing on other important things that are going on in your life.”

In terms of the reasons given as to why these six participants had never actually left Instagram, two (n=2) indicated that it would make them lose connections with the world.

P2: “I will feel out of touch if leaving Instagram now.”

P11: “I haven’t done it because I just have a lot of memories, like a lot of conversations with people, pictures, and I just don’t wanna lose everything.”

Two (n=2) others spoke of being dependent on the platform admitted that they had never actually left Instagram because of their addiction:

P14: “I’m kind of addicted to it.”

P17: “You leave and then you start missing anything. I’m missing out so then go back to check what’s happening, and the addiction restarts.”

The last two (n=2) did not give any reasons as to why they never left Instagram.

Three (n=3) of the 20 participants in my sample (P4, P12, P19) reported that they had previously left Instagram only to return. Their reasons for having left Instagram were not linked with anything relating to privacy and security. All three made clear they had left the platform to focus more on either school or themselves.

Likewise, all three reported the main reason they started using Instagram again was the desire to avoid losing connections with the world and other people.

P4: “I’ve done it before. Back in Grade 11, I wanted to stay more focused on school because I was going into grade 12. I just deleted my account completely. Then like just recently I created another account... Social media is a very important way to make you come back to the world or any other people.”

P12: “I deleted all my social media for like a month during a final period, but then I got it back... It’s just easier because all my friends have social media.”

P19: “Before I came to Canada, I deleted all my social media, for focusing more on myself... [I came back] because I’m leaving for another country. I need to talk to my parents.”

Only one (n=1) person in my sample reported having completely left Instagram (P18). As with the others in the sample who had walked away from Instagram only to later return, their rationale for leaving had nothing to do with privacy and/or security considerations. Their departure from the platform, was, instead, tied to a sense that, as an app, “is very convoluted to use”. In their words,

“You can only use it on the phone. I spent an enormous amount of time trying to only use it on a web page.”

This person added that, ultimately, they had switched from Instagram to Twitter “for ease to use” when it comes to connecting with people.

The 20 participants were also asked if they believed it is possible for people today to live without social media. Among them, 15 thought it is impossible to do so and five (n=5) suggested it could still be done:

P3 [in relation to never thinking about leaving Instagram]: “It would be hard without Instagram when other people send me messages, but I can still live without Instagram... because I don’t post too many photos or stories [anyway].”

P7 [in relation to thinking about leaving Instagram but never having done that]: “For some people, there's more of like a personal emotional connection. But for others, it doesn’t really matter, it’s just for fun. I think I’m one of those people. I don't really post that often right now. I just posted my story sometime. So yeah, it depends on the level of connection or the dependency you have on Instagram.”

P11 [in relation to thinking about leaving Instagram but never having done that]: “Is it difficult? Yes. But we can totally do it. I'll say wish social media didn't exist and just say go back. Like how we were when we were kids, we would enjoy life with nothing.”

P18 [in relation to totally leaving Instagram but still using other social media] told a story that changed his mind while he had thought it would be impossible to live without social media before. He had a Tencent account with lots of friends who he got to know through the Internet on it. He thought that he would never leave Tencent because he needed to keep connections with all his friends, but later his account was stolen/hacked and he never got it back, so he was forced to leave Tencent. After that, he found his life still going on the same and did not feel actually lost anything. “I just found it’s actually not that hard.”

P19 [In relation to leaving Instagram before but having already come back]: “I had a friend. She doesn’t have a cell phone ever after she went to university. She can still talk to people, so I think it’s possible. You know, we live before we have those stuff.”

In sum, although a few participants reported that they had left social media or were thinking about leaving social media for various periods of time, none had ever considered permanently leaving Instagram, or social media more broadly, for privacy-related considerations.

3.8 Shifting Platform Preferences

It merits noting that when discussing their favourite apps, nearly half ($n=9$) of the 20 participants mentioned TikTok, with only four ($n=4$) identifying Instagram as their preferred platform. Moreover, 12 participants believed that TikTok, was the most popular app among their generation. However, among the 16 participants who did not identify Instagram as one of their favourite apps, three ($n=3$) emphasized that Instagram nonetheless remained their most *used* app for messaging their friends or families.

This suggests that, within my sample at least, Instagram may be more likely to be perceived as a communication tool that is thought of largely in an instrumental manner rather than in terms of satisfaction.

3.9 Conclusion

The findings presented in this chapter revealed the participants’ perceptions of online privacy issues from various aspects. Overall, the evidence suggests the participants appeared to lack privacy concerns and have low privacy literacy. Moreover, the privacy protection strategies they reported used reflected a level of naivety insofar as the reported behaviours tended to be linked to an oversimplified understanding of the Instagram’s data collection activities and its targeting of ads. The findings also imply the participants do not appear to consider online privacy as a right

that must be protected but rather a negotiable commodity that they can use to trade for services provided by the Instagram. In the next chapter, the implication of the findings for how undergraduate students perceive their online privacy are discussed in detail.

Chapter 4: Analysis

The discussion in this chapter analyses the implications for theory and practice of the findings presented in Chapter 3. In the first section I examine how the participants' levels of privacy literacy, their privacy concerns, and the privacy protection strategies they reported using converge and diverge from the findings of the studies reviewed in Chapter 2. The discussion in the second section considers showing the participants' attitudes towards the prospect of leaving Instagram for privacy-related reasons aligns with the findings of previous studies. The third section discusses the participants' naivety, from different aspects, when facing online privacy issues. The fourth section focuses on the tendency that people consider online privacy a negotiable commodity that they can use to trade for free services, rather a basic right that needs to be guaranteed.

4.1 Privacy Literacy, Privacy Concerns, and Privacy Protection Behaviours

4.1.1 Privacy Literacy

Bearing in mind Baruh et al.'s (2017, p. 29) definition of privacy literacy as comprising “declarative knowledge of privacy risks” and “procedural knowledge about how to protect one’s privacy,” the findings presented in the previous chapter suggest that the participants in my sample generally had low levels of privacy literacy. In other words, they seemingly lacked awareness of online privacy issues relative to the individuals who participated in the studies conducted by Brown (2020), Afriat et al. (2021), and Hinds et al. (2020).²⁵ It seems plausible that the difference between the findings of my project and those of the latter studies may be linked to two factors. First, the individuals in my sample were younger than those in the three studies cited above.

²⁵ The reader will recall that all participants in Brown (2020) reported being aware of the Facebook-Cambridge Analytica scandal. Likewise, more than two-thirds of the participants in Hinds et al. (2020) reported being aware of the scandal, with one third mentioning it without prompting. In Afriat et al.'s (2021) study, some two-thirds of participants reported being aware of the economic surveillance of online activities even prior to news of the scandal breaking out.

Indeed, they would have only been enrolled in elementary or middle school when news of the Facebook-Cambridge Analytica scandal first broke. Second, Brown (2020), Afriat et al. (2021), and Hinds et al. (2020) all conducted their studies in the wake of the scandal and, as such, their participants may have had a heightened level of privacy awareness or, at least, heightened sensitivity to privacy-related concerns compared to those who participated in my project.

This finding is simultaneously surprising and unsurprising. On the one hand, it is surprising because despite social media being integrated into to their daily lives, the participants seemingly had little sense of the foundational business model of social media platforms – i.e., they are pillars of the advertising industry that are able to provide free and/or personalized services by selling users' information – personal and other – to third parties (Mansell & Steinmueller, 2020; Arora & Agarwal, 2020; Xue, 2022). On the other hand, it is not surprising insofar as the participants may have been taking for granted the free services, they enjoy in exchange for being exposed to advertisements. In other words, given that one can largely ignore, or otherwise bypass advertisements to one's various social media feeds, and that one's daily life may not seem to be directly affected by the trade of personal and non-personal information, it is relatively easy for users to put aside online privacy considerations.

4.1.2 Privacy Concerns

In their investigations of how different variables impact the gap between people's privacy concerns and their actual privacy protection behaviours, the authors of the studies discussed in Chapter 2 focused on the privacy paradox. These authors seemingly presumed their participants were all concerned – albeit to differing degrees – about online privacy issues. Such an assumption, however, does not appear to hold in the case of the people sampled for my project. Indeed, the majority of participants in my study reported having only low levels of privacy concerns.

Although the participants in Brown (2020) reported heightened concerns about their privacy security after hearing about the Facebook-Cambridge Analytica scandal, none identified themselves as being sufficiently concerned so as to leave Facebook. Of ten participants, only one reported having once deactivated their Facebook account in response to the scandal (Brown 2020). In merits noting, however, that this individual also reported that, shortly thereafter, they had returned to Facebook to reconnect with their friends. In Afriat et al.'s (2021) study, which was conducted right after news broke of the Facebook-Cambridge Analytica scandal, the participants were found to be much more concerned about their social privacy than their institutional privacy,²⁶ with none viewing closing their Facebook account as a valid option for protecting one's privacy. This is consistent with the views expressed by members of my sample insofar as one third of my participants were seemingly more worried about hackers than misuse of users' information by social media platforms, and none viewed leaving Instagram as a realistic, let alone viable, option for protecting one's online privacy.

The participants in Hinds et al.'s (2020) study expressed a wide range of views about online privacy spanning from "I'm not bothered" and "I have nothing to hide," to "I'm extremely concerned" and "I feel powerless but there's nothing I can do." The participants in my project echoed these views, advancing comments like "I'm not anyone important" and "I can't change it [the fact that Instagram connects to their personal information] anyway." It also merits noting that, contrary to the participants in Hinds et al.'s (2020) study who articulated a sense of powerlessness but who had not resigned themselves to a loss of control, the individuals in my sample who

²⁶ The reader will recall that, social privacy refers to "the control of information flow about and when personal information is shared with other people" whereas institutional privacy pertains to "how institutions such as governments, banks and businesses, use or misuse the personal information" (Raynes-Goldie, 2010, n.p.).

expressed a sense of powerlessness had resigned themselves to this loss of control and had ostensibly given up on trying to take actions to protect their online privacy.

