Appealing to the Masses: The Allure of Social Media

By

Anna Alexandra Ndegwa

BSocSc. University Of Ottawa, 2014

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

In the
School of Criminology
Faculty of Arts and Social Sciences

SIMON FRASER UNIVERSITY
Spring 2018

Approval

Name:	**Anna Ndegwa**
Degree:	**Master of Arts (Criminology)**
Title:	**Appealing to the Masses: The Allure of Social Media**
Examining Committee:	**Chair:** **William Glackman** Associate Professor
	Richard Frank Senior Supervisor Assistant Professor
	Bryan Kinney Supervisor Associate Professor
	Lynne S. Bell Supervisor Professor
	Peter Chow-White External Examiner Associate Professor School of Communication
Date Defended/Approved:	January 26, 2018

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

a. human research ethics approval from the Simon Fraser University Office of Research Ethics

or

b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University

or has conducted the research

c. as a co-investigator, collaborator, or research assistant in a research project approved in advance.

A copy of the approval letter has been filed with the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

Update Spring 2016

Abstract

Social media is one of the most prevalent forms of communication in today's society. However, research has consistently noted that there are risks associated with the use of social media. The current study looks to understand what makes social media appealing to users that they forego or limit their privacy and security online.

Consistent with previous research, the current study found that users considered both self-disclosure and self-exhibition as appealing characteristics of social media. Users want to both look at other users and expose themselves to other users. However, the findings indicated that the way users treat social media depends on their awareness and cognition of the risks of social media use. Users utilized the platforms to limit the information dispersed about them, but were not as limiting with service providers. The findings also indicated that users lacked knowledge or understanding of what "personal identifiable data" entails, to the detriment of their online privacy.

Keywords: Surveillance, Social Media, Personal Identifiable Information, Self-Disclosure, Privacy, and Security

Dedication

Kwa Mama Wangu mupendwa Shitandie, asante kwa upendo wako, faraja na usaidizi katika safari hii. Nimekuwa na bahati kuwa binti wako. Nakupenda sana mama. na omba Mungu akubariki milele na milele.

Acknowledgements

I never thought I would be completing an MA. If you were to ask me this question 3 years ago, it was Law school or nothing. However, I realized sometimes life takes you on a path of growth that you would have never dreamed of. My MA was a right turn in my path through academia. Although Law school is on the horizon, this MA has led to so much growth within myself, which I do not think I would have gained if I entered Law school three years ago.

I am forever thankful for my mother, who through all of this gave me the direction I needed to complete this MA. I am, and will always be, an individual focused on the 'end' goals. Academically, I have always been the type of person who focused too much on the finish line and never on the path. My mother taught me that life is never how you dream it or try to control it. Life just is. Life should be led without too much worry on the miniscule and trivial things and I have learned to not focus on those. It took me a while to see that sometimes what stopped me from moving forward was my focus on trivialities and myself. My mother pushed me, and without her, this MA would not be what it is today. I am thankful for her truth, candidness and love. Shukurani sana Mummy.

I am forever grateful for my brothers Anthony and Albert. They carried me a long through the ups and downs with a lot love, laughter and support. We will always be the three musketeers. I love you back, my little womb-mates. Kwa Ndugu zangu Upendo wenyu na msaada kwa miaka mingi, Ninawapenda sana.

I would like to thank Dr. Ted Palys for his supervisorial guidance through this thesis and MA. He is an astounding academic and I appreciate the time shared while completing my MA. I would also like to thank Dr. Richard Frank and Dr. Brian Kinney for their supervisorial guidance in the final months of my thesis. Thank you for your help and support and for going out of your way to assist me in completing my thesis. I will forever be grateful.

I would like to thank Dr. Simon Verdun-Jones. I enjoyed every TA class and however-long sit-downs talking about anything and everything. I will always be grateful for your support and kindness throughout my MA and your belief in my path to being a lawyer. Words can neither qualify nor quantify your guidance and useful advice. I will forever be grateful to you.

I also would like to thank Dr. Lynne Bell. She gave me confidence to believe that I can be a published academic. Lynne never really liked my smelly burritos, but she put that aside and aided in my academic development. Thank you Lynne for also being a part of my committee.

I would like to thank my friends both home and away for sticking with me through this MA, as well as William and Emily and their children Oliana and Ethan for the support and assistance throughout my stay in B.C.; it was difficult, but I am grateful for all your love and encouragement nonetheless.

Finally, I would like to thank my participants, without them this thesis would never have happened. All my participants took time to talk about a subject that affects their lives every day. Social Media is one of the most prevalent forms of communication in the world; large populations of the world are users. I hope this thesis provides insight to its prevalence through the discussions I had with my participants. I thank them for taking time out of their day to sit and talk with me about a subject that sometimes seems so frivolous but is so relevant to society today.

Table of Contents

List of Figures

List of Acronyms

GIF	Graphics Interchange format: a lossless format for image files that supports both animated and static images.
PID	Personal Identifiable Data
FAQ	Frequently asked Questions

Glossary

Facebook	Content sharing Social Networking Site: Primarily used to connect with others
YouTube	Video sharing Social Networking Site
YouTube Guru/YouTuber	A YouTube user who creates content with a following of other (unknown) users
Newsfeed	Updated content from friends provided on the Home page of a user's profile
MySpace	Defunct Social Networking Site
Stream	The transmission or reception of data (photo, video, etc.) over the internet as a steady continuous flow
Thread	Linked messages posted on an internet forum that share a common subject or theme
Twitter	Text-based Social Networking Site
Ad-space	Area on webpage dedicated to online advertisements
App Store	Online Application software commercial marketplace
Web blog	Website consisting of entries updated frequently by website owner
Web sphere	Internet Web
Blogger (1)	A person who regularly writes material for a blog
Blogger (2)	A web-based Social Media platform allowing users to keep a blog, journal, or diary online
Post	A piece of writing, imagery, or other content published online
Snap	A post on Snapchat
Instant sharing	The exchange of posts/texts/content in real time
Friendster	Originally a Social Networking Site similar to Facebook, it is now a social gaming site
Social Media Correspondent	Individual with social media knowledge and influence
LiveJournal	Social Media platform which allows users to keep a blog, journal or diary online
SixDegrees.com	Social Networking service based on six degrees of separation; can list known individuals by the user on the site or externally
Chatroom	A space online where users can communicate about specific topics

Meet the Internet: Faces of Social Media

Source: https://wallhere.com/ko/wallpaper/545213

Chapter 1. Meet the Internet

"Smart phones and social media expand our universe. We can connect to others or collect information faster and easier than ever" – David Goleman

The evolution of Social Media is a breakthrough the 2000's will be known for, for years to come. Social Media, a broad term that encompasses social networking websites and a variety of social mobile applications has infiltrated the daily lives of the ordinary person in North America and the world. There are over 2 billion active individual users of social media applications and websites worldwide and this number grows by the second (Kemp, 2016). This phenomenon, which took its first modern strides in the early 2000's with websites like *Friendster* and the well-known *MySpace*, is now a dominating segment of the internet with the likes of *Facebook*, *YouTube*, and *Twitter* paving the way (*Digital Trends,* 2016). As such Social Media is of interest as a research topic due to its prevalence in contemporary culture. This thesis will be analyzing the fascination many individuals around the world have with Social Media and their perceptions of privacy and security in the online realm. Social Media platforms can be defined as services that allow users to "connect, communicate and interact" (McNealy, 2012b, p.139). Boyd and Ellison (2008) defined Social Media platforms as:

> …Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site (p.211).

For the definition to be complete a fourth element should be added which distinguishes actions made by the user within these services in addition to their function as social connectors. Social media within current technological culture expands past connectivity alone. As such, the definition of social media should include: (4) Social Media allows users to create and disseminate *content* to other connected users and/or the overall public. *Content* is defined within this thesis as any applicable medium permitted on the users' preferred social media platform within which the content is disseminated, (i.e. photo, audio, video, GIF or text etc.). For Social Media to remain relevant it must engage the user apart from being a primary resource for connectivity. Thus, by continuously innovating ways for the user to create content and share content onto their individual platforms maintains Social Media's importance.

In the age of the Millennial, individual users are both creator and consumer; creating careers making content or discussing content, (i.e., YouTube Guru, Social Media Correspondent) and consuming content with every newsfeed, stream or thread clicked onto. Social Media platforms are user-friendly, convenient and services provided are now indispensable to most. These virtual communicative platforms have cemented their spot in the minutiae of the ordinary individual and should be considered carefully to determine their impact, however unfavorable or positive it may be.

Social Media platforms allow users to curate social media outputs while also acting as audiences to other users' content. However, underlying these actions is the caveat, that, for better or worse, there is an acknowledgement and acceptance of a lack of privacy. Social Media platforms have been shown to forgo individual user privacy and cater to ubiquitous surveillance by corporations and governmental bodies (Angwin, 2014). Popular Social Media platforms are cost-free. However, corporations providing these services must profit somehow, otherwise what would be the point?

Initiated by technology giant Google, the advertising model of revenue accumulation serves to benefit technological firms like Facebook by commoditizing user data as a product to sell to companies for profit (Zuboff, 2015). These sites are in the business of accumulating small, inconsequential bits of user behavior and experience and aggregating them for the use of profit for other companies or advertisers. Zuboff (2015) coins this practice as *surveillance capitalism*. The established modes of revenue accumulation have been transformed to reflect both the business model of fee-free services and the technological advancements of these corporations. The ability to know more about individuals on a key-stroke-by-key-stroke basis and to use that information for profit is a turning point within the modern free-market system. Information about people have become more valuable in today's market and Social Media platforms are reaping the profits due to their built-in design model of *user-based sharing.*

Social Media platforms make use of the continuously updated information provided by users, such as demographic information and the different websites, content and items a user 'likes,' by selling said information and content to other corporations for a fee (Keenan, 2014). For example, currently *Facebook* has 1.71 billion active users worldwide (Statista, 2016). Through the use of advertisements, Facebook can charge corporations for ad-space on the Facebook platform and its subsidiaries, (e.g., *Instagram)*. Ads are then targeted to Facebook users, who either have

used the external sites or are within the targeted demographic of the corporations buying ad-space.

However, Facebook states within their Help Centre that they do not sell user information. Users have control over how their information is shared through the privacy controls on their account (*Facebook Help Centre,* 2016*).* Specifically, Facebook does not sell or rather ***share,*** *personal identifiable information* unless it is permitted. Facebook specifically uses the term *"sharing"* and specifies "identifiable information" to divert the user's attention from the fact that information other than the stated "personal identifiable information" is being sold. Personal identifiable information includes, but is not limited to, a user's name, email or phone number, (i.e., their contact information) (*Facebook Help Centre*, 2016). Users can control shared information within account settings. However, these controls are found under *Adverts* rather than *Privacy* (see Appendix 2). This is not easily found for the ordinary user and default settings allow Facebook to target advertisements based on user behavior. Moreover, Facebook has the ability to show adverts to user connections, i.e. Friends or Followers based on the user interests, (i.e., liking or sharing a post and target advertisements based on user preferences) (Facebook, 2016; see Appendix 2).

Facebook is not sharing information that would completely infringe users' privacy; however, the information being 'shared' to third parties is user information that is considered 'Big Data.' It indicates user preferences, which are valuable to corporations selling products. Facebook also has software that works external to their platform and subsidiaries called the Facebook *Pixel*. In summary, the Facebook *Pixel* is a type of coding software that companies and corporations can add to their website to "measure, optimize and build audiences for [their] ad campaigns" (*Facebook business*, 2016; See Appendix 2). It is a tool used with Facebook advertisements to build the corporation's consumer base by utilizing Facebook's own user base. The goal is to *connect* businesses with potential customers. Thus, though not explicitly selling user information, Facebook, and companies like Facebook, are "sharing" user information that is not "identifiable" to third parties. This information is more valuable to third parties as it reflects user preferences concerning different activities (e.g., cycling), events (e.g., presidential election), vendors (e.g., Whole Foods) and interests (e.g., sports teams), which can be used to target audiences who will buy products and/or share product information to other users.

Information-sharing applications and platforms like *Facebook, Snapchat, Instagram* and *YouTube* are changing how individuals communicate and interact with each other. In no other era

has it been so simple to communicate with another person in the same city, let alone in a different country, continent and time zone. However, the appeal of Social Media is not solely based on its basic communicative function. Social Media has allowed individuals across the globe to do more than *just* communicate with each other. The advent of Social Media and its numerous platforms have allowed individuals to participate in activities and engage individuals not possible without Social Media.

Social Media: A (very) brief history

In the late 90s, web-logs were introduced to the Internet as spaces to 'publish' personal commentary or journals online. At first, the web-log community was limited to those who had the affinity to make websites, but as more individuals created web-blogs, the more innovative Internet developers became. Web-blog services like *Blogger* and *LiveJournal* were introduced into the web-sphere, providing interested users a free and easy way to design and publish their own web-logs without the know-how of a HTML or website editor (Blood, 2000). Web-logging is the grandfather of Social Media platforms utilized today, as they mirror similar user behavior. Web-log users discussed their daily lives, provided social commentary and built communities through the exchange of content and interaction between bloggers. Coexisting at this time were sites like the now defunct *SixDegrees.com* and *Friendster*, which provided Internet users services where they could connect with other users already in their In-Real-Life social network. Early sites were platforms where users could give brief autobiographies and connect and communicate with real life friends online (Boyd & Ellison, 2008). *MySpace* and *Facebook* and later Social Media platforms were modeled roughly around the previous platforms' framework: virtual spaces where individuals can connect with other individuals within their social network to easily communicate. As these sites gained popularity however, they became more innovative and niche, attracting different user-bases based on interest, (e.g., photo-sharing *Flickr* or video-sharing *YouTube*) (Boyd & Ellison, 2008).