Here, differences between concerns about social privacy and institutional privacy seem to be at play insofar as this dichotomy can be understood as encompassing a distinction between data being leaked as a result of nefarious activity versus data being shared for commercial and/or other purposes. When one's personal information, like a date of birth, home address, and/or personal email address is leaked or stolen, the repercussions can be swift and, potentially, very negative (e.g., identity theft) for the victim. By contrast, the perception among members of my sample was that the sharing of users' details to third parties by social media platforms has little 'real' effect beyond influencing the types of targeted ads that appear on one's pages. It seems plausible that this perception may help to explain, at least in part, why the undergraduate students with whom I spoke were seemingly unphased about any potentially negative consequences arising from the data collection and reselling activities of social media platforms.

4.1.3 Privacy Protection Behaviours

As was reported in Chapter 3, three quarters of participants in my sample (15/20) claimed to take actions to protect their privacy while using Instagram. This said, the most frequently cited means for doing so was the setting of one's account as private. This finding is consistent with the observations made by Hinds et al. (2020) in their study of Facebook users. In that study, the participants' privacy protection actions seemed to "be limited to their own posts/disclosures to their friends [or] followers [or other users]," rather than considering "the broader implications of their interactions and how these may inform the design of targeted advertisements" (Hinds et al., 2020 p. 8). In the case of Instagram, as with Facebook, setting one's account to private only prevents

other random users from viewing one's account page and/or seeing what one posts. It does not stop Instagram from collecting users' data and targeting ads to them accordingly.

Here too, we observe the distinction between social privacy and institutional privacy at play. Specifically, the top three reasons given for restricting/blocking/muting other Instagram accounts by those in my sample had to do with avoiding people they did not like, fake/spam accounts, and/or harassment. For these individuals, an onus was placed on taking action to protect themselves from getting 'hurt' by other users.

The participants in Hinds et al.'s (2020, p.8) study reported being aware that "they 'probably should check' their privacy setting, and read the Facebook's terms and conditions." However, they also intimated that they were not inclined to do so and seldom had the time for such actions. According to Hinds et al., (2020) this state of affairs largely reflects "people's lethargy over constantly changing security policies and data breaches" (p. 8). By contrast, none of the participants in my study expressed any sense of feeling the need to check and/or update their privacy settings, (re)read Instagram's terms or policies, or generally take more actions – whatever they may be – to protect their online privacy. Indeed, even my describing to them Instagram's data collection activities as described in the platform's data policy seemingly made no difference in their views.

This perspective is not particularly surprising given that most people consider the privacy policies of social media platforms to be too lengthy and complex to invest their time and effort into reading them (Steinfeld, 2016; Sandle, 2020; Nelli, 2022). It was with this concern in mind that Soumelidou and Tsohou's (2019) proposed a new more user-friendly format for Instagram to use to presenting its data policy to users. Despite – or perhaps because of – the potential of

Soumelidou and Tsohou's proposed format to facilitate and raise users' privacy awareness levels, Instagram's Data Policy continues to be presented in the conventional lengthy and verbose way.

This said, one cannot help but question whether Instagram users would take the time to read the platform's Data Policy even if was offered in a short, concise, and easily understandable manner. At issue here is the contractual form users enter into with Instagram when they use the platform. Specifically, if agreeing to its policies is a necessary condition for accessing and using free of charge the services Instagram makes available, it seems plausible that users who valorize these services are likely to have little motivation to invest themselves in reading, let alone understanding, the Data Policy and its broader implications regardless of how it is presented. This, in turn, presumably plays a role in facilitating the transformation of thinking about privacy as something to be protected on the basis of rights into something to be treated as a commodity.

4.1.4 How Privacy Literacy, Privacy Concerns and Privacy Protection Behaviour Are Associated

Given the small size of the research sample (N=20), the information gathered from both the pre-interview questionnaire and the interviews could not be submitted to any statistical analyses that might identify statistically significant associations between variables. This said, the findings emerging from my project do appear to be broadly consistent with those of Baruh et al. (2017) who identified a statistically positive association between levels of privacy literacy and levels of privacy concerns in their sample of participants. In the case of my project, this appeared to be manifest in the identification of a large portion of the sample members (n=14) who reported not knowing or not being sure about what information Instagram collects from its users and/or who had only limited awareness of incidents of social media-related data breaches (n=12) (i.e., privacy literacy) combined with their reported absence of concern about Instagram's data collection

activities and/or its use of their personal information for commercial purposes (i.e., privacy concerns).

Bartsch & Dienlin (2015) likewise found that higher levels of privacy literacy led to more privacy protection behaviours being undertaken and a sense of feeling safer. In the case of my project, the individuals who demonstrated higher levels of privacy literacy also reported taking more actions to protect their personal information when using Instagram than those with seemingly lower levels of privacy literacy. However, these same individuals were also found to be more resigned than their lower literacy counterparts to the idea that there are no truly effective privacy protection strategies. To this end, the only participants who reported viewing their privacy protection behaviours as effective were those with lower levels of privacy literacy. Were this observation to be generalizable beyond my sample, it could be seen as challenging Bartsch & Dienlin's (2016) contention about elevated levels of privacy literacy being associated with people engaging in behaviors that make them feel safer when online.

Saeri et al. (2014) found no statistically significant association between privacy concerns and actual privacy protection behaviours. Paralleling this observation, Baruh et al. (2017) likewise found no statistically significant association between privacy literacy and information-sharing behaviours. In the case of my project, only a few of the participants who reported elevated levels of privacy concern put additional privacy protection strategies into action, with most reporting implementing even fewer privacy protection behaviours because they did not believe any privacy protection strategies were *actually* effective. Likewise, even those participants who were identified as having the highest levels of privacy literacy reported not being able to permanently stop using Instagram or other social media platforms in order to protect their personal information. Taken together, it seems plausible that both of these observations are at least minimally illustrative

of the phenomenon identified by both Saeri et al., (2014) and Baruh et al. (2017) regarding the absence of a relationships between privacy concerns and actual privacy protection behaviours, and between privacy literacy and information-sharing behaviours.

Hoffmann et al. (2016) proposed that “privacy cynicism moderates (i.e., weakens) the effect of privacy concerns on protection behaviour” (p. 7). Building on the latter study, Lutz et al. (2020) posited that the four main components of cynicism are: uncertainty, powerlessness, resignation, and mistrust. As discussed in the previous chapter, in my project, 11 participants expressed uncertainty about both the type(s) of information Instagram collects from users and why it does so. Ten (n=10) went so far as claiming they could not do anything to counter Instagram’s data collection activities, thereby articulating powerlessness. In terms of feelings of resignation, I observed this from five (n=5) participants who equated their sense of powerlessness as simply being a facet of the environment of surveillance capitalism in which we live. It was notable, to me at least, that none of the participants reported having any feelings of mistrust toward Instagram.

Overall, it seems plausible that within my sample three of the four elements of privacy cynicism – uncertainty, powerlessness, resignation – likely are having at least some effect on the participants’ privacy protection strategies. Interestingly though, mistrust was not identified as a potential motivator of either privacy cynicism or the implementation of privacy protection strategies.

Both Choi et al., (2018) and Tang et al., (2020) suggest that privacy fatigue is the element that negatively affects people’s privacy protection behaviours. The observations emerging from my project do not appear to accord with this claim insofar as when discussing data breaches and privacy concerns, approximately 90% (n=18) participants did not convey any sense of weariness with these topics. Only one (n=1) participant, who also demonstrated high levels of privacy literacy

and who reported privacy concerns, expressed that they tried not to think about the fact that Instagram connects to their personal data, adding that they did not believe there were any really effective privacy protection strategies.

Given that the research for this thesis took place during the COVID-19 pandemic, there are grounds for hypothesizing that being stuck at home and heavily reliant, if not dependent, upon social media platforms for socializing with others could contribute fueling cynicism about online privacy, especially in the form of resignation. As an important tool for people to work from home, obtain health-related information updates, and maintain connections with friends and family, people could hardly live without social media or, more broadly, social network services. It seems plausible that, this may explain, in part, the seeming absence of any association between the levels and types of privacy concerns and the actual privacy protection behaviours reported by the participants in my sample. In other words, despite any uncertainties about Instagram's data collection activities, the participants did not implement any substantive actions to protect their online privacy. Instead they resigned themselves to the fact the collection of their data is the cost of the accessing the services provided by Instagram and that, this cost was a necessary burden, especially in the pandemic context.

4.2 To Leave or Not to Leave; That Is Not the Question

The one issue about which all the participants in my project seemed most passionate was a steadfast refusal to entertain any notion of leaving Instagram or social media more broadly. For those who reported having contemplated this idea, the reasons they gave for having done so had nothing to do with privacy-related considerations. Here, I observe parallels between some of those in my sample and Brown's (2020) finding that students' perceptions of the Facebook-Cambridge Analytica scandal were not sufficient to get them to consider closing their Facebook accounts. As

Brown (2020) points out, the participants in that study appreciated the benefits Facebook brought to their lives and had resigned themselves to the view that their privacy was the cost of exchange for this social media service.

Three (n=3) participants in my project expressed similar views. While talking with them about the Facebook-Cambridge Analytica scandal, one (n=1) participant indicated that in the case of this scandal, it is social media users who should have taken the main responsibility rather than the platform because the affected users had chosen to sign the user agreement and use the platform for free. Six (n=6) other participants clarified that even though they did not like the idea of Instagram collecting data about them, using Instagram is a *necessity* in their lives. That is, they need to maintain connections with their friends, families, and the world, and Instagram is a vital means by which to do so. This, as the majority of participants in my project pointed out, was particularly so throughout the COVID-19 pandemic.

Afriat et al. (2021) observed that the participants in their study advanced three main reasons for not viewing leaving Facebook as a viable privacy protection option:

1. reliance on information provided by the platform;
2. 'addiction' to the platform; and
3. living without a platform equates with a desire to be unique.

The reasons given by 15 participants in my project as to why they would not leave Instagram to protect their personal information aligned with the first two above rationales. No participants conveyed anything akin to the third item.

In terms of Hinds et al.'s (2020) findings regarding this matter, they reported that none of those who had participated in their study were indicated being motivated in any way to leave Facebook explicitly because of the Facebook/Cambridge Analytica scandal. Here, one observes a parallel with the findings of my project insofar as the participants in both studies indicated the

desire to leave Instagram or other social media was not motivated foremost by privacy-related considerations. This said, unlike the resounding ‘no’ conveyed by the individuals comprising my sample when asked about the possibility of leaving Instagram, the participants in Hinds et al.’s (2020) study held more ‘mixed emotions’ about the possibility of leaving Facebook insofar as they reportedly felt they should leave Facebook but felt obliged to remain in order to “maintain connection with others” (p. 9).

One of the reasons given by the participants in Hinds et al.’s (2020) for not leaving Facebook was that they “consider Facebook to be a part of their history... [and] a part of their identity” (p. 9). This view was far from widespread in my sample, but one participant did express similar feelings in relation to Instagram, pointing out that they had a lot of memories on Instagram and, as such, deleting their Instagram account would mean losing part of themselves. This participant’s observation raises an interesting way of thinking about Instagram and/or social media platforms more broadly, insofar as it moves thinking away from viewing social media foremost as a basic tool with which large swathes of people engage daily, into something that is constitutive of their memories, histories, and even identities. Put simply, those in the age demographic comprising my sample have largely grown up using social media to record myriad aspects of their daily lives. Many of the photos and videos they have posted on their accounts are regarded as part of their indelible memories. Therefore, for them, social media is not just a daily tool, but even like a part of their being (See, for example, Pan, 2017; Mukwevho & Ngoepe, 2019).

4.3 Naivety

Hinds et al. (2020) reported that many of the participants in their study “tend[ed] to view online privacy simplistically” (p. 6) and, as such, were somewhat naive. This naivety, they claim, is comprised of four principal elements. The first centered upon the absence of privacy concerns

being linked with a sense of one having nothing to hide. This view, and/or the idea that in the absence of having elevated economic or social status one's information does not matter, was articulated by five (n=5) of the participants in my project. Hinds et al. (2020) further observed that the sense of having nothing to hide was more pronounced among those in their sample who lacked awareness of incidents of data breaches, a claim that also is consistent with what I observed in my sample.

The second element advanced by Hinds et al. (2020) as suggesting naivety on the part of the participants in their study was a sense of detachment from the Facebook-Cambridge Analytica scandal. Specifically, that they “considered themselves... unlikely to be influenced” (p. 6) by this kind of data breach, in part, because they believed themselves to be “‘well-educated’ about their political beliefs” (p. 6) and, therefore, unlikely to be subjected to targeted political advertising. In my project, one participant echoed this type of thinking. According to this individual, people are likely to be fairly certain about whom they plan to vote for at election time and, as such, the machinations of the Cambridge Analytical scandal were not likely to succeed because people would not have been that easily affected by the political ads.

Hinds et al.'s (2020) third element of naivety focused on their participants' perceptions of targeted ads, in particular, the notion of targeted advertising being useful. Here, one observes parallels with Afriat et al.'s (2021) observation that some participants in their study “considered surveillance an advantage in itself” because it conditioned the advertisements, they saw on their Facebook feed. Four (n=4) participants in my project indicated that they found the targeted ads that appeared on their screens to be helpful. However, unlike the participants in the two previous studies, the majority of which reported finding targeted ads annoying, 11 participants in my project claimed to simply ignore the ads on their screens. Indeed, one participant from my sample

maintained they had never noticed the presence of ads on their Instagram pages. This said, the aspect of naivety that was particularly pronounced in my sample was a seeming lack of unawareness that targeted ads are a direct result of surveillance.

The fourth element of naivety identified by Hinds et al. (2020) had to do with the participants being “unaware that personal information could be inferred through their interactions or via their friends’/followers’ interactions within their networks” (p. 6). I found this to also be case within my sample. Indeed, among the one third of participants in my sample who demonstrated a lack of privacy literacy, most appeared to be genuinely surprised upon learning that the information Instagram is collecting is not only about themselves, but also includes information about the accounts in their network communities (e.g., friends, family) and their interactions with these accounts (e.g., comments, private messaging).

There were two additional aspects of naivety I observed among the participants comprising the sample for my project that Hinds et al. did not touch upon. The first has to do with the participants' privacy protection strategies. As previously noted, the most frequently reported privacy protection strategy among the participants was simply to set one's Instagram accounts as private. Most participants believed this alone offered effective privacy protection. Four (n=4) participants reported that their privacy protection strategies include limiting the frequency of posting information to one's accounts. Among those who reported using this strategy, three quarters believed this to be an effective means of protecting one's privacy on Instagram. It merits noting that each of the latter strategies focuses foremost on protecting one's information from other individuals (i.e., social privacy) as opposed to protecting one's information from the Instagram platform (i.e., institutional privacy).

The second aspect of naivety among the participants in my sample pertains to the recognition of people's dependence on social media. Although all participants were unequivocal about their never permanently leaving Instagram or other social media platforms, four (n=4) nonetheless maintained that people could live fulfilling lives without engaging with social media. They viewed the idea of leaving social media as a theoretical possibility but could not see themselves doing so in practice. Equally noteworthy was a propensity among the participants to seemingly fail to recognize that the tight personal bond they held with social media was not limited to them but rather is widespread social phenomenon. When discussing their privacy concerns, the participants tended to only focus on whether and/or Instagram's data collection activities effects on them individually, with little to no consideration of the potential implications of a platform gathering, holding, and using for its own purpose's vast amounts of information about vast quantities of people. This was most evident in the pervasive lack of awareness among the participants that Instagram not only collects information about them as individuals but also of their interactions with other accounts.

Overall, the level of naivety identified among the sample participants is not particularly surprising given the low levels of privacy literacy they exhibited. In the absence of basic knowledge about the concept of surveillance capitalism, how algorithms work, and the complexity of networks, there is no basis for anticipating, let alone understanding, that targeted ads and platforms data collection activities are not just about individuals but have broad based implications across societies.

It is equally important not to lose sight of the mediating role of the COVID-19 pandemic period in fomenting strong dependencies on social media platforms, thereby potentially conditioning how people both perceive and understand online privacy issues. For example,

although the sample participants have seemingly become accustomed to encountering targeted ads and take them as a natural part of their pages, they would easily take these ads as just a part, a useless part at most, of the services they received from the platforms. In this way, they risk overlooking the fact that these ads constitute part of the price they are paying for ‘free’ services they receive.

4.4 Rights vs. Needs

At the core of the concept of surveillance capitalism is the notion of people’s personal data being commoditized and monetized which is a process that transforms people’s privacy from a basic right into a commodity that can be used to trade for other things (e.g., free services provided by the social media platforms) (Zuboff, 2015; Afriat et al.2021). In such a context, commercially motivated surveillance can come to be understood as an advantage rather than a rather than a violation of people’s basic right to privacy.

Such a shift in perspective may help to account, at least in part, for the observation that most participants in my project reported privacy protection behaviours were intended foremost to protect their personal information from other individuals as opposed to the platform providing whose services with which they engaged. Implementing protection strategies to guard social privacy, like setting one’s Instagram accounts to private, does not affect one’s use or enjoyment of the services Instagram offers. By contrast, tools and means of constraining Instagram’s ability to collect one’s personal information comes at the cost of limiting what one can do with Instagram.

It also is notable that the hacking of one’s personal information was perceived by the individuals comprising my sample as being a far greater risk to their privacy than Instagram’s sharing of their information for commercial purposes. Presumably, this bifurcated view may be accounted in part by the sense – whether rightly or wrongly – that the effects flowing from having

one's personal information misappropriated are more immediate and direct whereas the perceived effects of the commercial trading of one's information are less immediate and more banal (i.e., targeted advertising). It seems plausible that this bifurcation may also account, in part, for why most participants in my project cared more about their social privacy than their institutional privacy.

It also merits pointing out that around two third of participants in this project reported that they did not know the only way to stop Instagram from collecting their personal data is to delete their Instagram accounts, although it is clearly stated in Instagram's Data Policy. One (n=1) participant expressed that the policy was too long, complicated, and hard to read. No participant claimed to read the user agreements or data policies of any social media platforms. The most common rationale given for not reading these documents was that they all tend to be too long and unreadable. The ease with which the vast majority of people simply consent in an uninformed manner to the terms and conditions of user agreements, points toward a tacit acceptance, albeit perhaps begrudgingly, of the notion of privacy as a negotiable commodity. Indeed, one cannot help but question whether most people would take the time to read these policies even if they were far shorter and easier to understand. The cost of not consenting is the denial of access to desired service(s) and, as such, is not really an option for most.