In 2017, there are a multitude of Social Media platforms that are cross-utilized by users and corporations worldwide. As such, larger Social Media corporations have taken to incorporating and acquiring smaller Social Media platforms to their portfolios with varying results. *Facebook* has grown to become a multi-billion dollar corporation and acquired popular photo-sharing application *Instagram* and messaging service *Whatsapp* (Constine, 2015; Constine & Culter, 2012). Google acquired the well-known video-sharing website *YouTube.* Both have incorporated user profiles from their own web-services into the sign-on parameters of *YouTube*

and *Instagram*, however, whereas *Facebook's* change in sign-on parameters (merging a user's *Facebook* profile to their *Instagram* profile) showed no real issue in integration, the linking of *Google*+ accounts and *YouTube* accounts caused some stir (Tassi, 2013). Some Users of YouTube were upset because the merging or linking of Google accounts/Google+ accounts diminished privacy for some users (i.e., anonymous users' real names were exposed) (Amadeo, 2015). While other users who discussed the linking of in real life accounts like Gmail to anonymous accounts as insignificant. Social Media has provided users the ability to discuss current events and share up-to-the-minute videos and commentary on daily occurrences others around the world would not be privy to, like the tweets and videos of the Arab Spring.

Although there are advantages to participating in Social Media, users are entering into an agreement, which can leave them at a disadvantage. Social Media corporations for the most part run unregulated in the handling and dispersal of user information, leaving the user in an insecure position (Goldfarb, 2015). Nonetheless, the service providers are not compelling users to post content. The user chooses to do so with the knowledge that the privacy and security of their information once uploaded is limited. Considering these conditions users enter into, what about these platforms is so appealing that users seem to forgo the privacy and security of information for the chance to post, snap or stream their lives?

This thesis looks to add to literature that focuses on the individual user. Its purpose is to understand the appeal of Social Media. Social Media Platforms are in constant demand, with new applications coming into existence every day. The processes of the applications used remain fixed, as functioning to maintain the continuous instant sharing of user content to audiences worldwide. However, the processes of the individual user, what they share, how they share it and the perceptions of both the user sharing and the users viewing are not fixed. Toward this end, the current thesis set out to better understand these processes and user justifications through discussion with individual users of social media.

Chapter 2. Social Media: A Review of Literature

"It's fine to have social media that connects us with old friends, but we need tools to help us discover new people as well" - Ethan Zuckerman.

Considering that Social Media, as we know of it today, has only been available little more than a decade, research into its use and impact is varied. The following review focuses on social media scholarship within the past 15 years. The following review discusses pertinent research on gratifications received due to use of Social Media and issues in online surveillance, specifically with concern to corporate surveillance and user privacy.

2.1. Definitional Distinctions

Prior to the discussion of social media scholarship, specific definitions must be made before enumerating on the literature. The definition of social media that will be used within this study is stated above, however, there are key concepts needing to be defined to better place what will be discussed within this thesis. Primarily, how does this thesis conceptualize *privacy*, public and private spaces online and as well as how *exposure,* or in Facebook terms: *reach,* is defined within this thesis.

2.1.1. Privacy Online

Privacy is defined within literature in a multitude of ways. Overall, it has been defined in terms of "secrecy (Posner, 1998); intimacy (Innes, 1992); [and] information control (Westin, 1967)" (McNealy, 2012a, p.255). McNealy (2012a) states that part of the reason behind the diversity in definitions is due to theoretical differences in discerning what is essential to the "kinds of information or relationships the law should protect" (p.255). As such, privacy can be understood in terms specific to law and the protection of individual rights. However, as stated, the definition of privacy does vary. Those used within law can vary from jurisdiction, just as definitions used without law as a qualifier can vary.

Consequently, conceptualizing privacy online is difficult due to its ambiguity. Moreover, for the online user, what is considered private is not necessarily privileged information by lawmakers. Conversely, the law can privilege information that users do not otherwise consider private. Moreover, definitions of privacy between users and within privacy scholarship can differ greatly,

as is reflected in usage of social media. Users disclose information online to varying degrees; however, there is a presumption that some of this information is concealed (i.e. direct messaging between users on platforms). However, the nature of the Internet, which is characterized as a boundless space, does not marry well with privacy as defined in terms of accessibility and the restriction of information.

2.1.2. Privacy Theories

Privacy has been conceptualized as "spatialized right to solitude and…an informational right to confidentiality (Squires, 1994 *in* McNamara, 2009, 11). However, to some these conceptualizations are "being eroded as a result of the … exploitation of new technologies of communication and observation" (338 *in* McNamara, 2009, p.11). As stated, there is debate over how to define and apply a definition of privacy that fits the scope of the Internet. For the purposes of this thesis privacy was defined using a combination of five theories that held relevancy to current research question; Westin's (1967) and Altman's (1975) theories of privacy, Petronio's (2002) Communication Privacy Management theory; Strahilevitz (2005) Social Networks Privacy theory and Nissenbaum's (2004; 2010) Contextual Privacy theory. An applicable definition of privacy for the online world should provide both an understanding of relationship between a user and service provider as well as the agency a user holds when interacting with and within online spaces.

Westin (1967) and Altman's (1975) theories of privacy both focus on how individuals limit access to information about themselves. Each focus on the agency an individual has when determining how much information is dispersed to others about themselves. Westin (1967) views privacy as a function that allows an individual the ability to limit the amount of information dispersed about them and the extent they were observed by different means (i.e. psychological or physical) (Margulis, 2011, p.10). Altman (1975) included agency in his definition but added an understanding of privacy as a social process that involves both cultural norms and spatial understanding of an individual's social world. This process was a dynamic interplay between individuals, where the individual negotiates access between themselves and others (1975; 1990, *in* Margulis, 2011, p. 11).

Petronio's (2002) theory of privacy is consistent with both Altman (1975) and Westin (1967). Petronio (2002) adds to the literature by discussing privacy in terms of a rule-based system of boundaries, where the individual claims ownership over information about them and

controls the flow of that information to others. The individual regulates to whom information is shared, how much is shared and "the level of shared ownership" with others (Margulis, 2011, p.12). Individuals then become co-owners of that information, once it is shared, (i.e., shared responsibility the management of its dispersal). Thus, if tension occurs between owners, the management of the flow of information could fail, as the obligation to protect that information is not upheld (Margulis, 2011, p.13). This dynamic of co-ownership of information is important to the relationship between users and service providers. If the user is placed in a position of relative power with regards to regulating the dispersal and flow of their information, the service provider, by being placed on equal footing, takes on a level of responsibility that is actionable, if or when they fail to uphold their obligation to protect the information shared to them.

Westin (1967) and Altman (1975) place value in the agency held by an individual when controlling the amount of access others have to information. Petronio's (2002) theory furthers both theories by giving nuance to the process of boundary negotiation between users, how much to disclose and the collaborative relationships held by co-owners when maintaining individual privacy. This negotiation is important as users could be assuming the user-provider relationships are collaborative in nature, when it has been shown to be otherwise.

Strahilevitz's (2005) social networks theory of privacy is a legal discussion of how courts should treat the expectation of privacy when discussing the exposure of user information. Rather than ask the question "did this individual reasonably expect their information to remain private?" Strahilevitz (2005) asks how much exposure would the information have had in the eyes of the person disclosing it i.e. how far-reaching would the exposure be. Important to the current thesis is Strahilevitz's (2005) discussion of super-nodes and peripherals, which could be viewed in terms of Friends (super-nodes) and Acquaintances (peripherals). Any information a person discloses is dispersed to varying degrees based on how strong or weak their ties to other individuals are. As such, a person's expectation of privacy is based on whether the risk of the information being disseminated beyond their social circle can be realized. So, individuals make calculated risks in whom they disclose to by assuming the information disclosed would remain within a radius giving them a reasonable expectation of privacy. This marries with the previous theories as individuals negotiating both the access and co-ownership must also have rules of disclosure based on the level of intimacy they have with others in their social circle.

At the time of writing Strahilevitz had issues with how to apply this theory to online networks, as intimacy between users is not completely detectable (McNealy, 2012b, p.154). The

inability to differentiate between connections neglected “the fact that an SNS user may want to disclose information to some connections and not to others” (p.154-155). However, this issue could be resolved through user behavior, their treatment of different social media and the varying sizes of followers per Social Media platform. A user could restrict each friend group by the intimacy shared with each friend; thus, the larger the following, the higher likelihood of weaker ties, the lesser likelihood of the user disclosing exceedingly private information. This would be an interesting resolution if found within the current thesis’ results.

Finally, Nissenbaum’s (2004) theory of contextual privacy adds to this discussion as it focuses on privacy’s relation to public surveillance. This is important to the current thesis as I focus on the yielding of privacy by users for a service, which could be viewed as permitting surveillance. Similar to Strahilevitz (2005), Nissenbaum’s is consigned to legal scholarship’s understanding of the expectation of privacy. Namely, public surveillance is common because individuals give up privacy when entering public spaces; a person cannot have a reasonable expectation of privacy in public because it would limit others freedom (Nissenbaum, 2004p. 135-136). Nissenbaum discusses privacy in terms of context. Should an individual expect privacy based on the contextual understanding of their situation? Two norms support this; whether it is appropriate to reveal information about a person in a given context and whether the information should be revealed at all. These norms work with relational norms to regulate the flow of information. This complements the previous theories as how intimate a person is with another user as well as the context within which they disclose the information can guide how that information can be dispersed.

Consequently, privacy within this thesis will be understood using characteristics of the aforementioned theories. Firstly, privacy can be understood as an individual’s ability to control and limit the accessibility of their information to others (Altman, 1975; Westin, 1967). Boundaries between the individual disclosing information and those they disclose to, are negotiated spaces (Altman, 1975; Petronio, 2002). Moreover, the level of intimacy held between these parties, (i.e. the discloser and the disclosed to, dictates to whom and how much information is dispersed). The relationship between the two parties should be collaborative. (Petronio, 2002; Strahilevitz, 2005). Finally, these should be placed within a contextual understanding of exposure (Nissenbaum, 2010; Strahilevitz, 2005). An individual’s expectation of exposure when disclosing information inclusive of those disclosed to, and the information disclosed, is important to understanding how users view their self-disclosures when engaging Social Media.

2.1.3. Virtual space

At its root, what distinguishes public and private spaces is “the distinction between things that should be shown and things that should not be hidden” (Arendt, 1958, in Fuchs, 2012, p.147). In relation to the Internet, it is a space that can be considered public due to its broad accessibility. Virtual public spaces are generally considered spaces where (1) all users have access without restriction and (2) spaces where users share content to the overall ‘public’. As there are no restrictions on access by other users or restrictions over the sharing of content, there is no expectation of privacy over the information shared. However, some users assume they have a level of privacy over some of the online spaces used, specifically those spaces which the overall public cannot directly access. If users can restrict access to their content, the expectation is that those without permission will be unable to access the restricted content. However, considering the public character of the Internet, regardless of restrictions, a user has an audience tied to the content they share. As such, their expectation of privacy is not warranted. Any information within the social media platforms used can be dispersed outside of the user’s social network, (e.g. when another user screenshots an image or message and sends it to other individuals outside of a social platform), negating their privacy.

2.1.4. Exposure

Finally, within the discussion of privacy and virtual spaces, how ‘exposed’ an individual is on their social media was important to consider when discussing the appeal of social media. Within social media, exposure is represented as *reach*. Reach is termed as the “number of unique people who have seen content associated” with an individual user or corporations’ profile (Smitha, 2013). A user’s content can be viewed a multitude of different ways, (e.g. like, share, comment, reaction). Those actions can appear on each user’s friends’ feeds, thus expanding the number of unique users viewing the content. *Exposure* within the current thesis using this understanding of reach is defined as:

> How far reaching a user’s activity, (i.e. postings, shared content, liked content), is on their prescribed social media in relation to the number of unique users who view, follow, like, comment and/or share that user’s content.

When considering how exposed an individual user is, how far reaching their posts or profile is, is significant. If an individual acknowledges that what they post may be viewed by an innumerable amount of unique users, they must understand that their privacy is limited. What will

be considered within this thesis is: if this is an underlying acknowledgement, how do users justify the limit in privacy with continued use. Herein, I am specifically considering users thoughts on having an audience as reach signifies *both stated and known views and unstated and unknown views.* Users do not have the ability to accurately estimate the amount of views a post will have as other users do not have to react to the content (e.g. a user can look but not take action).

2.2. Theoretical influences

This thesis used the Straussian grounded theory approach, which allows for some prior knowledge gathering to analyze findings. Two theories: Clay Calvert's work on *Mediated Voyeurism* and Erving Goffman's work on *Self-Presentation in Everyday Life*, will be applied to the overall findings and discussion.

2.2.1. Clay Calvert's *Mediated Voyeurism*: The Peeping Masses

Calvert (2000), conceptualized the notion of *mediated voyeurism* as " the consumption of revealing images of and information about others' apparently real and unguarded lives, often yet not always for the purposes of entertainment but frequently at the expense of privacy and discourse, through the means of mass media and Internet" (p. 2). Although developed a decade prior to the popularization of social media, social media can be viewed as the contemporary means of consumption fitting this idea. Calvert argues that mediated voyeurism "thrives when privacy is devalued and privileges spectating over interaction and discussion"; the devaluation of privacy within mediated voyeurism involves the willing consent by individuals to diminished privacy (p.3). Individuals must be willing participants to their exposure. Furthermore, individuals must also acknowledge their desire to view such exposures. If society accepts and encourages both, the culture of mediated voyeurism will persist. For Calvert, the emergence of new technologies, (i.e. camcorders, electronic surveillance equipment etc.), has led to "more intense and even more intrusive and pervasive forms of voyeurism than at any time in history" (p.10). At the time of its publication, Calvert's *Mediated Voyeurism*, spoke about 'new' Reality TV, which included *The Real World*, True-life *Dateline* and the early renditions of cam-girl sites on the Internet.