Put simply, and in line with the users' rights versus needs dichotomy set out by Petronio (2002), what appears to be occurring with the members of my sample was a negotiation between accessibility and retreat. To this end, some participants distinguished between data being leaked and data being shared or traded. For these individuals, Instagram's sharing of users' information with other third parties is in no way akin to the notion of Instagram 'leaking' user information. The former was considered a legitimate commercial practice that enabled the platform to serve

them with more personalized services. By contrast, leaking was associated with illegitimate activities. Seen through this lens, my observations point toward the presence of the distinction Petronio (2002, p. 3) draws between understanding privacy as a basic right that must be protected, versus individuals choosing to reveal or conceal personal information “based on criteria and conditions they perceive as salient.”

Hinds et al. (2020) also expand upon this idea suggesting that individuals “establish privacy boundaries” based on their “perceived costs and benefits of information disclosure” (p. 4). They describe this process as reflecting a type of ‘privacy calculus’ wherein individuals’ “behaviour is determined by the outcome of the privacy trade-off.” (p. 3). For the participants in my project, the cost of not using social media platforms was not considered to be even remotely acceptable. As such, the more than half of participants who had no clear idea about what information Instagram collects or why, were still able to do the calculus without knowing all the costs or benefits. Put simply, the privacy calculus has already been completed before individuals can fully evaluate all the costs and benefits.

We also see evidence of perceiving privacy as a negotiable commodity among the individuals comprising the sample for my project through, for example, assertions that although it would not be right for Instagram to use their data for political purposes, it is acceptable for the platform to use their data for commercial gain. For these individuals, privacy is never something that must be guaranteed. Instead, they prefer to determine their privacy boundaries. In the words of one participant, it is “a fair trade” (P12) in which the company gets users' data while the users get to use the app. Even those who were more reticent about Instagram’s data-collection activities nonetheless maintained its surveillance of their activities was advantageous insofar as it contributed to them receiving personalized services.

In considering the rights versus needs dichotomy, in relation to the participants in my project, it is clear the perceived need of using Instagram far outweighs any considerations about privacy rights. If this observation about the perception of privacy as a bounded negotiable commodity is indeed illustrative of a more ubiquitous phenomenon, it suggests that the understanding of the concept of basic privacy among contemporary young adults is shifting away from the premises that have guided its conceptualization by previous generations. This, in turn, may point to the need for a rethinking of both the types of approaches needed for privacy education and, potentially, privacy policy more broadly.

4.5 Conclusion

Overall, it seems clear that the participants in this project did not appear to view their online privacy as a right that needs to be protected. Indeed, they appeared to be comfortable, even perhaps at ease, with the notion of privacy being a negotiable commodity that they can use to trade for free services. In contrast to the findings of the comparator studies, the participants in my project lower levels of privacy concerns. However, in line with these same comparator studies, the privacy protection behaviours reported by those in my sample focused foremost on protecting their social privacy rather than their institutional privacy.

In the next, concluding, chapter, I turn my attention to the overall implications of my findings.

Chapter 5: Conclusion

Inspired by the work of Hinds et al., (2020), this thesis has examined the perceptions of a small sample of young adults regarding online privacy issues and the extent to which their perceptions affect their privacy protection behaviours when they engage with Instagram. Much of the contemporary literature about young adults' views regarding online privacy and online privacy protection points to a gap between people's privacy concerns and their actual privacy protection behaviours (i.e., a privacy paradox). Hoffmann et al. (2016) suggest that this so-called privacy paradox is rooted in cynicism about Internet companies' data collection activities. In seeking to examine whether Hinds et al.'s findings were replicable in relation to Instagram, I conducted semi-structured interviews with 20 undergraduate students from the University of Ottawa who identified as being regular Instagram users. The empirical evidence presented in this thesis suggests the presence of privacy apathy as opposed to any cynicism-based privacy paradox per se. Put simply, the participants in this study did not appear to be particularly concerned about protecting their privacy online.

Chapter 2 set out the theoretical foundations of the thesis. The discussion reviewed the findings of previous studies regarding online privacy and online privacy protection strategies. Chapter 3 outlined the research design and methodology used to conduct this project and set out the findings to emerge from the warm-up questionnaire and the interviews. Chapter 4 offered an analysis of the findings and situated their implications within the broader context of contemporary privacy research. The discussion set out in this, concluding, chapter is divided into four sections. In the first section, I revisit the research questions that guided my project. In the second section I outline some of the limitations with my project and their impact on the conclusions that can be

drawn from it. This is followed, in section 3, with a discussion of potential directions for future research. Section 4 wraps up the thesis with some concluding remarks.

5.1 Privacy Cynicism or Privacy Apathy

In the aftermath of the Facebook-Cambridge Analytica scandal, Hinds et al. (2020) investigated the perception of Facebook users regarding their online privacy and the strategies they used to protect their online privacy when engaging with the platform. Today, Facebook is no longer the preferred social media platform of young adults, having been overtaken by Instagram. It was with this in mind that I sought to investigate whether the observations published by Hinds et al., were replicable with regard to Instagram. As such, the central research question guiding this project asked:

Are Hinds et al.'s (2020) findings regarding people's perceptions of online privacy issues replicable among a sample of undergraduate students who are regular users of Instagram?

Echoing Hinds et al.'s (2020) Facebook-centric findings, the evidence gathered from this thesis suggests that naivety, feelings of powerlessness, and gaps between privacy protection intentions and privacy protection behaviours were evident among those who volunteered to participate in my thesis research.

Within my sample, naivety was manifest in such ways as maintaining that the level of concern merited of commercial data collection practices is directly linked to one's social and/or economic status, that platform surveillance for advertising purposes is a helpful service, the idea that limiting the frequency of one's posts to Instagram is an effective privacy protection strategy, and the belief that 'others' could live without social media. Interestingly, the sense of powerlessness was most pronounced among those individuals who demonstrated higher levels of privacy literacy. These individuals implemented various privacy protection strategies but had little faith in their effectiveness. These participants' expressions suggest that a higher level of privacy

literacy can potentially lead to a higher level of privacy cynicism, and further feed privacy apathy. This said, it merits recalling that the privacy protection strategies used were oriented foremost to limiting the ability of others to access the participants' personal information (i.e., social privacy) rather than constraining Instagram's capacity to collect their data (i.e., institutional privacy).

Where the findings emerging from my sample seemed to diverge from those of Hinds et al., (2020) was in relation to the issue of privacy fatigue, and the idea of closing one's social media account. The participants in Hinds et. al., reported being fatigued from frequent news reports about data breaches. In the case of participants in my project, they predominantly lacked knowledge of data breaches. Indeed, they did not appear to be suffering from privacy fatigue but rather to be manifesting a form of privacy apathy. That is, they seemingly did not care about data breaches or the fact that their personal information is collected by the platforms. Indeed, discussion of data breaches did not arouse any intention among the participants to augment their online privacy strategies. It seems plausible that the difference between my, and Hinds et al.'s findings may be explained, in part, by the fact that their study was conducted on the heels of the Facebook-Cambridge Analytica scandal.

The other distinguishing finding emerging from my project is the observation that participants flatly rejected any notion of permanently closing their Instagram accounts. Even those who reported having temporarily left Instagram or who expressed a desire to leave were adamant about not closing their accounts or permanently leaving the platform. The key factor here was the expressed need to maintain connections with their friends and families.

In sum, the findings from my project suggest that rather than privacy cynicism, the participants in my project are predominantly experiencing a sense of privacy apathy.

5.1.1 Data Breaches and Targeted Ads

The second research question guiding my project focused on perspectives about Instagram's data collection activities. It asked: *What concerns do undergraduate students in my sample have about Instagram's use of their data to facilitate the targeting of advertising to their screens?*

In conducting this project, one of the striking observations, for me, was the pervasive lack awareness among my sample of data breaches. While I had not expected all participants to be well versed about such events, I had presumed most would have at least passing familiarity with some of the major instances that have garnered media attention in recent years (e.g., Facebook Cambridge Analytica Scandal in 2018; Facebook's leak of users' data in 2019; the 2021 hacking of LinkedIn's customer database). What particularly stood out for me was that, among those who were able to provide examples of data breaches, the examples focused almost exclusively on individualized instances of personal information being leaked by hackers, rather than data leaks associated with particular platforms.

Another observation that really stood out for me was the finding that nearly one half of the participants were not aware that the ads appearing on their screens are one of the consequences of Instagram's data collection activities. Although most of the participants reported having little use for the ads appearing on their screens, they were ambivalent about their presence. This ambivalence, or lack of annoyance with the targeted ads, seemed to be linked to the notion of their not being affected by Instagram's data collection activities.

Overall, the participants had little-to-no concerns about the targeted ads, with some even articulating that their presence on their screens as was part of a fair trade for being able to access the personalized services provided by Instagram for free.

Taken together, the participants' feelings about data breaches and targeted advertising point to their not viewing online privacy a basic right to be guaranteed. Instead, the dominant view among my sample leaned toward perceiving one's personal information as a commodity that can be traded for other things one may desire such as 'free' online services.

5.1.2 Privacy Protection Strategies

The third research question centered upon the strategies used to protect online privacy and their perceived efficacy. For this, I asked:

What strategies do the undergraduate students in my sample use to protect their online privacy? And, do they view these strategies as effective?

It is fair to say that among the individuals comprising my sample, little effort appeared to be expended on protecting their online privacy. To this end, the most frequently reported privacy protection strategy was simply to set one's Instagram account as private. I hypothesize that this state of affairs reflects an orientation toward protecting personal information data from other users or hackers rather than from the platform itself.