Social Media has eclipsed some of these mediums, like a catchall, as it satisfies users' needs to view other people's lives in one sitting. This form of voyeurism "values watching over discussing, sacrifices privacy for others' entertainment and enlightenment, and demands

protection for often aggressive and intrusive gathering of visual images and information" (p.24). In effect, mediated voyeurism is the allowance of surveillance of others with the protection of anonymity (p.69). This situates the voyeur in the "privileged, and powerful position of [a watcher]" (p.69). This position is a selling point for most providers of reality media. Though less popular now, the principle of reality media remains: "reality sells" (p.101). Individuals want to consume another individuals' reality. To Calvert "voyeurism thrives on our diminished expectations of privacy and our willingness…to expose our lives on camera or to tolerate such exposure" (p.82).

Calvert uses Derlega & Berg's (1987) definition of self-disclosure to inform his discussion; self-disclosure was "loosely defined as what individuals verbally reveal about themselves to others" (Calvert, 2000, p.83). Self-disclosure within mediated voyeurism is described as the engagement of impression management "by selectively and strategically revealing certain pieces of information to influence others' opinions" (p.84). For Calvert, exhibitionism in the form of self-disclosure served mediated voyeurism. If there was no one *disclosing* anything, then what would we watch? However, Calvert notes that the need to be a voyeur conflicts with an individuals need for privacy and the "control [of] the dissemination of information" about themselves (p. 82). Thus, a voyeur must strive to balance their need to see with their need to keep hidden. Mediated voyeurism could be applied to social media, which appears to be a more intrusive and more pervasive method of surveillance than the early 2000s camcorders and early electronic surveillance mediums.

2.2.2. Goffman's *Self-Presentation in Everyday Life:* Staging the Self Online

"*All the world is not, of course, a stage, but the crucial ways in which it is not are not easy to specify." – Erving Goffman (1959, p.72)*

Erving Goffman's theory aligns itself to the online world as most social interactions are migrating online. The theory of self-presentation provides the metaphor of the social world as a stage, where individuals are actively providing an impression of themselves to others. Goffman understood social interaction as a conversation of control; where the individual guides the impression given to others while others obtain information. These impressions are claims made by the individual of how they "are" as a person to be believed by an audience. The individual is thusly judged on the impression given (Lemert & Branaman, 1997, p. 21). The management of this front stage is related to keeping the impressions or claims made to an individual's audience consistent. The individual provides signs to their audiences, which are substitutes for reality (p.22). The complete picture is not shown but full control over the desired impression given is

impossible. Individuals provide verbal and nonverbal signs constantly. The biggest concern for an individual is if their impression can be discredited (p.25). If individual's claims are not consistent, their whole identity can be called into question. However, complete consistency may not be attainable as different roles call for different claims, thus individuals isolate audiences to mitigate these conflicts. Finally, for some individuals claims and impressions are means to an end, whereas others reflect their true selves. Goffman's theory can be applied onto social media as social media is based in social interaction. I posit that each platform can be viewed as a stage with different audiences and different or similar claims made about an individual's self. The interactions that take place in real life can be, to some extent, paralleled onto the online realm. Therefore, how individuals manage impressions they make in real life could be viewed as similar or consistent to those they make online.

2.3. Previous studies

Two smaller studies were conducted prior to the commencement of the present study, which provided a foundation for the present thesis. Each was completed in 2015; the first was an exploratory study that provided the motivation to complete the second study and this thesis. Each study gave an understanding of user's perceptions of social media and its use in their daily lives. Each study used a similar study design, which was adopted again within the current thesis.

Generation non-disclosure

The exploratory study undertaken in the Spring of 2015 was designed to gain preliminary insight to the management of online social identity. The primary research question was: *How do individuals manage and project their identity onto social media platforms and how do their real life roles and responsibilities affect this projection?* Study participants were university students between the ages of 18 and 25. Findings indicated that there was a decision-making process used by participants when sharing content that was guided by their awareness of the risks posed by social media use. Their strategies focused on filtering content to alleviate these risks, while also maintaining an authentic virtual self. Participants were aware of how far-reaching posts shared could be and managed their outputs using this awareness (Ndegwa, 2016). If posts shared online are not secure and there are limits to controlling viewership of shared content, selective filtering prior to sharing is important to how users chose to curate their online presence and consumption. The agreement users enter into and acknowledge is much like a unilateral non-disclosure agreement. Party A discloses information to Party B with the condition that the

information provided will remain confidential (Kowalski & Krattiger, 2007). However, Party A fails to read the fine print which allows Party B to leak information onto the larger Internet for commercial purposes, leaving Party A to manage their information with the knowledge that any ownership claim to their information once shared is lost. Therefore, the user places themselves in a position where they are managing the *dispersal* of their online identity rather than the identity itself and moreover are managing this dispersal without full knowledge or understanding of the policies or actions of Party B, the service provider (Ndegwa, 2016).

Anonymous Creep Factor

The pilot study conducted prior to the current research study was undertaken in the Fall of 2015. The study used a similar sample group to the exploratory study. The primary research question was: *If users were entering into an agreement that held them at a disadvantage; what made Social Media so appealing that users a) agreed to the conditions of their use and b) in compliance to those conditions, set conditions upon themselves to 'safely' participate within the virtual platforms without complaint (or lack of substantial complaint)?* Findings indicated that participants were utilizing social media as a form of user-to-user surveillance. However, this voyeuristic behavior was viewed as a pervasive and commonly accepted practice within social media. Being a 'creep' within social media was a fluid notion. Participants understood that their level of anonymity or lack thereof in relation to those they were creeping played a factor in whether their 'creeping' behavior was seen in a positive or negative light. As such, unknown users who notify the viewed user of their creeping behavior are viewed negatively, whereas those who do not notify are neutral creeps (as there is no perceived harm). Overall, findings suggested that the consumption of other users' lives was aided by social media platforms. The accessibility provided to be spectators to other users, to compare, vilify, glorify or just watch, held some fascination with participants. However, though creeping was normalized, it was engaged in private.

The previous study indicates part of the appeal of social media is based on the gratifications received by the peeping and revealing for information. I assumed prior to commencing this research that users were more accepting of creeping behavior (both theirs and corporations') due to the normalization of the behavior. This proved to be a reasonable assumption. However, within the second study I was unable to assume that this normalization would substantiate an allowance of ubiquitous surveillance. As such, the current study looked to delve deeper into the gratifications received by users to determine whether the user was misguidedly valuing platform appeal without thought of the ubiquitous nature of the Internet.

2.4. User Gratification

Research into the gratifications individuals receive when viewing media is far-reaching. Relevant to the current study is research concerning voyeuristic, narcissistic and exhibitionist tendencies and gratifications related to social media use. Relevant voyeurism research discussed voyeurs as external to previous sexualized and pathological definitions (Baruh, 2010). Being a voyeur, within this conceptualization, can be viewed as a common characteristic of the ordinary person (p.203). Unlike the sexually deviant voyeur, who gains gratification through compulsively "observing, stealthily, [their] erotically preferred gender" (p.203), the 'common' voyeur "desire[s] to peek at what should normatively not be accessible" through safe or sanctioned means (p.204). This "peek" is usually fulfilled when the information they desire is "readily available for easy and safe consumption" (Mann, Ainsworth et al, 2008; Sullivan, 2008, as cited in Baruh, 2010, p.204). Different forms of media provide the means to satisfy this desire for the common voyeur or 'lurker' ("someone…who observes") namely reality television and now social media (Baruh, 2010; Bagdasarov et al, 2010; Ferrucci et al, 2014; Panek, 2014; Munar, 2010, p.412).

As such, studies have discussed how social media permits the user to 'peek' into other user's lives, which satisfies the voyeuristic desire as well as conversely how social media permits users to disclose to other users their lives publicly, satisfying exhibitionist tendencies (Baruh, 2010; Wang, 2015). Moreover, technology corporations are "increasingly building Internet services that elicit ever more detailed disclosure from individuals" (Joinson et al., 2011, p. 34). In life, to self-disclose is a normal part of social interaction. By promoting self-disclosure, social media allows the user to be both voyeur and exhibitionist. This conceptualization of the voyeur-exhibitionist could inform the underlying motivations of the sharing of content and to an extent the purpose users espouse to social media (Wang, 2015).

Research has also discussed social media as a platform for narcissism. Users' impression management relies on their valuation of online social attractiveness and sociability. The 'like' button functions to reinforce the attractiveness of their constructed identity. As such, social media may facilitate the elevation and maintenance of self-esteem as it satisfies users' desire for approval (Buffardi & Campbell, 2008; DeWall et al, 2011; Gentile et al, 2012). Overall, this scholarship is of interest to the current thesis' discussion of appeal. If users are receiving gratification from social media use, it follows that this gratification could hold a higher value than privacy to the user.

2.5. Issues in Online Surveillance & Privacy

2.5.1. Issues in corporate surveillance and user privacy

Research on social media and social networking sites and platforms has focused a considerable amount on the risks associated with the use of such platforms. Research has discussed the dark side of social media, namely hacking and cybercrime (Cross, 2015). Risks can affect both corporations and the individual and scholarship discusses ways to mitigate them: such as restricting access to user profiles, changing names on social media or using less popular and supposedly more secure platforms to do similar activities (Angwin, 2014; Cross, 2015). However, by doing so, these restrictions could cost a user the "functionality and/or ease of use" that popular Social media platforms provide (Angwin, 2014; Cross, 2015). This research also discussed how individuals are risk-takers by agreeing to the terms of service and the default settings provided by service providers seemingly without concern over whether these settings protect the user's privacy. This may be due to misinformation or ignorance (Fogel & Nehmad, 2009). A user is left to self-regulate the disclosure of their information, without clear knowledge of how the platform 'shares' their information (Fuchs, 2012, p.142). This research has also included discussion on the risks faced by corporations as well, like data leakage (due to hacks or social media use within corporations) and the issues in implementing solutions to lessen the impact (Everett, 2010). Any risks faced or created by corporations invariably have a detrimental effect on user security.

A large majority of research on social media and social networking sites has focused on corporations and governmental use of user content and information to their own ends. There is constant evidence that the information and content individual users upload is never secure, and corporations are not regulated to maintain user privacy either (Goldfarb, 2015). Schneier (2015) discusses how corporations like Facebook and governments collect and store user data for their own agenda. Corporations use this information to sell to advertisers and other corporations and even academics. Corporations do not share the same restrictions as other third parties, (e.g. law enforcement), in terms of access to content, as "no laws are being broken by retrieving information from public airwaves" (Keenan, 2014, p.202; Qi & Edgar-Nevill, 2011). Moreover, users have agreed to this retrieval when agreeing to the terms of service upon signup (p.203). Social media corporations can commodify user behavior and private information uploaded onto the site, while "hiding these processes" from their user base (Fuchs, 2012, p. 147). Social Media platforms are taking the "surplus value [user content] [which is then] appropriated and turned into corporate

profit" (p.143). This surplus can be anything from "generated data, personal data, [and] transaction data about browsing and communication behaviors" (p.143). Social media giants like Facebook push the idea that sharing is better; what would be the point otherwise? However, "sharing…in economic terms means primarily [the corporation] shares information with advertising clients" (p.155). Social Media's understanding of privacy is completely "property-oriented" in terms of them owning user content (p.155). For the ordinary content creator, being paid for their creation may not be an achievable reality in today's marketplace. There are users who make a living creating content, (i.e. YouTubers, Influencers, Bloggers/Vloggers, Gurus), however for the ordinary user, once content is uploaded onto public third-party sites, the uploaded content is not owned by the user (p.143). The content takes on a more public character and the availability of this information allows social media to maintain its "capital use of personal data" (p.142)

Furthermore, corporations and governments are carrying out ''ubiquitous surveillance'' on the populations that use these platforms with an almost laissez-faire consent by the users. Schneier (2015) muses that "[something being] free warps our normal sense of cost versus benefit and people end up trading personal data for less than its worth" (p.136). Facebook exemplifies the cost of agreeing to the ubiquitous surveillance as it continuously changes the terms and conditions of use. Facebook "regularly update[s] its privacy policy to obtain more access to [user] data and give [users] less privacy" (p.137). Users are left insecure but seemingly "do not mind based on convenience" (p.139). Keenan (2014) discusses similar points to Schneier' (2015) including FBX: the Facebook exchange; "real life-bidding platform where companies' purchase access to [user] eyeballs through sponsored advertisements" (p.204). The Facebook Pixel and other Facebook applications, as stated previously, fall into this FBX. To some, the *quid pro quo* exchange between user and service provider could be normalized due to its supposed benefits (Varian, 2014 *in* Zuboff, 2015, p.82, 84). However, is the exchange actually beneficial? Zuboff (2015) states that the exchange is not an 'exchange'; it is a unilateral decision on the part of the surveillance capitalist corporations to take the information. There is no real reciprocity between the user and the service provider. The user is not viewed as the costumer in surveillance capitalism; the advertisers and those buying user data are viewed as the customer (p.80). Thus, the use of user information is one where the user loses certain rights to privacy for the benefit of the service provider's bottom line.

Policies managing corporations' use of user information promote self-regulation. Corporations are defining "their own personal data processes," as such commercial surveillance is not "hindered by regulatory processes that may look to interfere with their bottom line" (p.147).