The participants' self-evaluations of the effectiveness of their privacy protection strategies appeared to be polarized. Some individuals seemed to be very confident that their strategies could effectively protect their online privacy whereas others maintained there was no effective way to protect oneself from the platform's data collection activities. Here, there appeared to be a clear lack knowledge about how to protect one's online privacy. Those individuals who demonstrated the lowest levels of privacy literacy tended to rely upon only the simplest of privacy protection strategies and to be overly confident about the effectiveness of their strategies. By contrast, those who demonstrated higher levels of privacy literacy had little confidence with the efficacy of the strategies they used to protect their privacy, especially from the Instagram platform.

5.1.3 Contribution to Knowledge

This thesis makes two complementary contributions to advancing knowledge about understanding the privacy paradox. First, viewing online privacy a negotiable commodity rather than a basic right call into question the very idea of a privacy paradox insofar as the commodity-based view of privacy seemingly changes – and perhaps even diminishes – both the perceived causes for concern and the types of protection strategies needed. Second, it seems plausible that a commodity perspective of privacy also nourishes a sense of apathy about online institutional privacy protection insofar as actively striving to protect one's online institutional privacy impedes access to desired services. Put simply, viewing one's personal information as something that is acceptable to trade for access to other products and services alters the very meaning of guarantying and/or protecting a right to privacy whether on- or off-line.

There is another point meriting of consideration here. Social media is now embedded into people's daily lives. As reported by the participants in my project, Instagram is not just something for enjoyment; it is basic tool of communication and, in some cases, even a perceived necessity. As such, it seems plausible that the more people sense they cannot live without this, and other, social media platforms, the less users may view online privacy considerations are a source of concern.

5.2 Limitations

There are some limitations that must be acknowledged when interpreting both the observations I reported and the conclusions that can be drawn from this thesis. The first issue pertains to the small size of the research sample. With only twenty participants, both the scope and generalizability of my findings across the target demographic (i.e., young adult users of Instagram) are constrained. Bearing in mind that my project was intended to be an exploratory study that was completed as

part of Master's level program of graduate study and that my project had to be completed with only very limited resources, I had to keep this undertaking to a manageable size. This said, it seems plausible that my results may nonetheless be indicative of what one might find if similar research was conducted on a larger scale.

Another limitation pertains to the social media platform at the heart of this project – i.e., Instagram. I opted to focus on users of this app because at the time my project began, 2021, it was the most commonly used social media app among young adults in North America (Auxier & Anderson, 2021). However, from the period spanning the start to completion of this project, a demographic shift away from Instagram toward TikTok occurred. Reflecting this shift, and despite all the participants in project being regular users of Instagram, the app they most frequently identified as their favourite was TikTok. They expressed that they enjoyed using TikTok most for entertainment, but Instagram was a necessary tool in their daily lives. This observation speaks to the need, ideally, for a larger multi-platform examination of the perceptions of young adulthood regarding their online privacy and the privacy protection strategies they employ across platforms.

There also were some limitations with the interview process itself that I must acknowledge. First, with the interviews being conducted online, I could sense during the meetings that some participants seemed distracted and/or somehow less engaged in the moment. This leaves me wondering about the reliability of some of the responses I obtained from the interviews. Second, and relatedly, some participants appeared to be in a rush to complete the interviews. For some, one sensed the main motivation for participating was simply to get the course credit point as opposed to any interest in the subject matter per se. As a researcher, I cannot help but feel, perhaps mistakenly, that these challenges may not have been manifest as strongly during in-person interviews.

5.3 Directions for Future Research

This project was designed to investigate the perceptions of young adults regarding online privacy and the strategies they employ to protect their privacy. The findings that have emerged point to a few possible areas deserving of future research. The issues set out below are exemplary of what which undertakings might zero-in on:

1. *Shift of definition of privacy.* The findings suggest that the participants tend to understand their privacy as a negotiable commodity that they can use to trade for free services provided by social media platforms, rather than a basic right that must be guaranteed. It seems plausible that the definition and/or understanding of privacy is shifting as social media and surveillance capitalism becomes ever more ubiquitous. This suggests the need for further research about privacy not least because if such a change in understanding is happening, it has implications for both educational and social policy.

2. *Shift of role social media plays.* The participants reported various roles that social media plays in their lives, including not only a necessary tool that they can keep in touch with their friends and families, but also a window through which they can learn about the world outside, and even an archive containing the most essential parts of their memories, histories, and how they built their own identities and found the communities they belonged. To fully understand why people take their privacy as a negotiable commodity, it would be beneficial to better understand what, exactly, they believe they are trading their privacy forth. This suggests the need for more research focusing on, in people's perceptions, what different social networking platforms mean to them, and how these perceptions affect their perceptions of their online privacy.

3. *Data collection beyond social media platforms.* This project has suggested a deep bond between the participants and the social media platforms. The participants expressed that they would not

stop using social media for any privacy-related reasons. With this in mind, it is necessary to learn how users perceive the data collection strategies of other platform companies including, for example, virtual mapping services. When people use virtual maps or transportation services apps, their location information is shared with the platform company, and even with other individuals. Therefore, to understand how people perceive online privacy issues more comprehensively, it would be useful to learn how they perceive their online privacy issues while using different types of social network services.

5.4 A Few Tentative Suggestions About Privacy-Related Education

If, as the findings of this thesis suggest, we have indeed reached a historical juncture wherein individuals view their privacy as a negotiable commodity and protecting one's online institutional privacy is deemed to be a matter of little relevance lest one's access to services be impeded, it perhaps also is time to reconsider how privacy education is approached. To this end I offer a few tentative suggestions:

1. The notion of privacy as a negotiable commodity implies that we cannot (should not?) think of privacy as an absolute but rather as a construct that is informed by a combination of cultural and pragmatic considerations and about which individual decisions are made in accord with the notion of privacy calculus. This, in turn, suggests that contemporary privacy education might better connect with intended audiences by giving greater centrality to the notion of individual data/information sovereignty. Specifically, in educating not only about the importance of protecting privacy – and digital rights more broadly – but also about the ways in which individuals and communities and participate in, steward, and control data/information that is created by, with, or about them. The idea here would be to educate students toward better understanding how they might take control of their own data and, in the process, benefit

themselves from its intrinsic value. Institutionally, we can already observe movement in this direction with the EU's General Data Protection Regulation (GDPR)²⁷ insofar as it provides citizens of the EU with far greater power over the use of their data than currently is the case in Canada. The GDPR likewise regulates much more strongly what private entities can do with people's data and information than current Canadian legislation.

2. My findings suggest that that one possible way of having students come to better understand what individual data sovereignty might mean for them would be to construct in-class assignments along the lines of:

A. It is widely taken as a truism that no one has time to read the User Agreements to which we sign on to use particular apps. Yet, reading these documents, or at least portions thereof, can be a valuable learning exercise on many levels. With this in mind, I can envisage having undergraduate-level course assignments based upon having students engage in a close reading of relevant portions of these agreements, followed by any number of analytical exercises – *What is revealed about how your data is used? How is your data protected? What recourse do you have? What would you like to see changed in the agreement?* And, if one is really keen, *How do the policies of App X compare to those of App Y?* The idea here would be twofold. First, to have people gain greater insight into what they are giving away and how it is being used. Second, to get students thinking about what they would like to see changed and how such change might come about.

B. Zuboff (2019b) sheds light on how data gathered about individuals through their online activities is increasingly being used to directly shape peoples' offline behaviour without them being aware. This process, known as nudging, relies algorithmic profiling to

²⁷ See, <https://gdpr-info.eu/>

manipulate behavior for commercial purposes. One example she highlights, and which could serve as the basis for a fun classroom exercise demonstrating how personal data is used to tune, herd, and guide behaviour without one's knowledge is the game *Pokémon Go*. When playing this game, players walk from place to place to catch Pokémon and to compete with others. What many do not realize is that they are also being directed toward specific retail outlets, restaurants, and other business who pay the creators of *Pokémon Go* to direct players to their service outlets. Here, one can easily envisage having students play *Pokémon Go* (or any similar augmented reality game) while keeping track of the consumer outlets the encounter in seeking Pokémon. From this, one can envisage developing any number of mapping, research, and reflective exercises. The idea here is to 'bring to life' how one's data trails can be, and are, used to shape our offline behaviours for the commercial gain.

C. There clearly are parallels between nudging today, and the notion of persuasion that has long been associated with broadcast media. With this in mind, one can envision a host of historical comparative exercises that would have media and communication studies students reflect upon the points of convergence and divergence of these phenomena and the implications thereof. The idea here would be to help educate students about the fact that privacy related concerns are historically situated. The technologies and challenges may be 'new,' but the fundamental nature of the issues at stake are not necessarily novel.

5.5 Concluding Remarks

When I started this project, I thought that the topic of online privacy was already a well-discussed subject of which people generally had adequate knowledge and understanding. I assumed that it would not be difficult to find evidence of the privacy paradox. However, I was quite surprised to find just how unfamiliar many of the participants in my study were platform surveillance. Indeed,

I am left feeling troubled by the lack of knowledge many of the individuals demonstrated about platform data collection activities, the institutional privacy risks associated with using social media, and strategies for protecting one's online privacy.

Ultimately, what I uncovered was not another example of a privacy paradox but rather, a form of privacy apathy. None of the participants seemed to view privacy as right that must be protected. Instead, their focus was on services provided by social media platforms. And, here, the trading of one's information seemed to be an accepted and fair price to pay. This view was also evident in privacy protection strategies people reported implementing. No privacy protection measures that might hinder access to the services provided by Instagram were entertained, let alone implemented.

If such perspectives are widespread, it is time to reconsider the foundation of policy-making on privacy. Approaching privacy a negotiable commodity rather than a basic right calls for a shift in how we approach privacy regulation, privacy protection, and privacy education both online and offline while everyone is living in the context of surveillance capitalism.