Fuchs states that by "leaving commercial surveillance untouched in order to maximize profitability" the protection of user information is lost; "when privacy regulation is voluntary, the number of organizations protecting the privacy of consumers tend to be very small (Bennett & Raab, 2006, p.171 *in* Fuchs, 2012, p.147). The model of surveillance capitalism serves to redistribute privacy rights from the individual user to the corporations using user information (Zuboff, 2015, p. 83). By relying on self-regulation and the free-market system, corporations seem to have more rights to privacy than individual users. Zuboff (2015) notes, de-regulation has allowed corporations to "deprive populations of choice in the matter of what about their lives remain secret" (p.83), essentially removing the choice of an individual to opt-out of their surveillance. This removal is marketed as a necessity and concealed from users due to their lack of comprehension and the delayed response by lawmakers. As such, corporations are able to maintain their continuous surveillance of user populations and the development of more sophisticated applications (Zuboff, 2015).

2.5.2. User privacy concerns & user-to-user surveillance

Research has indicated that users are varied in how well they "guard[ed] their privacy" online (Keenan, 2014). Service providers like Facebook's ever-changing privacy settings and conditions leave many users concerned over the loss of control and accessibility of their information (Hoadley et al, 2010). Danah Boyd's (2014) book *It's Complicated* focused on a specific group of users: Adolescents. Adolescent users were more concerned with having privacy from real-life institutions and people (i.e. school authorities and their parents). As such, social media was viewed as a personal space for interaction and escape. This did not mean that their online presence was a free-for-all, adolescent users did not provide all-encompassing information about themselves (p.203). Boyd's research also indicated that there was disconnect between adults and adolescents in terms of definitions of privacy and perceptions of privacy (p.209-215).

Similar to other research, adolescent users' utilized strategies to maintain their privacy on social media, however like most users, the convenience and ease of use of these social platforms could trump restrictions that could improve their privacy (p.232). Moreover, like other users, adolescents were unlikely to use extreme measures (deactivating accounts, exclusion tactics like posting to specific individuals) to maintain their privacy (p.255-256). Furthermore, adolescent users understood that to achieve a modicum of privacy, privacy was an "ongoing process because social situations are never static" (p.218-219). Moreover, as Boyd notes "it is hard to manage how information will flow within a social situation when the underlying affordances change regularly"

(p.221). As such, users were concerned over controlling information dispersed to other users rather than to service providers (Heyman, De Wolf & Pierson, 2014, p.29). These strategies were of interest within the present study. If similar types of strategies were found, the current study would complement Boyd's work.

Users can also be part of the problem. Users can breach other users' profiles by simply figuring out, stealing, or knowing the password to log on. For example, ex-intimate partners could log into each other's social media platforms due to the other delaying changing their password. These types of breaches could lead to malicious postings such as Revenge Porn and/or a complete lockout of the profile from the owner. Users could also be part of the problem by simply deceiving other users they interact with online (Keenan, 2014). Deceptive interactions between users can include forms of disinformation ranging from posting misleading images to users creating completely separate identities, which has been termed as 'cat-fishing' (Schulman, 2014). The discussions on individual to individual deception has centered on why individuals may resort to these forms of deception, which is of interest as this could relate to users' interest in surveillance. However, this research has mainly discussed how an individual's environmental and psychological situation (depression, loneliness, feelings of needing an escape) could lead to these forms of deception (Schulman, 2014). In his book, *In Real Life*, Schulman (2014) chronicles his foray into the 'cat-fishing' phenomenon where individual users deceive other users about their identity. The book was of interest as it discusses some reasons why users take on alternate identities and how others fall into these traps. The focus centered on users creating a different reality, but the book did discuss alternative 'cat-fishing' like fraud, which Keenan discusses in *Technocreep* with the example of email scams (Keenan, 2014; Schulman, 2014). Schulman's first-person discussion on individual user interactional issues does lend itself towards privacy concerns as more often than not the identities created by the 'cat-fishing' users are taken from real people and their social media platforms.

Overall, the literature on social media focuses on varying points of discourse that either delve deep into issues of privacy within social media use and surveillance or discuss user-to-user interactions within social media. The research question of the current thesis is to understand *whether the appeal of social media mitigates the apparent lack of privacy given to users participating in social media* (i.e. relinquishing ownership of information/content). I hypothesize that the appeals or gratifications provided by Social Media will not mitigate the limits of control users have over their information and their perceptions of how much control they have. Privacy

and security of information could have a higher value than connectivity or other gratifications discussed in the literature above.

Chapter 3. Methods

"Social Media is an amazing tool, but it's really face-to-face interaction that makes a long term impact" - Felicia Day

3.1. Methods

The methods used within the present study are modeled from the two aforementioned smaller research studies conducted in 2015. The first study conducted provided a framework to the current research design with regards to sampling and data collection. The secondary study acted as a pilot study, where the interview structure and questions used were employed within the current study. Focus groups and singular interviews were deemed useful to the proposed research, as the method allowed for open-ended discussions between the interviewer and the interviewee as well as between interviewees within focus groups. Interviews and focus groups used a semi-structured interview schedule, which provided the flexibility of pursuing ideas or further discussions and allowed for participants to elaborate and probe other participants where other methods would not have allowed for such inquiry (Gill, Stewart, Treasure & Chadwick, 2008). By using a conversational method of interaction during interviews, the information gained from a discussion, especially in terms of the processes used by users to post, rather than focusing on the post itself, seemed more substantial of an endeavor. This combination of methods proved fruitful in my exploratory studies; the current research study implemented a similar structure in data collection and analysis.

Focus groups and interviews provide a 'permissive [and] non-threatening environment" wherein which participants can discuss their perceptions of an area of interest without censure (Kreuger, 1988). Specifically with regards to focus groups, a group interaction provides a dynamic where information is revealed where it may not have in any other environment (Kitzinger, 1995). An interview offers the same objective of gaining information through conversation, which lends itself to the participant's perspective, and level of comfort (Berg, 2009). This dynamic has proven to be fruitful in the previous undertakings as it led to conversations concerning differing uses of similar platforms, differences in how users manage social media, and differences and similarities in user perceptions of privacy and surveillance on social media and how these perceptions affected their use of social media. Due to the success in implementation of the aforementioned

methods in my previous smaller studies, the current research study implemented a similar structure in data collection and analysis.

3.2. Data Collection

Two different populations were sampled: Adolescents and University Students. Accordingly, two parallel sampling procedures were used to recruit research participants. Convenience sampling was used to recruit participants at the university level. Students were required to be current students of Simon Fraser University in either undergraduate or graduate programs. University students were chosen because they are young adults who have grown up in a digital world, and many, if not most, are connected to more than one social media site or application. For the University sample, a study protocol and information sheets were provided to the Research Ethics Board (See Appendix 3). The adolescent participants were not as easily accessed. Adolescents are considered a vulnerable population and different district school boards have varying ethical review processes researchers must undertake prior to accessing a sample population within a primary or secondary school. I was able to gain access to an Adolescent sample within a semi-private school within the greater Vancouver area due to my own social network. The school is a well-respected day school providing International Baccalaureate programs for students in kindergarten through to grade 12 and boasts a high percentage of graduates attending universities across Canada and around the world. A family friend who has children that attend a semi-private co-educational independent day school in the lower mainland placed me in contact with senior administration that were amenable to a study being conducted at their school. The school had its own internal ethical review processes to which I submitted a proposal and met with administrators. With regards to the overall ethics review process, due to the use of adolescents within my sample population, I had to provide a vulnerable persons Criminal records check (CPIC) to both the secondary school and Simon Fraser University Research Ethics Board to be able to have any interaction with the adolescent participants (See Appendix 3). Also within the ethics review process, the secondary school provided a Letter of Amenability to the Research Ethics Board as part of the documentation needed for data collection. This documentation will remain confidential, as it has identifiable information that could limit the anonymity of my adolescent sample group. I submitted 2 different information sheets for both Parents and Adolescents, which were provided to both the school and the Research Ethics Board (See Appendix 3). Appendix 3 also includes the Adolescent study protocol submitted to the Research Ethics Board. A sample of the questions to be asked to each sample population was

also provided to the Research Ethics Board. Please see Appendix 3 for the Minimal Risk approval Form and Annual Renewal approval form.

Recruitment

University level participants were recruited using two different methods. The first began by sending an email to all department secretaries at Simon Fraser University, which included both undergraduate and graduate departmental secretaries (See Appendix 1). Four departmental secretaries acknowledged my email and posted the email invitation to their students; this generated 9 participants. The other method used in recruitment was through a flyer distributed around Simon Fraser University (See Appendix 1). This recruitment method did not gain any participants. In the end, eight undergraduate students and one graduate student participated. All were aged between 18 and 45, with four participants between the ages of 25 and 45. Five participants were male and four were female. Interviewees were provided with an information sheet prior to the commencement of the study once indicating interest. I also discussed the information sheet with the students prior to the commencement of the interview. Interviewees provided verbal consent once they understood the overall objective of the study and their ability to withdraw. University Students were individually interviewed within the study process. This structure was chosen due to previous experience with scheduling conflicts with focus groups at the University level. Individual interviews with University students allowed for more flexibility in scheduling. Each student was interviewed within a secure room in the School of Criminology, between the 15th of June 2016 to the 30th of June 2016.

Adolescent participants who volunteered were scheduled at a mutually convenient time during school hours. Students were provided information sheets indicating the purpose of the study, which were also provided to students' parents (See Appendix 3). If both the parent and student were amenable to the study, verbal consent was to be provided by the parent and student to the school administrators. If parental units were not amenable to their child participating, students would verbally indicate as such prior to the commencement of the study. If parental units were amenable, students would verbally indicate as such prior to the commencement of the study. Only those with the aforementioned consent were allowed to participate in the interviews. The school administrators had a list of students who were amenable to the study and had provided required verbal consent. On the interview day, these students were given a choice of a time within which they could participate. The focus groups were conducted in the morning between 830AM to 1230PM. Focus groups were primarily used to interview the adolescent sample as it proved

more convenient a method of data collection and due to the scheduling conflicts provided a larger sample than individual interviews could have provided. However, students were provided the choice of individual interview or focus group interview and were more amenable to focus group interviews with their peers. The study was conducted on the 16th of June 2016. The secondary school provided a secure room within which the focus groups were conducted within the school. Scheduling difficulties and end-of-year activities precluded a broad cross-sectional sample. Primarily, the study looked to gain participants between the ages of 13 and 17 and prior to issues in the length of time taken in ascertaining ethics approval, it was posited that the study would gain participants within the grades of 8, 9, 10 and 11. Students in grade 12 were deemed less amenable to participate as they were constrained by academic responsibilities. When the study was conducted, students in lower grades were not on the school premises as they were away on an excursion, therefore unable to participate. As such, the participants sampled were students within grade 11 in the 2015-2016 school year. The final school sample included 11 grade 11 students who were interviewed in 2 separate focus groups of 5 and 6 participants, respectively. The two mixed-sex groups included three males and eight females. Each focus group was 90 minutes in length.

In sum, this study involved 20 participants roughly equally divided between high school (n=11) and university (n=9) students.

3.3. Analytical Approach

A grounded theory approach was used as an analytical foundation to understand the data collected. This provided the most effective framework as it "sees social beings [with] experiences, ideas and assumptions [which can] contribute to their understanding of social processes observed" (Baker et al. 1992 in Heath & Cowley, 2004, p.143). While the aim of grounded theory is to "explore basic social processes and to understand the multiplicity of interactions that produces variation in that process," Straussian-grounded theory allows for the usage of both the self and scholarship as initial influencers (Heath & Cowley, 2004, p.142). Past experience, general knowledge and literature, for Strauss, provides space "to simulate theoretical sensitivity and generate hypotheses" (Strauss & Corbin, 1987 in Heath & Cowley, 2004). I began by open coding my data, which consists of comparing "events, actions and interactions…for similarities and differences." These are then conceptually grouped together to form groupings and sub-groupings concerning the topic at hand (Corbin & Strauss, 1990, p.5). I moved on to axial coding which is "defined as data analysis process whereby data is used to highlight the linkages between the

various categories of the grounded theory" (Strauss & Corbin, 1990 in Howard-Payne, 2016, p. 56). Within axial coding, I further developed the categories and subcategories and their relationship by systematically comparing data and by scrutinizing the categories to detect the conditions that arise, the context of it arising and different actions and interactions at play as well as their consequences (Strauss & Corbin, 1990, p.13). Finally, I selectively coded my data to unify categories to provide central themes that offered a thorough explanation of what was found within the data collected (Strauss & Corbin, 1990, p.14). This phase streamlined the categories found as well as allowed the removal of categories that proved to be superficial or insignificant in the overall analysis of the subject matter.

3.4. Ethical considerations

To ensure informed consent, I provided research participants with information about the purpose of the study and informed prospective participants they could withdraw at any time. Consent was verbal. All recordings, transcripts and data were kept secure on a password protected USB to maintain confidentiality for participants. All participants were anonymized through the transcription process to maintain confidentiality. All audio recordings were destroyed after transcription.

Chapter 4. Results

"Don't say anything online that you wouldn't want plastered on a billboard with your face on It." - Erin Bury

4.1. Theme 1: A Multiplicity of Identities

A note on connectivity

Connection is the primary function of social media. Many studies including my own previous work have discussed this function; as such it would be superfluous to dedicate a whole chapter to this result. All participants within this study discussed connectivity as the primary basis of social media use. Social media provided participants the ability to be aware of what other users were doing without the added commitment of a real life interaction. When asked why social media was popular, users had very similar responses. For some participants participating in social media was less of a commitment to a real life interaction.

> George: "It seems like less of a commitment."
>
> Jay: "It's always for a low effort communication. Going and talking to someone is an involved process, less than talking on social media, low impact, and low effort."
>
> Harriet: "I think people want to connect with each other but not spend too much time."

In sum, social media allows for the ability to interact without the need to spend so much time actually *interacting*. Sending a tweet, text or snap suffices until the next "interaction." However, connectivity was key, regardless of how much or how little users were interacting with each other.