Bibliography

- Acquist, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Paper presented at the proceedings of the 27th international conference on information systems*, 1563-1580.
- Afriat, H., Dvir-Gvirsman, S., Tsurriel, K., & Ivan, L. (2021). “this is capitalism. it is not illegal”: Users’ attitudes toward institutional privacy following the Cambridge analytica scandal. *The Information Society*, 37(2), 115–127. <https://doi.org/10.1080/01972243.2020.1870596>
- Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: *Implications for new media*. *Journal of Consumer Marketing*, 33(2), 98–110. <https://doi.org/10.1108/jcm-06-2015-1458>
- Ajzen, I. (1991). Theory of planned behavior. *Organizational Behaviour and Human Decision Processes*, 50(2), 179-211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T).
- Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research*, 3(1). <https://doi.org/10.5430/elr.v3n1p39>
- Arora, T., & Agarwal, B. (2020). An Empirical Study on Determining the Effectiveness of Social Media Advertising: A Case on Indian Millennials. *International Journal of e-Business Research*, 16(2), 47–68. <https://doi.org/10.4018/IJEBR.2020040104>
- Auxier, B., & Anderson, M. (2021, April 7). *Social media use in 2021*. Pew Research Center: Internet, Science & Tech. <https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/>
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- 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>
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and Privacy Management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Brown, A. J. (2020). “should I stay or should I leave?”: Exploring (dis)continued facebook use after the Cambridge Analytica scandal. *Social Media + Society*, 6(1). <https://doi.org/10.1177/2056305120913884>
- Chhabra, S. (2021). Why Does Privacy Paradox Exist?: A Qualitative Inquiry to Understand the Reasons for Privacy Paradox Among Smartphone Users. *Journal of Electronic Commerce in Organizations*, 20(1), 1–20. <https://doi.org/10.4018/JECO.292470>

- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51. <https://doi.org/10.1016/j.chb.2017.12.001>
- Claxton, C. M. (2021). Private Offerings in the Age of Surveillance Capitalism and Targeted Advertising. *Vanderbilt Law Review*, 74(4), 1187–1229.
- Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting & Social Change*, 161, 120299–. <https://doi.org/10.1016/j.techfore.2020.120299>
- Confessor, N. (2018, April 4). *Cambridge Analytica and Facebook: The scandal and the fallout so far*. The New York Times. Retrieved April 3, 2023, from <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- Croucher, S. M., & Cronn-Mills, D. (2019). *Understanding communication research methods: A theoretical and practical approach* (2nd ed.). Routledge. <https://search-ebscohost-com.proxy.bib.uottawa.ca/login.aspx?direct=true&db=nlebk&AN=1776493&site=ehost-live>.
- Dixon, S. (2022, October 18). *Topic: Social media use during coronavirus (COVID-19) worldwide*. Statista. <https://www.statista.com/topics/7863/social-media-use-during-coronavirus-covid-19-worldwide/#topicOverview>
- Goodyear, V. A., Wood, G., Skinner, B., & Thompson, J. L. (2021). The effect of social media interventions on physical activity and dietary behaviours in young people and adults: a systematic review. *The International Journal of Behavioral Nutrition and Physical Activity*, 18(1), 1–72. <https://doi.org/10.1186/s12966-021-01138-3>
- Guo, X., Zhang, X., & Sun, Y. (2016). The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, 16, 55–65. <https://doi.org/10.1016/j.elerap.2015.11.001>
- Guynn, J. (2018, March 29). *Delete facebook? It's a lot more complicated than that*. The Des Moines Register. Retrieved April 3, 2023, from <https://www.desmoinesregister.com/story/tech/news/2018/03/28/people-really-deleting-their-facebook-accounts-its-complicated/464109002/>
- Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication (Online)*, 3737–3752.
- Hinds, J., Williams, E. J., & Joinson, A. N. (2020). “it wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>
- Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the Privacy Paradox. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3319830>
- Instagram. (2022). Instagram Help Center. Retrieved May 31, 2022, from https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

- Isaac, M. (2021, October 28). *Facebook renames itself Meta*. The New York Times. Retrieved April 4, 2023, from <https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html>
- Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer* (Long Beach, Calif.), 51(8), 56–59. <https://doi.org/10.1109/MC.2018.3191268>
- Kaiser, B. (2019). *Targeted: the Cambridge Analytica whistleblower's inside story of how big data, Trump, and Facebook broke democracy and how it can happen again* (First edition.). Harper, an imprint of Harper Collins Publishers.
- Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization-Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, 34(2), 369–400. <https://doi.org/10.1080/07421222.2017.1334467>
- Koeze, E., & Popper, N. (2020, April 7). *The virus changed the way we internet*. The New York Times. Retrieved April 19, 2023, from <https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html>
- Laterza, V. (2021). Could Cambridge Analytica Have Delivered Donald Trump's 2016 Presidential Victory? An Anthropologist's Look at Big Data and Political Campaigning. *Public Anthropologist*, 2021(1), 119–147. <https://doi.org/10.1163/25891715-03010007>
- Lee, D. (2018, March 22). *Facebook's Zuckerberg speaks out over Cambridge Analytica 'breach'*. BBC News. Retrieved April 3, 2023, from <https://www.bbc.com/news/world-us-canada-43494337>
- Leetaru, K. (2018, April 2). *Why are we only now talking about Facebook and elections?* Forbes. Retrieved April 3, 2023, from <https://www.forbes.com/sites/kalevleetaru/2018/03/19/why-are-we-only-now-talking-about-facebook-and-elections/?sh=3b1154f48383>
- Li, L., Wang, Z., Zhang, Q., & Wen, H. (2020). Effect of anger, anxiety, and sadness on the propagation scale of social media posts after natural disasters. *Information Processing & Management*, 57(6), 102313. <https://doi.org/10.1016/j.ipm.2020.102313>
- Lin, Y. (2023). *Instagram age demographics [update Mar 2023]*. Oberlo. Retrieved April 4, 2023, from <https://www.oberlo.com/statistics/instagram-age-demographics>
- Lomas, N. (2020, January 6). *Facebook data misuse and voter manipulation back in the frame with latest Cambridge Analytica leaks*. TechCrunch. Retrieved April 3, 2023, from <https://techcrunch.com/2020/01/06/facebook-data-misuse-and-voter-manipulation-back-in-the-frame-with-latest-cambridge-analytica-leaks/?guccounter=1>
- Lovari, A., & Bowen, S. A. (2019). Social Media in Disaster Communication: A case study of strategies, barriers, and ethical implications. *Journal of Public Affairs*, 20(1). <https://doi.org/10.1002/pa.1967>

- Luik, P., & Lepp, M. (2021). Changes in activity and content of messages of an Estonian Facebook group during transition to distance learning at the beginning of the COVID-19 Pandemic. *Journal of Computer Assisted Learning*, 37(6), 1629–1639. <https://doi.org/10.1111/jcal.12602>
- Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, 22(7), 1168–1187. <https://doi.org/10.1177/1461444820912544>
- Lydeard, S. (1991). The questionnaire as a research tool. *Family Practice*, 8(1), 84-91. <https://doi.org/10.1093/fampra/8.1.84>
- Manokha, I. (2018). Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective. *Theory & Event*, 21(4), 891–913.
- Mansell, R., & Steinmueller, W. E. (2020). *Advanced introduction to platform economics*. Edward Elgar Publishing.
- Martin, K. (2020). Breaking the privacy paradox: the value of privacy and associated duty of firms. *Business Ethics Quarterly*, 30(1), 65–96. <https://doi.org/10.1017/beq.2019.24>
- Mehta, P. (2021). Work from home—Work engagement amid COVID-19 lockdown and employee happiness. *Journal of Public Affairs*, 21(4). <https://doi.org/10.1002/pa.2709>
- Meredith, S. (2018, April 10). *Facebook-cambridgeanalytica: A timeline of the data hijacking scandal*. CNBC. Retrieved April 3, 2023 from <https://www.cnn.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>
- Molla, R. (2021, March 1). *Posting less, posting more, and tired of it all: How the pandemic has changed social media*. Vox. Retrieved April 19, 2023, from <https://www.vox.com/recode/22295131/social-media-use-pandemic-covid-19-instagram-tiktok>
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital citizenship : the internet, society, and participation*. MIT Press.
- Mukwevho, J., & Ngoepe, M. (2019). Taking archives to the people: The use of social media as a tool to promote public archives in South Africa. *Library Hi Tech*, 37(3), 374–388. <https://doi.org/10.1108/LHT-11-2017-0228>
- Nelli, S. (2022, March 3). *Most people never actually read terms and conditions, but it's a major data risk*. Entrepreneur. <https://www.entrepreneur.com/money-finance/most-people-never-actually-read-terms-and-conditions-but/417976>
- Nig @ EnJay Solutions. "Game Rules at Ultimate Top Trumps". Retrieved April 4, 2023, from [Ultimate-top-trumps.co.uk](https://ultimate-top-trumps.co.uk).
- Nur -A Yazdani, D. M., Abir, T., Qing, Y., Ahmad, J., Al Mamun, A., Zainol, N. R., Kakon, K., Agho, K. E., & Wang, S. (2022). Social media addiction and emotions during the disaster