> Winston: "We are social creatures. We like knowing what is going on with people we care about. We like when other people are interested in what we are doing."

Participants enjoyed the ability to view other users "lives" as a catch-up. If no interaction was occurring, browsing other users' pages was enough to take the place of real-time user-to-user interaction.

> Frederick: "For me its connection, like the ability to browse people's opinions and anything at my own leisure."

> Nancy: “I just scroll through and see what everyone is up to. I don’t have TV, I’m not really into TV watching, and that’s kind of my TV.”

Due to all these factors, the overall convenience of social media provided a rationalization to continued use. However, it would be too easy to assume users rationalized their use due the prevalence of social media. Participants indicated an awareness of the permanence of the Internet; the dangers touted by mass media and other users’ experiences of these dangers. Participants assumed that risk was invariably associated with continued use. Participants indicated that it was common sense to protect personal identifiable information on the Internet. This was learned from both experience and viewing others (in media or in real life) being exploited or violated while using social media and the Internet.

> Tom: “No one taught me how to be safe on the Internet. I sort of taught myself what to do, like do not share your passwords, don’t share your credit card number, and don’t share your personal information. I just saw people that did that and what happened to them afterwards and learned what not to do.”

> Frederick “Don’t post if you don’t want people to see it… for a while I thought that was common sense.”

The awareness was present, but participants stated that convenience sometimes trumped this awareness.

> Nancy: “…Also people lost track of the fact that once it's out there it's out there, because it's so convenient.”

However, participants understood that whatever good may come out of social media and the Internet, there will invariably be bad associated with it.

> Nancy: “There’s a quote I read somewhere ‘the Internet is the collective conscious of humanity and there are some dark weird terrible corners in there and there some incredible stuff too.’ I don’t know if you can really have one without the other.”

There is a yin-yang quality associated with the use of Internet and social media. For users, risks are a given. There is a sense that justification of use relies on how individual users decide to (1) treat social media and (2) participate within social media. *Why* users use social media is not mutually exclusive to *how* they use it, they are two sides of the same coin. Thus, my findings indicate that what makes social media appealing to users is underscored by their treatment of social media to alleviate their concerns over privacy and security of information.

4.1.1. Fake Accounts, Real Identities

The first key finding was that participants had multiple accounts for different uses. It is not uncommon for an individual user to have multiple accounts. However, participants described their use of multiple accounts as a way to alleviate their concern over how much information is dispersed about them. Users create different accounts with varying levels of privacy because of two factors: (1) how *much* they want to disclose (2) and to *whom* they want to disclose to. Users are controlling their visibility online based on the level of intimacy shared with others in their social network (Papathanassopoulous, 2015, p.1). Participants indicated that their use of multiple accounts isolated them from other users who lacked the intimacy needed for certain types of disclosures. Thus, if participants chose to disclose more personal information, there is a higher probability it was disclosed to the friend groups with higher intimacy. These two factors also indicated that an appealing characteristic of social media was the ability to present a user's self-image to others. Users were aware of the varying degrees of reach per social media platform; therefore they limited their self-disclosures per social media platform. This did not negate the authenticity of their self-presentation; it just varied how far reaching the dissemination of that self-presentation was. This aligns with Calvert's theory of mediated voyeurism; exhibitionism, in any form, serves voyeurism. To limit reach does not negate *viewership*.

4.1.2. Disclosure! Disclosure!

Social media is a public space where disclosures occur. However, as in most situations in real life, individuals tend to limit the amount and types of disclosures with different people (Joinson et al., 2011, p.144). As discussed within the literature, disclosures occur when users are exhibiting part of themselves to an audience satisfying their need to reveal. Findings suggest that these disclosures are nuanced between platforms.

Participants within the current study discussed platforms in terms of the identity displayed and the types of disclosures made. In effect, the platform used dictates what the user discloses. Their disclosures are affected by the level of intimacy held by their followers on each platform. Control over these audiences guided participants' perceptions of privacy online.

> School Group 1
> Jay: "I use Instagram, but I don't have much of a personal account on Instagram. It's kind of like a hobby."
> Jordan: "Don't you have 2?"
> Jay: "I have 4."

Group laughs
Jay: “I take pictures for fun and post them on Instagram.”
Jordan: “Of planes.”
Researcher: “So you like taking pictures?”
Jay: “Yeah. None of my friends follow me on [that] Instagram.”
Jordan: “I follow his selfies.”
Researcher: “So you have specific accounts for specific things?”
Jay: “Yeah.”

This dialogue shows users have different accounts for different uses. In this case, Jay has four separate Instagram accounts. His largest following was his plane-spotting account and his smallest was his selfie account. His plane-spotting Instagram was the least personal of his profiles, as it showed only planes. Therefore, any disclosures made on this particular account were solely of his interest in planes. His selfie account, which was named after himself, was much more personal as it showed his every-day “self” and moreover his face.

Jay: “For me at least, it's about what I don’t want to share and what I want to keep private. I'd rather be open with my friends and how I do that depends on the app.”

Jay's group agreed unanimously with this statement. For these participants, the closer the friendship the more open they were, but as such, the space within which they disclosed needed to have a certain amount of privacy available.

Nancy: “If it’s something a little edgier, I will put it on my Twitter handle because fewer people know about it. I have much tighter privacy settings on Facebook than I do on Twitter.”

Elizabeth: “I never post personal stuff to Twitter.”

Different platforms allowed for different types of disclosures as Nancy and Elizabeth’s statements show. Twitter was viewed as having a much more public character as there was a higher likelihood of unknown followers and the ability to re-tweet and follow unknown users. Thus, the disclosures they made were less personal. Nancy, for example, divulged instances on Twitter where she needed to ‘rage.’ However, these disclosures were not exceedingly personal in her view, thus were not viewed as requiring stricter privacy with regards to (a) what she chose to disclose and (b) whom she disclosed it to. On the other hand, Snapchat was viewed as one of the more private platforms.

Bethany: “I think that’s what makes Snapchat, what makes it different from a personal level, like Instagram again, it's like filtered to the best, and Snapchat is like look at me being disgusting.”

> Myrtle: “On Instagram it's not my mum following me or anything. It's not like I post anything inappropriate, but other people I've noticed tend to post more inappropriate things to Instagram or other forms than to Facebook. Because you have your grandma following you or you can't say a swear word on Facebook, but you can on Instagram.”

Snapchat allowed users to self-present to a restricted follower group. Since the user was posting to or messaging users both known to them and in their real life social circle, the ability to exhibit their truer self was valued more. What these findings suggest is that ‘space’ matters. As stated previously, Goffman understands self-presentation as “an attempt to control or guide the impression that others might make of a person by using verbal and nonverbal signals” (Kramer & Haferkamp, 2011, p.128). Within social media, there is stage-work occurring constantly by users, however, ‘stages’ on social media are not limited to one front-stage and one backstage. Users can have multiple ‘stages’ and disclose more of their ‘backstage’ based on both the platform and audience they are disclose to. Stages could be paralleled to different platforms used and the different claims made within each platform. Each platform may have claims that are congruent to each other, but based on the varying levels of intimacy between audiences, these may have claims or impressions made that are not congruent or provided to audiences in other platforms with weaker ties. It could be considered similar to the roles users play in real life, claims made within each ‘staged-role’ can be congruent to other claims, but may have differing claims based on the audience being impressed upon. For example, the staged role of the individual as an employee is different to that of them within their family unit. However, there is congruency between the claims made in each role. The differences include claims or impressions that are needed within a job that will not be needed within a family unit.

Snapchat is a platform where there is a higher level of perceived privacy; users control completely who can view their posts and whom they can interact with. This space is similar to the backstage, as disclosures are more intimate. Front-stage platforms are Instagram or Facebook, where impression management guides users posting behavior. The audience is larger and much less intimate, thus the disclosures made are less personal. Self-disclosure is defined as the “act of revealing private information to others and is thus closely related to privacy” (p.128). This form of disclosure places “higher priority on the quantity and the kind of personal information provided, while self-presentation focuses on controlling the impressions that other persons form based on the given information” (p.129). These two work together on social media. Moreover, with users being concerned over where and to whom their information is dispersed to, the ability to control this dispersal is valued.

4.1.3. Audience Matters

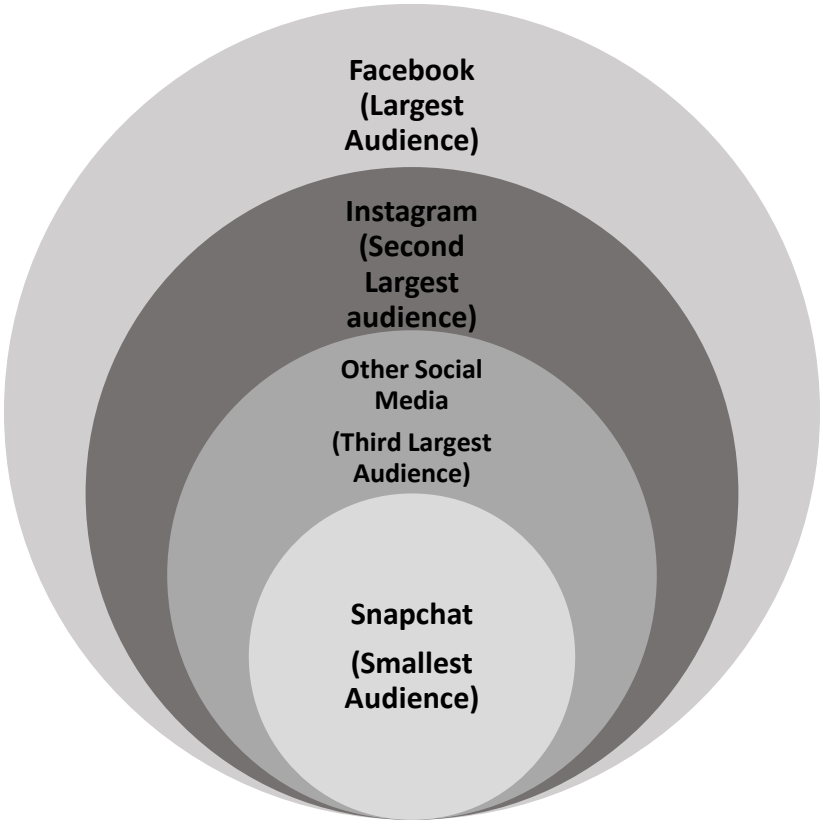


Figure 1: Audience Overlap

The audience of a user makes a difference in what the user chooses to disclose. As stated above, users are still managing their identity within all platforms, however the disclosure of intimate details will more likely be disclosed to those with higher levels of intimacy. Users are thus constantly managing levels of intimacy shared with other users and their distance to other users. The followers a user has on Facebook may not include followers they have on either Instagram or Snapchat. Additionally, users can transition users from either platform or on to a different account on the same platform, when higher levels of intimacy are achieved. The above figure (Figure 1) is an illustration of the audience overlap. For the average user, Facebook has the larger follower list with a larger preponderance for weaker ties. Followers a user has on Facebook may not be someone a user chooses to have on Instagram due to said user's usage behavior or level of intimacy associated with the platform; as the level of intimacy heightens, the smaller the audience and preponderance of weaker ties within the platform. Snapchat is considered the platform with the smallest audience, as it is more likely to have more intimate ties. There is overlap between the audiences due to some followers being within all social media platforms used.

With regards to an audience's relation to privacy, the amount of views a post receives, (i.e. how far reaching the dispersal of information), relies on which audience a user decides to disclose to and whether there is overlap between them.

> Harriet: "You wouldn't say or post pictures on Instagram, on Facebook. The people you follow on Instagram are also different from the people you would friend on Facebook. I have all my family on Facebook [and] on Instagram I didn't have any of my family, just closer friends or people I interact with more. I think there's a different platform for that, it's a different kind of interaction…"

For these participants, if the interaction a user has with another user on Facebook is dissimilar to those they have on Instagram, they will not willingly post anything that goes against that interaction. The different "selves" a user has must remain authentic to the overall "self" being projecting on all social media platforms. The audience on each platform must confirm the self-presented as authentic for the whole presentation to work. To put this in real life terms: you would not tell your parents all the activities you do with your friends and you would not disclose everything that happens in your home to your friends; however, each audience maintains you are the same individual. You afford yourself a level of privacy for each interaction.

> Harriet: "On Snapchat, I have really close friends no one else."

> Elizabeth: "I resorted to Instagram and Snapchat, which is very secluded to a number of people. I feel safer now than before."

> George: "…More and people added me [on Facebook]. I didn't want to share to all those people. Sometimes I'll post on Google Plus because I have less people on there."

As shown above, each platform has its defined audiences, by in large Snapchat was shown to be exclusively for more intimate categories of friends or followers. The platform allows the user to choose whether they would prefer a private profile, but additionally any photos or videos shared are deleted once viewed. The receiver of the snap cannot save them; the receivers can screenshot the post, but the sender will receive a notification of the action giving them the ability to control how the receiver uses the post. However, like Bethany states, Snapchat is where you post pictures of a more private self. Instagram can be included in this category. Participants indicated audiences on Instagram were much smaller than on Facebook, due to different disclosures. Moreover, wherever an individual user has a smaller audience or presence, the ease of disclosure is higher. Participants do not want to share to everyone in their social circle. My previous work indicated users were more likely to post a "cleaner" version of themselves on

Facebook than on other social media sites due to the audience they had, (i.e. parents etc.). The same can be said with this participant group.

> Harriet “I think a big reason why I deleted my Instagram or tried to limit my social media, sometimes you feel like you’re so out there with everyone. You’re just like, I have these people on Instagram that I’ve never spoken to, and I don’t want that kind of relationship with those people.”

> Courtney: “The level that I know the people who view my content dictates what I post. I would be very apprehensive to post a YouTube video or a link to a YouTube video on Facebook because I personally know everyone on my friends list. Not everyone knows that I have a YouTube, but on my Instagram I wouldn’t hesitate to post a photo saying hey check out my YouTube video, link is in the bio.”

Within this discussion of exclusivity of audiences, participants clarified their meaning. For the sender disclosing information on some platforms felt as though the amount of *reach*, (i.e. dispersal of information), was too large. Courtney was an atypical participant in this case as she is a YouTuber, however she maintains the position that audience dictates disclosure. Her Instagram was viewed in a public sense, she was not as intimately linked to all her followers, as she was her Facebook; more likely users who followed her YouTube channel followed her Instagram. Her Facebook, contrastingly had individuals who did not know about her YouTube channel and she maintained that ignorance. Thus, her disclosures on her Instagram tied to her more public image as a YouTuber, whereas her Facebook was tied to her real life self.

> School Group 1
> Jay: “I have my planes, which is a world of opportunities and then I have my others. Like if someone wanted to follow my jayselfies, well no, I wouldn’t let them. They'll probably be weirded out by me…just ...me.”

> Bethany: “I think there are levels. Facebook is like, you've met them once and it’s okay to add them. Instagram is like you talk to them regularly, and Snapchat, I don’t have it, but its close friends.”

> Jay: “Snapchat you pretty much have to meet the person... you can't just send them your username over messenger that would be weird...like you generally have to know someone well enough to be like...like you couldn’t Snapchat stalk anyone... like if you look up your friends Snapchat you can’t...”

Participants viewed different platforms in much the same way you would view different relationships. Some individuals are acquaintances; they are allotted to a specific Social Media platform of the user’s choosing. The closer you are to an individual dictates which Social Media platform another user was a part of. This was exemplified by Elizabeth’s discussion of an incident with a former workmate.

> Elizabeth: “I would never accept anyone from my workplace (on Snapchat) because it’s important to keep that separate.”

For Elizabeth, a workmate was not an individual who, to her, warranted an add or follow to Snapchat. Snapchat was a platform used primarily for close friends; her circle was small and the disclosures made on this platform were indicative of her everyday life. Her other platforms were not as personal. An incident occurred wherein which she was somewhat pressured into adding her former workmate on Snapchat. This workmate and Elizabeth were not close; they saw each other once a week and in Elizabeth’s view were not “on that level yet” to be considered a follower on Snapchat.

> Elizabeth: “But she kept pushing, so I said, just so you know if you come back, this is very personal and it was kind of a warning. I didn’t feel like she was on that level.”

Although, Elizabeth did agree to add the workmate, she was not happy. Snapchat was a personal space and separating individuals and audiences was important, in agreement with other users. Furthermore, the ability of this user to see intimate posts made Elizabeth hesitant.

> Elizabeth: “You can scroll through Facebook and I probably don’t see if you saw my post, like you probably have more people on Facebook than Snapchat. I’m pretty sure she won’t see my posts [on Facebook] and I don’t care on Facebook. Snapchat she saw my post, she saw my post.”

There’s a modicum of anonymity available on platforms with larger audiences. In addition to limited disclosure, the amount of posts from other users available to see is exponentially larger than those platforms with smaller audiences. Any other user could hypothetically ‘miss’ a user’s disclosure without noticing. However, on platforms with smaller audiences, these disclosures are harder to miss. If there are users within a platform that the sender is not close to, this limits their ability to self-disclose, as they must account for the outlier(s) within this audience group. This detracts from the appeal the platform has to self-disclose. If a user is unable to disclose based on outliers or unintentional audience overlap, the utility of the platform is decreased.

4.2. Theme 2: What is in a Name?

“On Twitter we get excited if someone follows us. In real life we get really scared and run away”

- Unknown

Participants discussed anonymity in two distinct ways. Anonymity is "defined as a type of privacy that occurs when it is possible to move in public without being recognized or without being the subject of attention" (Taddicken & Jers, 2011, p.145). On Social Media, being anonymous is relatively easy. A user can be anonymous through their own handle/username or just by "lurking"; "in addition in many social web applications it can be possible to become a member of a community without providing one's real name" (Taddicken & Jers, 2011, p.147). Some SNSs have strict real name polices, like Facebook, which means "disclosure is usually connected to a non-anonymous individual who relies only on the privacy settings of the site (and the trustworthiness of the organization behind the site) to protect their privacy" (Joinson et al., 2011, p.34). However, an individual can maintain anonymity on a site like Facebook regardless of a real name attachment. Lurking on Facebook or other Social Media is easy if the Lurker does not notify others of their behavior. Moreover, if individuals have more relaxed privacy settings this lurking behavior is much easier. Furthermore, the real name policies are not fool proof; creating a fake name on Social Media is relatively easy. Facebook has "algorithms to attempt to distinguish "real" from "fake" users (Breyer & Zuckerberg, 2005 *in* Joinson et al., 2011, p.34). These algorithms are not foolproof. There have been instances where individuals have created fake accounts on Facebook for their own endeavors (See MTV "Catfish: The Show", incidents are recent to this year).

Anonymity on social media can be appealing to users. The ability to look at what is being disclosed by other users is appealing for many reasons. My previous study indicated that the appeal was due to the gratifications received by spectatorship and social comparison. However, my findings were too superficial to be able to extrapolate on surveillance issues. With the current study's participants however, an added layer within spectatorship was discussed. Anonymity gave a sense of security for users. Essentially, what *harm* could a user do, if they were anonymous to the other user? If an individual user is anonymous, other users are as well. You as a user cannot limit the ability of others to be anonymous. Therefore, the names users gave within each platform were important to maintaining their anonymity. The name a user attaches to a platform is as important as the content disclosed; content disclosed relies on username. There is a difference between content attached to a real name and content attached to a created username, which links to the degree of exposure received on each platform. The appeal of lurking is not superseded by how users treat each social media platform. It is acceptable for all users to lurk on social media. However, the security received within this anonymity is not automatic. Noted within this discussion was the presumption by participants that anonymity created by differing usernames made it harder for service providers to data-mine because of a lack of identifiable information attached to

real life individuals, (i.e. fake emails). However, the provider can still data-mine content regardless of a real life attachment. The provider will still have access to information about the user and user preferences that can still be sold to third parties. A name does not need to be attached for the service provider to have enough information to target users.

4.2.1. To be Anonymous

Anonymity came in many different forms. For some participants the ability for other users to know when you were online was a negative.

> Myrtle: "On Snapchat people don't know when you're on, but on Facebook there's that green dot that says that you're there. I don't like that because then my grandma would message and I'm like OMG. People know when you're on…so I don't go on."

Having the ability to be on social media without having others know allowed the participant user to roam online freely. By using accounts or interfaces that maintained their anonymity, the user can look, lurk or creep without any added pressure of other users tracking their movements. For some this may be for entertainment purposes, so not having an account to link a user's activity is ideal, and for others, in addition to entertainment, it allows the ability to 'keep up' without any interaction.

> Winston: "Reddit, I do use it but mostly for lurking I don't have an account to post…I'm purely a guest."

> Jack: "(On Facebook creeping) it's more comfortable form because it's anonymous. You can go and look without them knowing, like you can know what's going on in their life without having to ask them."

Moreover, like in my previous study, participants felt comfortable as the anonymous user. Going through posts of either their interests or individuals they followed without having to interact was preferred in some cases. As stated on my note on connectivity (chapter 4: 4.1), social media is much less of a commitment to actual interaction. Anonymity allows users to decrease the interaction even more. Like Frederick and Nancy stated, it is similar to a newspaper or TV, they, as the user, are observers of other users' everyday life and vice versa.

> Tom: "I'm a big fan of anonymity in general. Only anonymous can people truly be themselves, on anonymous forums and message boards. They allow for every single type of culture because users have an anonymous identity, they can't make a name for themselves. People [can] express their genuine opinions, they aren't afraid of judgment and you can see people are usually worse than they claim to be."

> Harriet: (on anonymous liking and sharing) "I like it, I always follow a few girls who are into fitness. Like when they have the progress picture. They are also very personal, what she

studies what she does. You get to know them a little bit more, and then you comment… [I also follow] People that are for nature. I do not get to know them because they are not vulnerable. I become a fan of what they do, like I want to be like that person or learn what they are doing, or have their skills. I think it really depends on who you're interacting with. If it's on Facebook I will be a little creeped out."

Frederick: "I'm used to that anonymous aspect of the internet. You look at the message boards like 4chan, no one has a name, and everyone's anonymous. That's where that anonymous collective comes from. So if you post and a bunch of people like it, you know who likes it but you don't who they are that's something I grew up with."

Regardless of form, anonymity also allowed participants to express themselves. The ability to look at individuals outside one's own social circle, similar to my previous study on creeping behavior, allowed participants the option to view and express other interests not shown to their overall audience. Interaction with other users, while being an anonymous user, was not seen as "creepy" unless it involved a social media platform like Facebook, which requires real names or a platform with restrictions on who can interact with a user i.e. Snapchat.

School Group 1

Jay: "Like in my groups (flight simulator), I don't know many of the people on there. And you like posts; pretty much everyone is anonymous liker… Generally, they don't get many likes, it's just kind of supporting, but it's a small group. You should keep doing that job. In that case you're not one of 2million likes, it's like 30…like you're making a difference. It's encouragement."

School Group 2

Patrick: "If you're the official poster, you've already agreed to this stuff that's going to happen to you."

Bethany: "I think it's cool. You can still show you appreciate that content but you can link yourself to it without showing yourself. The Internet is full of risks and for someone who's scared of those risks then you can still have a level of privacy."

Patrick: "You definitely feel more comfortable with that added security."

Participants also recognized the difference between users who specifically post content for monetary gain (i.e. YouTuber and the average user). However, this did not change the way they interacted with either. As a verified user or average user, being the anonymous liker for each party was a show of support. Security was maintained by anonymity and an acknowledgment was made of the users' interest.

George: "YouTube, that's real anonymous liking. I think I used YouTube more than Facebook. I, actually, before there used to be friends on YouTube, and they're [were] just people who are subscribed, and [you] know who they are. I used to like every video I wanted but now I am careful because what are they going to think about what I like? Liking comments is better because they're not going to see who likes the comments… (On use behavior) at least for liking and favoriting and subscribing, I used to be more true to myself."

However, user behavior was affected by real name policies. For some participants with the arrival of real-name attachments to previously anonymous -platforms, users did not feel able to express as much of themselves as they had done before while anonymous. Although they continued to use social media, they were conscious of what they liked, shared or subscribed to. A key example is YouTube's merge with Google.

> Tom: "You have to realize that you have a real you, and that real you can have a phone number and buy real stuff online. And then you have another identity, for example forums, where you don't need to represent yourself fully. You don't need to put your real name and your email, you can have a completely separate identity."

> Elizabeth: "If you're anonymous, the things you share or post aren't really you, as in a person. I think safety goes side by side with anonymity. But, in terms [of] what people post and their anonymity; it can be connected to who you truly are as person. But with social media, the fact that you attach what you post to who are as a person, what you post says a lot about to you. It's attached to your name, people can judge and comment and it's not ideal for someone to post something provocative using their own name, like they don't want their friends to see it. So the fact that it's anonymous. It's not them as a person, I get a good feeling about posting, but I can post it because it's not really "me" who is posting it, it gives a type of excitement."

Furthermore, due to the anonymity gained online, users could create separate selves. The "self" associated to individual users' real life self is more often attached to social media geared to sharing. Thus, the ability for a user to be separated from this and still be themselves was appealing. Moreover, due to this anonymity, concern over privacy of information was not as much of an issue in comparison to the social media profiles where there was a real name attached or affiliated with the profile (i.e. real life activities etc.).

> Nancy: "[on Twitter] I also use a handle so I don't have my real name on there. But I don't have any as far I can tell, many privacy settings on there. But Facebook I've locked down tight. You pretty much have to go on someone else's profile to find me on Facebook."

> Tom: "I have a pseudonym for gaming sites. For VK (Russian social media site) I use my real name, for Facebook as well."

> Jack: "I don't have my last name on Facebook, so even if they find out, it's not my last name that's on my official documents."

Self-presentation is a key appeal in continued use regardless of whether it is done under the guise of another 'self'. Moreover, if there are areas of life where an individual would not want to present to a known-audience, this allows them the ability to do so without one.

> Nancy: "Twitter, it's under a different name, under a different handle. There's actually very few people on my twitter list that I actually know. I'm not going to post anything flamey or

incendiary. If I'm having a bad day or there's some piece of news that's upsetting me, I'll just go and dump that. It's public, but is also not attached to me personally that much. Whereas my Facebook is intensely personal but it's really, really private."

George: "I'm thinking definitely the one [forum] I would even give away personal information. [That] one was about always-online games and I was saying that when I go home, I don't have Internet like back at my dad's place. I was talking about personal stuff but...I guess [it] made it, would be easier because I could say stuff…"

As expressed by George and Nancy, having a different name or handle made it easier to express certain issues. This anonymity works as a more concrete form of security.

Nancy: "I've had friends who used Facebook to talk about and get support for abusive relationships they were going through. And for them, if the person they were talking about might find them or discover what they were saying, and that's when the whole Facebook real name thing became an issue, because they were posting under handles that they felt safe under. That they knew people they were keeping away from couldn't find them. And all it takes is one person to report to Facebook and make Facebook shut them down and make them prove their identity, So that was huge for them."

Not having a name attached to a users' expression, especially vulnerable ones, was important for some users online. These spaces can be communities for a large array of groups and anonymity for some is paramount in maintaining their safety in real life, as shown by Nancy.

School Group 2

Courtney: "On social media, if it's like friends of friends or whatever that's fine. Like my Instagram is public and that's my face."