- recovery period—The moderating role of post-COVID timing. *PloS One*, 17(10), e0274898–e0274898. <https://doi.org/10.1371/journal.pone.0274898>
- Oladipo, T. (2023, January 24). *How to use Instagram close friends*. Buffer Library. Retrieved April 3, 2023, from <https://buffer.com/library/instagram-close-friends/>
- Pan, Z., Lu, Y., Wang, B., & Chau, P. Y. K. (2017). Who Do You Think You Are? Common and Differential Effects of Social Self-Identity on Social Media Usage. *Journal of Management Information Systems*, 34(1), 71–101. <https://doi.org/10.1080/07421222.2017.1296747>
- Pangrazio, L., & Selwyn, N. (2018). “It’s Not Like It’s Life or Death or Whatever”: Young People’s Understandings of Social Media Data. *Social Media + Society*, 4(3), 205630511878780–. <https://doi.org/10.1177/2056305118787808>
- Patra, P., Singh, V. V., & Singal, A. (2021). Coping with COVID: Cross-sectional study to assess the psychological impact and coping strategies utilized by Indian internet users during the lockdown of the COVID-19 pandemic. *Industrial Psychiatry Journal*, 30(1), 29–33. https://doi.org/10.4103/ipj.ipj_202_20
- Petronio, S. S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.
- Protalinski, E. (2012, April 9). *Why Facebook acquired Instagram for \$1 Billion*. ZDNET. Retrieved April 4, 2023, from <https://www.zdnet.com/finance/why-facebook-acquired-instagram-for-1-billion/>
- Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1), NP–NP. <https://doi.org/10.5210/fm.v15i1.2775>
- Read, A. (2023, March 27). *Instagram Stories: The Complete Guide to creating standout stories*. Buffer Library. Retrieved April 3, 2023, from <https://buffer.com/library/instagram-stories/>
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). *How trump consultants exploited the Facebook data of Millions*. The New York Times. Retrieved May 31, 2022, from <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>
- Ross, Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior*, 25(2), 578–586. <https://doi.org/10.1016/j.chb.2008.12.024>
- Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting facebook users’ online privacy protection: Risk, trust, Norm Focus Theory, and the theory of planned behavior. *The Journal of Social Psychology*, 154(4), 352–369. <https://doi.org/10.1080/00224545.2014.914881>
- Sandle, T. (2020, January 29). *Report finds only 1 percent reads “terms & conditions.”* Digital Journal. <https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127>

- Saud, M., Mashud, M., & Ida, R. (2020). Usage of social media during the pandemic: Seeking support and awareness about COVID-19 through social media platforms. *Journal of Public Affairs*. <https://doi.org/10.1002/pa.2417>
- Schaffer, N. (2023, May 30). Social Media Demographics: What Marketers Need to Know in 2023 [web log]. Retrieved July 12, 2023, from <https://nealschaffer.com/social-media-demographics/#:~:text=Which%20demographic%20uses%20social%20media,Facebook%2C%20Instagram%2C%20and%20Twitter.>
- Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online privacy literacy and online privacy behavior – the role of crystallized intelligence and personality. *International Journal of Human–Computer Interaction*, 37(15), 1455–1466. <https://doi.org/10.1080/10447318.2021.1894799>
- 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>
- Stouffer, C. (2022, August 3). *Computer cookie: A definition + how cookies work in 2022*. Norton. Retrieved April 3, 2023, from <https://us.norton.com/blog/privacy/what-are-cookies>
- Strobelt, H., Oelke, D., Rohrdantz, C., Stoffel, A., Keim, D. A., & Deussen, O. (2009). Document Cards: A Top Trumps Visualization for Documents. *IEEE Transactions on Visualization and Computer Graphics*, 15(6), 1145–1152. <https://doi.org/10.1109/TVCG.2009.139>
- Soumelidou, A., & Tsohou, A. (2019). Effects of privacy policy visualization on users’ Information Privacy Awareness Level. *Information Technology & People*, 33(2), 502–534. <https://doi.org/10.1108/itp-08-2017-0241>
- Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1410>
- Taddicken, M. (2013). The ‘Privacy Paradox’ in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248–273. <https://doi.org/10.1111/jcc4.12052>
- Tang, J., Akram, U., & Shi, W. (2020). Why people need privacy? the role of privacy fatigue in App Users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management*, 34(4), 1097–1120. <https://doi.org/10.1108/jeim-03-2020-0088>
- Teselios, D. & Savu, M. 2018. "Social Media - An Integral Part Of Daily Life," *Contemporary Economy Journal*, Constantin Brancoveanu University, 3(1), pages 59-78.
- Trottier, D. (2012). *Social media as surveillance: rethinking visibility in a converging world*. Ashgate.

- ur Rehman, I. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice*, 1-11.
- Valkenburg, P. (2017). Understanding Self-Effects in Social Media. *Human Communication Research*, 43(4), 477–490. <https://doi.org/10.1111/hcre.12113>
- Wang, X., Zhang, M., Fan, W., & Zhao, K. (2022). Understanding the spread of COVID-19 misinformation on social media: The effects of topics and a political leader's nudge. *Journal of the Association for Information Science and Technology*, 73(5), 726-737. <https://doi.org/10.1002/asi.24576>
- Wold, S. (2021, May 20). *Covid-19 is changing how, why and how much we're using social media*. Digital Commerce 360. Retrieved April 19, 2023, from <https://www.digitalcommerce360.com/2020/09/16/covid-19-is-changing-how-why-and-how-much-were-using-social-media/>
- Wong, J. C. (2019, July 12). *Facebook to be fined \$5 bn for Cambridge Analytica privacy violations – reports*. The Guardian. Retrieved April 3, 2023, from <https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftp-privacy-violations>
- Xue, J. H. (2022). Delegitimising Data Subjects' Economic Interests During Automatic Propertisation of Their Data: A Comparative Study of Data Protection on Social Media Platforms in the UK and China. *Global Media and China*, 7(2), 151–168. <https://doi.org/10.1177/20594364211060874>
- Yu, L., Cao, X., Liu, Z., & Wang, J. (2018). Excessive social media use at work: Exploring the effects of social media overload on job performance. *Information Technology & People* (West Linn, Or.), 31(6), 1091–1112. <https://doi.org/10.1108/ITP-10-2016-0237>
- Zeitlin, M. (2018, March 29). *Despite all the #deletefacebook talk, data shows we're using it more...* Inc. Retrieved April 3, 2023, from <https://www.inc.com/minda-zetlin/for-all-deletefacebook-talk-data-shows-were-using-it-more-not-less.html>
- Zialcita, P. (2019, October 30). *Facebook pays \$643,000 fine for role in Cambridge Analytica scandal*. NPR. Retrieved April 3, 2023, from <https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal>
- Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics*, 61, 101601–. <https://doi.org/10.1016/j.tele.2021.101601>
- 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>
- Zuboff, S. (2019a). *Surveillance Capitalism and the Challenge of Collective Action*. *New Labor Forum*, 28(1), 10–29. <https://doi.org/10.1177/1095796018819461>

Zuboff, S. (2019b). *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (First edition.). Public Affairs.

Appendix 1 – The Recruitment Text of REB Application

Student friendly study description:

Are you an undergraduate student at the University of Ottawa aged between the ages of 18-25? Do you use Instagram on a regular basis? Are you interested in the privacy implications of your Instagram use? If you answered 'yes' to any of these questions, I would love to chat with you!

I am looking for 30 participants who are willing meet via Zoom to chat about your experiences and perspectives about online privacy issues and protection in relation to Instagram. The only commitment is to participate in one meeting that will last approximately 45-60 minutes in duration. The purpose of my study is to see how young adults feel about online privacy issues and how their feelings affect their privacy protection behaviours. Even if you don't give much thought to privacy issues, your participation and input are wanted and relevant! The findings of my study will shed light on strengthening education efforts focusing on improving and implementing strategies to protect online privacy.

If you have any questions or wish to sign-up to participate in my study, please email me, Hongru Zhang at _____. Please note that this project is being conducted solely in English, and that participants will be selected on a first-come, first served basis.

I look forward to hearing from you!

Appendix 2 – The Questionnaire

Concerned Enough to Act? Privacy Concerns & Perspectives among Undergraduate Instagram Users Questionnaire

Participant Code: _____ Date: _____

Use of Instagram

1. On average, approximately how long per day do you spend on Instagram?

10 min or less	10-30 min	31-60 min	1-2 hours	2+ h

2. Instagram is part of my everyday activity.

Strongly disagree	Disagree	Neutral	Agree	Strongly Agree

3. I feel out of touch when I haven't logged on to Instagram for a while

Strongly disagree	Disagree	Neutral	Agree	Strongly Agree

4. I would be sad if Instagram shut down

Strongly disagree	Disagree	Neutral	Agree	Strongly Agree

Instagram Account Privacy Settings

5. Is your account set to: Private or Public

6. Do you allow comments to your posts from:

Everyone? Yes / No

People you follow? Yes / No

Your followers? Yes / No

7. Do you allow yourself to be mentioned by:

Everyone? Yes / No

People you follow? Yes / No

Your followers? Yes / No

8. Do you allow yourself to be tagged by:

Everyone? Yes / No

People you follow? Yes / No

Your followers? Yes / No

9. Do you use the “Story” feature? Yes / No

If yes, who do you allow to view your stories?

Everyone	Everyone except selected accounts	Close friends	Don't know

If yes, who do you allow to reply to your stories?

Everyone	Everyone except selected accounts	Close friends	Don't know

10. Do you allow people to share your story to their story? Yes / No

11. Do you allow people to share your story in a message? Yes / No

12. Do you automatically share your Instagram story as your Facebook story? Yes/No

13. Have you ever restricted/blocked/muted any accounts? Yes / No

If yes, how many?

1-10	10 - 20	More than 20	Don't know

What are the top 3 reasons for you to restrict/block/mute other accounts?