Evelyn: "But if you're opening an account on a different platform with strangers, like that's a different situation so you don't want that."

Bethany: "I don't mind strangers following my Instagram. "

Jean: "You don't really talk to them. They're just liking your pictures."

Bethany: "Exactly. They don't know anything about me besides what I look like."

Courtney: "Because I have subscribers on my YouTube and they follow me on Instagram I specifically make sure to have stuff taken out, like they don't know my last name, my age, they know that I live in Canada. I make sure that, like when my friends tag me in photos, they can't see those photos. It's important for me to make sure at least my location is kept confidential."

Jean: "Because you never know who could be looking at your page?"

Courtney: "Right."

Evelyn: "Like on Facebook you can't?"

Bethany: "No, you don't know."

Courtney: "But my Facebook is super private, like really private."

Conscious decision-making was involved in the self-presentations viewed by other users. What users considered personal identifiable information – like an explicit statement of an

individual's location – was not indicated on these platforms for added safety from other anonymous users.

> School Group 2
> Patrick: "With discord, you can join servers with a bunch of people you don't know and talk to them and a bunch of weird things can happen."
> Bethany: "I like chat-rooms for that reason."
> Researcher: "You go on chat-rooms?"
> Evelyn: "Oh no!"
> Bethany: "I do, I go on when I'm like super bored and I can't focus on work."
> Jean: "You can talk about random people on that."
> Evelyn: "But what are you? They're predators!"
> Jean: "You just talk! It's hello..."
> Bethany: "Specialized chat-rooms. Like guys let's talk about this."
> Jean: "Yeah, you can put your interests, like fruits."
> Researcher: "So, it's tailored to what you want to discuss?"
> Bethany: "Yeah. If you want to put it in, and that's fun to be like, oh look, it's a chat-room where all of them like corgis, so yes! Let's talk about corgis for hours."
> Patrick: "Same with discord. It's kind of what you want to talk about who's interested it. It's kind like how people make friends over the Internet compared to real life."
> Researcher: "Do you feel more comfortable in chat-room?"
> Patrick: "In a way I do, I'm behind a screen."
> Jean: "They don't know me."
> Patrick: "They don't know who you are, so you can talk about a lot of things."
> Evelyn: "Is it anonymous?"
> Bethany: "Yeah, it's anonymous."
> Patrick: "It's anonymous as well."
> Evelyn: "I think I would feel nervous, but then I would feel more comfortable."
> Bethany: "Especially if it's not your first time being in that chat-room, and you see someone you may have talked to like, hey we had this awesome story thing."
> Patrick: "In a way, sometimes I don't, I don't know what they'll do. Like, if I'm telling confidential information, I'm kind of afraid they'll leak that information to someone else."

Interestingly, some participants viewed anonymous behaviors as unsafe while others viewed this anonymity as a security measure. Both gaming sites and chat-rooms allow the use of handles rather than a real name. For some, these SNSs were the epitome of dangerous, while others viewed them as more of an escape. Individual users can filter out the people they would like to speak to and the anonymity of the space provides a sense of security and freedom of expression. However, participants did concede that there is a risk in revealing information that may undermine their anonymity. Information could be linked and leaked to others without their knowledge or permission.

> School Group 2
> Researcher: "Why do you feel uncomfortable?"
> Evelyn: "I don't use them. I don't know I guess if it's anonymous, then I guess it would be okay. You don't know who you're talking to. I feel comfortable talking to my friends about things because I know who they are, and I know they won't talk about me. If I'm talking to someone online, I don't know who they are. I don't know what gender they are. It raises a few red flags for me."

Jean: “But wouldn’t you talk to a friend’s friend, you don’t know them, but just because a friend knows [them]. You would still talk to them.”
Evelyn: “Possibly, but she’s your friend. I don’t know, I’ve heard all these stories about people getting targeted through chat-rooms.”
Researcher: “Like cat fishing.”
Courtney: “Does that stuff actually work?”
Researcher: Cat-fishing is when an individual misrepresents whom they are as a person, for example creating a fake profile of a model and acting as if they were this person even though they are not. There is a show on MTV with the same name that is based on figuring out whether or not individuals on the show are being cat-fished by someone they are talking to and/or dating online.
Evelyn: “Especially now, with technology. How it’s advanced.”
Jean: “You can make fake profiles.”
Evelyn: “Yeah, and fake numbers to talk to someone and through messages.”
Patrick: “Yeah, that kind of scares me.”
Bethany: “For me, that’s where I find myself naturally drawing the line, like I feel comfortable in chat-rooms, but I know they're not getting any personal information from me. We can just have a conversation here.”

Other participants were more cautious of anonymity online. For Evelyn, these risks were found through media and possibly other users experiences of dangers faced by both adolescents and adults in chat-rooms; I gave the example of cat-fishing (a user passing themselves off as a completely different person) for context. Once this example was provided the other users were quick to agree that the risks associated with chat-rooms and other forms of anonymous forums were not unwarranted. However, participants did indicate that as a user, you must be conscious of what you disclose and whom you disclose to. Users are calculating the risks associated with being able to maintain their anonymity.

4.2.2. Or not to be Anonymous

For participants, having their name on social media was an exceedingly different experience to their more anonymous profiles. There is a responsibility attached to that name and in a sense a user reaps what they ‘sow’ when putting themselves in the public eye.

Elizabeth: “I follow pages that allow for that all, for the public to follow them. Like vine or 9gag or NBA, I like that. I would never let someone do that to my page… From a personal perspective, the way I like it, I don’t have the intent to do anything with that information. As opposed to personal pages trying to get monetary gains…it’s your prerogative with what you do with your page, whether it’s public or private. And if someone were to take that information, I’m sorry you put it out there. You have to have the mindset that some people might use it for malicious reasons…”

For most participants, it is easy to be an anonymous consumer of content. However, the individual posting on a public platform must recognize the risks attached to that publicity, and participants were cognizant of this. The participants in the study with public pages specifically

separated their private pages from their public ones. Elizabeth gave an example of a friend who had found her image being used on an Instagram page named Vancouver-Babes. The page, as indicated by its name, featured women thought by the moderator to be 'babes'. Elizabeth's friend, once seeing the unauthorized use of her image, was upset and asked for her image to be removed from the page. Elizabeth, however, indicated she was unsympathetic towards the situation:

> Elizabeth: "You're the one with the public page. You put that out there, and then technically you can't do anything about it."

If an individual chooses to be public and have their name attached to that public profile, an incident similar to one shown above occurring would be to some, no one's fault but their own, as they made that information available. However, the individual using the unauthorized information or images must be held responsible for taking the information without consent.

> Frederick: "Sometimes, I'll look at a newspaper article but it's linked to a Facebook. I guess there's a responsibility attached to what you say, because now your name's attached to that comment or what you post and say."

Moreover, with regards to having a real name attached to a profile, whether public or private, a user must acknowledge the responsibility attached to what they disclose online. Furthermore, a user's audience is increased if they are attaching their name to viral content. Linking a user's profile to other users exponentially increases the amount of individuals viewing the post.

> Harriet: "If it's something personal on Facebook. Like, I posted a song and tagged my friends but their friends', people I don't know, have liked it. It's just a song; I don't care if they like it. But if I post a picture and a bunch of her friends or family comment on it, that's kind of weird and Ill delete it. In real life I knew your friend or knew of her and I said yeah "I know her" and that person went up [to] that girl and went she said she knows you and she goes "no she doesn't", that's the whole interaction. Like you know of me but you don't actually know me."

The content shared and platform which it is shared to, matters. Similar to my pilot study on creeping behavior, for an unknown user to comment or like content, regardless of whether that user was known to a user within an individual's social network, the behavior was viewed negatively. If there is no definitive link in real life other than a link on a friend list, then there is no reason for the behavior to occur. Essentially, "stay behind the screen." Even though anonymous creeping is a normalized behavior online, once an individual user discovers another's 'real name,' the amount of information available to them is extensive.

> Frederick: "We all do it. Like once you find out that persons true name online, like a nerdy lord of the rings reference there but once you know someone's true name you know

> everything about them. And it's so true in our online day and age. It used to be you can hide behind a made up username."

The ability to hide behind a username due to real name policies is somewhat limited. If other platforms attached to a profile forgo this policy, other users can discover the real name profile associated with the anonymous one.

> Harriet: "When I don't have my profile picture up as me, I had my profile picture as my dog, no one harassed me or if they did it was people who had gotten my name from somewhere."

Furthermore, real life incidents could occur where a users' real name is given without their consent. This happened to Harriet while she was a server. A man from New Zealand was provided her name by her manager and proceeded to message her online. She did not know who the man was and in actuality had only served him once prior to his messaging her. For most participants, engagement with their social media by individuals they had met in real life was based on permissions. For Harriet, she did not permit many individuals to know her social media. This was a breach for her. Moreover, Harriet was a prime example of harassment attached with knowing a user's true name. Most individuals in the study had experienced some form of cyber harassment, which included inappropriate conversations, stalking, or harassing messages. For Harriet one way of limiting this behavior was not associating her own face to her profile, which proved to be helpful.

> Elizabeth: "I don't feel safe when to comes to that (anonymous liking/sharing) and that's why I private my page. It's so easy to find people now on Instagram and Facebook. Let's say some one has a unique last name, it's easy to find them. Someone asked me to find someone on Instagram and all I had to do was type in their name…My friend and her friend couldn't find it, and I just typed in his same and they said they did that too. It's easy for people to find or share your stuff, like even if it's a funny thing or a two year old. I would feel unsafe for my child just because of all these things that can be done with that content."

Elizabeth reiterated Fredrick's statement with Instagram. On Instagram most individual users have a handle/username. However, Elizabeth noted that you could still find users on the platform regardless of a different username. This could be due to the multiple of ways Instagram associates pages to names, hashtags or affiliated pages. Social media was viewed as too insecure to guarantee the safety of their real name (associated with real-name policy platforms) from unknown users.

4.3. Theme 3: Privacy Devalued or Re-valued?

"Social Media gives one a family to share one's life with" – Sonu Nigam

As technology continues to advance, users are becoming more aware of the capabilities of service providers to use and store data. We live in an "information society capable of gathering, storing, and disseminating increasing amounts of data about individuals" (Shatz Byford 1996, p.1 *in* Joinson et al., 2011, p.33-34). For most participants in the current study, they had experienced some form of cyber security issue, like cyber harassment, cyber stalking and cyber hacking by others. Moreover, some users viewed platform security changes as part of the cyber security issue. Due to these experiences, how they viewed safety online relied on the amount of privacy available to them on a platform. My findings suggest that users want more control over their information from the service provider not just from user-to-user interaction.

The previous findings indicated that user's treatment of social media was ruled based on to whom and how far reaching the information they disclosed was per platform. Users viewed anonymity as part and parcel to social media, thus they used it to their advantage. However, their ability to privatize their content and the use of their personal data by service providers and third parties was limited. As such, users were concerned with how to change service provider settings and capabilities, all with the understanding that service-providers were businesses. Nonetheless, what became glaring was that users' concern over the limited privacy with service providers was somewhat mitigated *by* their treatment of the platform used.

4.3.1. Awareness & Security

Participants viewed social media risks as a given condition to using the platforms. However, participants viewed the strategies used to mitigate their limits in privacy as enough to alleviate the overall risks to social media use. For most participants, there was awareness that their information was being "skimmed".

> Nancy: "…Data skimming and data drilling, there's not a lot we can do about if we want to keep using face book. Even if you do have privacy settings on, they are skimming everything. Those emoticons they have that say 'I like this', 'I'm angry'; they're skimming all that. It's cute and fun but they're looking at the demographics of that, who's responding and in what way to the different posts and news articles."

Since social media platforms do not share “identifiable information,” it is much more agreeable to allow for this type of data skimming. Nancy stipulated that she was not fond of this specifically when it came to ad preferences. To mitigate some of the information being mined from her platform, on Facebook she chose to change her age to 74 rather than her actual 43 (at the time of the interview). She noticed even with an ad-block service in place she would still receive ads, messages and trending topics, which would be of interest to a 40-something female. These adverts had some effect on her self-esteem, and as such were not wanted, so she changed her age. Currently, the only ads she receives are “meet silver singles” ads or pain medication and the like.

Some participants showed more knowledge than others on how far-reaching the data skimming/mining was.

> Harriet: “Sometimes it feels weird. When I Google something like going to Ireland and then I go on Facebook and automatically there’s something about that. Like I just did this a few hours ago, how in the world did they know? It’s kind of weird in that aspect.”

> Nancy: “In terms of data security, that’s one of the reasons I'm careful about what I post. Because even if it’s private they can scrape anything. They're doing key word searches, they know what people post, how frequently people post after certain events, and it’s massive. It’s just massive the data their collecting.”

There were limits to user cautiousness; the service provider in any platform can see all the information. Furthermore, quite a few of these services are owned by one company. As stated in the introduction, Facebook owns Instagram, Google owns YouTube; thus the information a user shares can be part of one database.

> Tom: “They have to make a profit somehow, and of course they will be advertising and marketing. That’s sort of the tradeoff between convenience and privacy. You can have absolute privacy by going off the grid not using a phone, but that's not realistic.”

> Harriet: “I don't like that. It’s like you’re using people’s content without them approving it. But I mean we signed up for that when we signed up for Facebook. Yeah, I know it’s going to happen, even if I don't like it, it’s a given.”

Profit is the bottom line; otherwise these platforms would not exist as fee-free services. There was an understanding that the information participants provided would be used for ad services and the like. However, being “off-grid” (without any form of Internet use or social media) was not realistic. For most participants, much of their lives were dependent on Internet use (i.e. email, online banking, school work). Moreover, much of their daily interactions with others used the Internet or social media; being “off-grid” would mean being disconnected from those social

networks. “Off-grid” was also viewed in a somewhat negative light, as not having the latest technology, so flip phones and Nokia’s came to mind. In a sense it was considered going back to the dark ages, also known as the 90s and the early 2000s. Some participants indicated that they would remove themselves from using social media at different times (i.e. exams); and had deleted some platforms due to misuse or issues in security; however, to ask participants to completely give up social media was difficult.

> Winston: “… It’s true that my preferences are tracked, that’s how they get their money. I'm aware of that, but at the same time I don't put a lot of details about my interests or anything. So anything present is based on my usage habits. So any information that is not based on what I’ve freely given or what I've written out, in a way I’m okay with. It’s sort of a tacit understanding that if I’m using it, and then I’ll have things suggested. But it’s my prerogative as to whether or not I click on it. So I don’t find it much of an imposition. It’s not like you're giving up my home address to send additional mail to. I don’t feel unsafe in that way but perhaps I’m just naïve. Part of the reason is because I don't share that many details of my life so anything I put out are things I would say in real life and that I don't feel concerned about being associated with me. That’s why I’m not concerned.”

Furthermore, most participants agreed with Winston (above). They controlled their information and further, if ad choices were viewed on their social media, they chose not to click on the adverts. However, adverts were based on usage behavior for the entire Internet as Harriet noticed. Thus, the extent of how far-reaching social media data skimming was considerable. However, for most participants, there was less concern due to the restrictions they placed on how they used social media.

> Tom: “No. I don't post anything exceedingly personal. My phone number isn’t on there. My email is on there, but it’s not that sensitive. Sure message me what’s going to happen? I don't feel insecure because no one cares about my identity. Like sometimes people will go on and take peoples photos, or whatever to emulate their page or to defame them to post offensive stuff, that has never happened to me.”

For most users, since ‘personal information’ was not provided online, users were not aware of which information Social Media platforms used.

> Nancy: “It’s not that I’m particularly hiding anything from anyone or anything, but once you give up privacy you can’t get it back. That’s really what it comes down for me.”

Users felt that maintaining privacy was their “choice”. What they considered private remained outside the online world.

> School Group 2
> Patrick: “I think privacy dictates what you post, because how you feel about it and how many people you want to show.”

Bethany: “If someone tags me in a photo where someone can see, I don’t mind that much. If it’s something that I don’t mind people to see I’m fine with that but if it’s something that I don’t want people to see (friends or family), I would not be okay with being tagged.”

Patrick: “If you're putting yourself on Facebook and Insta, you're committing to maybe having that happen to you. And the only way to circumvent that is to not have an account. But you have to accept that this might happen to you at some point to use it.”

Jean: “Like on Facebook, how do people find you if they don’t know your name?”

Patrick: “Friends of friends.”

Bethany: “You can search up someone who likes this school’s Facebook page.”

Patrick: “If someone has like 3000 friends or something.”

Researcher: *Gives example Facebook/Instagram search bar*

Patrick: “That’s why you're committed to the risk.”

Jean: “For me, I'm not hiding anything I’m not posting anything bad, so I don’t see how it has to be so private.”

Jean: “My Facebook is not really private. I don’t really make things private. I don’t know what it’s going to do. Like my profile you can see my photos and some information but it’s not like I put my address. In case someone needs to find me, you have my phone number right there.”

Evelyn: “You have your phone number on Facebook unprivated?”

Jean: “Yeah.”

Evelyn: “Why would you do that?”

Patrick: “My phone number isn’t there.”

Jean: “It’s not like my address is there.”

Courtney: “But still they can find you on through your phone number.”

Bethany: “I don’t have my phone number or address on Facebook. But I don’t post a lot on Facebook. I'll post in private groups, like Instagram was private until a month ago, at which point I wanted to take part in a contest so I publicized.”

Jean: “My Instagram is private though.”

There was a lack of concern in some senses to *data* but more concern over what was considered *personal identifiable information* like a phone number. For one participant, Jean, it was not uncommon for her to have her phone number on social media. She did not view this as identifiable information. Her address however was identifiable information. The sentiment being, if there is nothing to hide, there should be no concern. They viewed it as an oxymoron: a user was using a sharing platform but was not sharing; what would be the use?

Researcher: “Did you feel that your information was insecure?”

Jack: “Yes, my contact information.”

Researcher: “Were you concerned?”

Jack: “Have I ever been concerned? No, not really.”

Researcher: “Why?”

Jack: “I don't really post. I post generic stuff. And I just haven't been worried. I guess anyone could save or screenshot my pics, but I feel like I’m so uninteresting that why would anyone want to do that?”

Researcher: “Are your settings good enough?”

Jack: “No. I feel like there are settings I don't know about, I think there's a lot of security lapses.”

Most participants viewed themselves as too uninteresting to have their information used. Although users understood the insecurity of the online world, their "uninteresting" posts alleviated their concerns. However, I concluded this lack of concern was due to users viewing other users as risky rather than the service provider. If the information posted was uninteresting to others, there was no real risk. Service providers viewed all information of user behavior as interesting. Participants, however, were more concerned with the settings and permissions given to service providers and the continuous changes in policies by service providers. For example, Frederick had an issue with a past stalker trying to add him on different platforms including Google-Plus. He viewed this as an invasion but was more concerned with Google creating a page he was unaware of with his information.

> Frederick: "Yeah, to try to add on there, and then I realized how much information Google was offering about me online without my permission. Creating a page for me without my permission, which upset me. I was more upset with Google than anything else."

Frederick considered his ability to control his information online adequate, however the platform was not being transparent. If he had been aware of the page, its settings would have been much more stringent than the default function. This proved to be a trend with other participants. There was a lack of awareness of information available about them, misleading settings and permission seeking by platforms.

> Jack: "On Facebook settings, I was just going through, a lot of stuff they changed. The policies now, it says viewable by the public, and I had to change it back to only friends or only me. I think they should have notified the users, because your contact information could be found by other people."

Policies for Social Media continuously change and consistently the default is to leave a user's profile as public as possible. Which was unsettling for participants. The need to be notified by the platform was unsatisfied. For Elizabeth, this was key to her distancing from Facebook.

> Elizabeth: "Because Facebook kept changing their policies, they didn't notify me and it was very vague, or misleading or hard to navigate. That's why I slowly stopped using [it], because there was so many things that I couldn't protect myself from. Like random strangers looking at my name or just knowing things about me that I don't want a stranger to know. It's not something bad I'm doing but I don't want strangers knowing like for example, I'm going to this school or my birthday. Facebook made me feel like you can't really privatize things.. But with Insta and Snap it's so much easier to navigate. You can just private or public your posts."

> Harriet: "I would improve privacy definitely. You would have to inform people if any of the policies are being changed regarding privacy, and definitely if someone wants to delete anything. The company shouldn't store it on archives, it should just be deleted. So, maybe

> legislation. I feel like a lot of the legislation hasn't adapted to the new age, Internet and social media."

Privacy settings for Facebook in particular were unclear and participants had a limited understanding of how to navigate the platform's settings to secure their information. Due to this insecurity, their information was far more accessible than they would prefer. Moreover, some participants viewed the lack of clarity of platform policies as an issue related to the regulation of social media platforms. How vague and inconsistent policies were online translated to how users were able to explain or understand their needs in privacy, if they could not pinpoint exactly where and what needed to be changed, how could they affect any change. Moreover, the use of social media affords the service provider certain permissions. For some participants, not allowing the use of these permissions was a way to mitigate their concerns.

> George :(on privacy settings) "As much as I can make them. They keep asking me, 'do you want to add your phone number to make it more secure?'"
>
> Researcher: "Why would you not do the phone, why do you think it's not a good idea?"
>
> George: "I just don't want them to have my phone number (laughs)... it's the same thing, [why] I don't use FB messenger app, because of all the permissions that it wants. I just use the Web-Chat."

The permissions asked by service providers like microphone usage, access to an individual's photo-album on their cell-phones, proved to be too much of an invasion by service providers. A phone number is searchable, but user's information on social media is more so. A user's information was accessible regardless of restrictions. Frederick, an older participant in his early thirties was much more cognizant of this than the younger users in the study.

> Frederick: "If you look at things like DMCA, and the TPP (Trans Pacific Partnership). So the big thing about that is that people would have to concede a lot of rights on the Internet to be similar to the United States, which opens them up to being sued for copyright infringement in American style courts. Which is really scary but not a lot of people think about that aspect. This really brings to light, like, if you look at Snowden and his leaks, they've been installing backdoors into all of our devices we use and every country does this."
>
> Researcher: "Is social media kind of like a backdoor?"
>
> Frederick: "It's not a back door, but people are stupid with it. Have you ever heard of social engineering? You got hacking, but the biggest flaw to any security network, is social engineering. Yeah, people, you're only as strong as your weakest link. Like what happens when you create a password for Facebook and you forget your password, you go through a password retrieval question. The questions are like what is your mother's maiden name or what is the name of your favorite pet, but if I go on your Facebook, I can find that information on there just like that and people don't think about that. Like those quizzes like what is your mother's last name and street that you grew up in and it creates your Porn Star name and you say that and bam you've given that information. And that's what gets a lot of security exploits things like that going."

Users provided sensitive information daily. The information provided online by users essentially is akin to a map of how to hack into their lives. Two entities can access user information. However, one entity must research the user, while the other has the information from the beginning. Only the former entity to participants is *treated* as risky. Even within the discussion of data skimming, users still viewed their ability to limit information dispersal as enough to limit the amount of information any service provider had of the user.

4.3.2. Restrictions

For participants within this study, concern over how to regulate privacy or restrict Social Media use of their content was of interest. As shown above, users' concerns with their own lack of knowledge over privacy settings and notifications of changes was worrisome. Previous studies have shown that users are either not interested in reading the privacy policies, lacked comprehension of policies or were trusting of the providers (Acquisti & Gross, 2006; Gross & Acquisti, 2005; Jones & Soltren, 2005 *in* Pitkanen & Tuunainen, 2012, p.20). Some studies indicated individuals still maintained a lack of understanding of privacy features (Pitkanen & Tuunainen, 2012, p.20). My findings show that though this could be true participants within this study did have suggestions on how to help or change the current status quo with service providers to benefit the user's interests rather than the service providers. Nonetheless, some of these suggestions were geared towards the mitigation of security risks from other users.

Participants indicated since they relied on privacy settings, these needed to be clearer. If a user does not understand a setting, they could not make an informed decision on how to use it on their profile.

School group 2

> Bethany: "I would change; I would make privacy settings, like you knew what it was the privacy setting did. Like more self-explanatory."
>
> Patrick: "Yeah."
>
> Bethany: "Privacy settings are so confusing. I kind wish there was a list where you can click what you want to show like you're name, your age, your location."
>
> Patrick: "Like they're good but it's so unclear."
>
> Bethany: "Yeah. Like it would be so helpful [to] like 'allow people to click on your profile picture and look at your comments'"
>
> Patrick: "More elaborate."
>
> Bethany: "Although, it would be super detailed. Maybe people are super lazy to do it, but I think people would do that and if you're lazy-"
>
> Evelyn:" Then you're taking the responsibility that, yes I would be okay with it. I didn't read it but I would be okay with what is and what isn't public. I think Instagram could do something like too, like two types of follows."

Courtney: “Like on Facebook friends and acquaintances.”

Bethany: “People who you want to follow or don't follow me.”

Evelyn: “Or like I want registered followers to see this photo and random followers to see that photo.”

Interestingly, some participants were open to a subscription-based option for social media platforms to restrict adverts available on their platforms and other invasions. Most participants were relatively satisfied with the inner workings of social media platforms however; a third party having their information was an issue.

Winston: “I’m pretty happy with how it works for now, with my own use, because I really only use it in the certain proscribed way; I don’t see how the features are lacking in any way. I don't want my information sold to third parties; I don't want my likeness used by other third parties. So, if there was a way to guarantee that that would be nice, but I really haven’t had problems with that. But I think if people want to use the platform with the understanding that it’s going to be used for target marketing, other than paying a fee, because the alternative would be to pay a fee a monthly subscription or something, I’m fine with that because it’s something you agree to when you use the service. You don't necessarily agree for all your information to be used wherever by whatever company. Maybe one change would be a possible subscription for those who are extremely concerned with their privacy where there information is not used in any other than extreme aggregation of viewing. Where it’s anonymous, if they don't want any targeting, then they could pay 5 dollars a month or something and that would cover the cost that was otherwise advertising.”

Nancy: “Advertising. I'm one of the few people; I would actually prefer to pay a little bit for an ad free platform. Especially if I can feel comfortable that they weren't data mining.”

Users were also concerned with the filtering out of information. On Facebook and other social media platforms, the algorithms function to also provide information to the user that may be interesting to them. For some participants, the ability to filter out this function or control for what they want to see or whom they want to see was important.

Nancy: “I don't know enough about the Facebook platform algorithms as I would like to. I have an app on my Facebook called Facebook purity, which undoes some of the Facebook algorithms. It doesn't just show me top trending posts; it shows posts in time order. It doesn't show me trending videos, or trending memes. There are certain sources, like; I don't want to see stuff from this source. So, that lets me filter out stuff that I don’t want to see. But, it would be nice if Facebook had controls like that. That would be a good thing. When you're using Facebook on your phone, there's that thing in the chat window that tells you if someone is online or not and how many minutes had it been since they've been online. I find that so frustrating. I don’t think it's anyone’s business. I've had, actually I’ve had some issues with it where I've had friends who’ve said things like I texted you an hour ago and I saw you were online 10 minutes how come you haven't responded? I actually went to the Facebook FAQ to find out if you can get rid of that and there isn't, like it’s part of the Facebook platform.”

Furthermore, one issue that participants discussed was interactions they experienced with unwanted