1. _____

2. _____

3. _____

This section is to access more general attitudes of Instagram

14. Approximately how long have you used Instagram?

Less than 6 months	6 months – 1 year	1-2 years	2+ years

15. Do you pay attention to the ads that appear on your screen while using Instagram? Yes / No

Do the ads bother you? Yes / No

Do you find these ads helpful? Yes/No

16. How satisfied are you with Instagram, overall?

Not Satisfied	Barely Satisfied	Neutral	Satisfied	Very Satisfied

Appendix 3 – The Interview Protocol

The Interview Guide

1. When you access/use Instagram, do you think about the fact that it connects to your personal data? Do you have any concerns about this?
2. Are you aware of Instagram's data collection activities? Do you know what information Instagram is collecting from you?
3. Do you know why Instagram collects users' data? Do you have any concerns about this?
4. Have you ever seen any ads on your screen? Do you know how this happened?
5. Have you ever heard of any data breach incidents? Can you provide any examples?
6. How do you protect your personal information while using Instagram?
7. How do you evaluate the effectiveness of your privacy protection behaviours?
8. Have you ever thought of leaving Instagram or other social media platforms for the security of your personal information?
9. Is Instagram your favourite social media app? Based on your observation, which social media app you think is the most popular in your generation?
10. Do you have anything else about this topic you want to express but I didn't ask?

Appendix 4 – The Ethics Clearance Certificate

05/11/2022

Université d'Ottawa

Bureau d'éthique et d'intégrité de la recherche

University of Ottawa

Office of Research Ethics and Integrity

CERTIFICAT D'APPROBATION ÉTHIQUE | CERTIFICATE OF ETHICS APPROVAL

Numéro du dossier / Ethics File Number

S-10-22-8518

Titre du projet / Project Title

Concerned Enough to Act?
Privacy Concerns & Perspectives
among Undergraduate Instagram
Users

Type de projet / Project Type

Thèse de maîtrise / Master's
thesis

Statut du projet / Project Status

Approuvé / Approved

Date d'approbation (jj/mm/aaaa) / Approval Date (dd/mm/yyyy)

05/11/2022

Date d'expiration (jj/mm/aaaa) / Expiry Date (dd/mm/yyyy)

04/11/2023

Équipe de recherche / Research Team

**Chercheur /
Researcher**

Affiliation

Role

Alina ZHANG

Département de communication / Department of
Communication

Chercheur Principal / Principal
Investigator

Daniel PARÉ

Département de communication / Department of
Communication

Superviseur / Supervisor

Conditions spéciales ou commentaires / Special conditions or comments

550, rue Cumberland, pièce 154 550 Cumberland Street, Room 154
Ottawa (Ontario) K1N 6N5 Canada Ottawa, Ontario K1N 6N5 Canada

613-562-5387 • 613-562-5338 • ethique@uOttawa.ca / ethics@uOttawa.ca
www.recherche.uottawa.ca/deontologie | www.recherche.uottawa.ca/ethics

Université d'Ottawa

Bureau d'éthique et d'intégrité de la recherche

University of Ottawa

Office of Research Ethics and Integrity

Le Comité d'éthique de la recherche (CÉR) de l'Université d'Ottawa, opérant conformément à l'*Énoncé de politique des Trois conseils* (2014) et toutes autres lois et tous règlements applicables, a examiné et approuvé la demande d'éthique du projet de recherche ci-nommé.

L'approbation est valide pour la durée indiquée plus haut et est sujette aux conditions énumérées dans la section intitulée "Conditions Spéciales ou Commentaires". Le formulaire « Renouvellement ou Fermeture de Projet » doit être complété quatre semaines avant la date d'échéance indiquée ci-haut afin de demander un renouvellement de cette approbation éthique ou afin de fermer le dossier.

Toutes modifications apportées au projet doivent être approuvées par le CÉR avant leur mise en place, sauf si le participant doit être retiré en raison d'un danger immédiat ou s'il s'agit d'un changement ayant trait à des éléments administratifs ou logistiques du projet. Les chercheurs doivent aviser le CÉR dans les plus brefs délais de tout changement pouvant augmenter le niveau de risque aux participants ou pouvant affecter considérablement le déroulement du projet, rapporter tout événement imprévu ou indésirable et soumettre toute nouvelle information pouvant nuire à la conduite du projet ou à la sécurité des participants.

The University of Ottawa Research Ethics Board, which operates in accordance with the *Tri-Council Policy Statement* (2014) and other applicable laws and regulations, has examined and approved the ethics application for the above-named research project.

Ethics approval is valid for the period indicated above and is subject to the conditions listed in the section entitled "Special Conditions or Comments". The "Renewal/Project Closure" form must be completed four weeks before the above-referenced expiry date to request a renewal of this ethics approval or closure of the file.

Any changes made to the project must be approved by the REB before being implemented, except when necessary to remove participants from immediate endangerment or when the modification(s) only pertain to administrative or logistical components of the project. Investigators must also promptly alert the REB of any changes that increase the risk to participant(s), any changes that considerably affect the conduct of the project, all unanticipated and harmful events that occur, and new information that may negatively affect the conduct of the project or the safety of the participant(s).

Kim THOMPSON

Responsable d'éthique en recherche / Protocol Officer

Pour/For **Barbara GRAVES** Président(e) du/ Chair of the **Comité d'éthique de la recherche en sciences sociales et humanités / Social Sciences and Humanities Research Ethics Board**

550, rue Cumberland, pièce 154 550 Cumberland Street, Room 154
Ottawa (Ontario) K1N 6N5 Canada Ottawa, Ontario K1N 6N5 Canada

613-562-5387 • 613-562-5338 • ethique@uOttawa.ca / ethics@uOttawa.ca
www.recherche.uottawa.ca/deontologie | www.recherche.uottawa.ca/ethics

Appendix 5 – The Interview Consent Form



uOttawa

Université d'Ottawa

Faculté des arts

University of Ottawa

Faculty of Arts

55 Laurier Avenue East

Ottawa ON K1N 6N5

tél/tel. 613 562-5238

téléf/fax. 613 562-5240

www.uOttawa.ca

Project Title: Concerned Enough to Act? Privacy Concerns & Perspectives among Undergraduate Instagram Users

MA Candidate: Hongru Zhang

Email:

Supervisor: Dr. Daniel Paré

Email:

Purpose of the Study: This project is being conducted in partial fulfilment of Hongru Zhang's M.A. Thesis. The purpose of the study is to investigate the online privacy concerns and perspectives of undergraduate students, as well as their privacy protection behaviours in relation to Instagram. The data collection strategy for this project involves collecting responses to a short questionnaire and the conducting semi-structured interviews with a sample of 30 undergraduate students who are regular Instagram users and who are currently enrolled at the University of Ottawa.

My participation consists of completing the short questionnaire and participating in an interview. The total time needed to complete both activities, together, is approximately 45-60 minutes. I have been informed that Hongru Zhang that the meeting will take place using Zoom it will be audio and video-recorded. Following this meeting, I will be provided with a transcript of the discussion and asked to review it for accuracy, and to provide any additional comments or feedback. Upon completion of the session, the recordings will be transferred to a secure password-protected external hard drive. These recordings will only be used for analysis purposes relating to this project.

The questionnaire and discussion focus on:

- My perspectives on online privacy issues
- My privacy protection behaviours while using Instagram
- How I evaluate my privacy protection behaviours; and
- If I ever thought about leaving Instagram and the reasons why.

Risks: I understand that my participation in this study as an interviewee entails minimal risks, and confirm that the information I provide is being disclosed on a voluntary basis.

Confidentiality and Anonymity: I understand that any information I share will be, and will remain, anonymized, and that it only will be used in relation to Hongru Zhang's Master's thesis research as well as any subsequent academic publications emerging from this project. I also am aware that only Hongru Zhang and her M.A. Thesis supervisor will have access to any information I disclose, and that my anonymity will be protected throughout all stages of the project by the removing any identifying characteristics from both the information I provide and its analysis.

Conservation of Data: The interview materials, including audio and video-recordings of the meeting, electronic and print versions of the transcripts, and electronic and print notes will be conserved by Hongru Zhang for a period of five years in a secure manner using a password-protected USB drive. Both the drive and the printed materials will be stored in a locked cabinet in Hongru Zhang's private home office. Only Hongru Zhang and Prof. Daniel J. Paré will have access to the discussion materials.

Benefits of the study: My participation in this study will contribute to my gaining research experience and first-hand knowledge about empirical research procedures and, in so doing, complement the education I receive in my program of study. I will also have the opportunity to voice my own interpretations, understanding, and concerns about online privacy issues and to potentially acquire more knowledge about how to protect my personal information when engaging the platform like Instagram in my daily own life.

Compensation: In accord with ISPR guidelines, my participation in this study entitles me to compensation of 1 course credit point. If I choose to withdraw from the study, I may still be eligible to receive the points for my participation subject to established ISPR policies and regulations.

Voluntary Participation: I am under no obligation to complete the questionnaire or to participate in this audio and video-recorded interview and can withdraw from the study at any time and/or refuse to answer any questions without suffering any negative consequences. If I choose to withdraw and do not want my data to be used, I can contact the researcher and provide my ISPR # in order for my data to be removed.

Acceptance:

I, _____, agree to participate in the above research study being conducted by Hongru Zhang.

If I have any questions about the study, I may contact either Hongru Zhang or Prof. Daniel J. Paré.

If I have any questions regarding the ethical conduct of this study, I may contact the Protocol Officer for Ethics in Research, University of Ottawa, Tabaret Hall, 550 Cumberland Street, Room 154, Ottawa, ON K1N 6N5. Tel.: 613-562-5387 Email: ethics@uottawa.ca

I have shared a signed copy of this consent form with Hongru Zhang and have retained a signed copy for my records.

Participant's signature:

Date:

M.A. Candidate's signature:

Date: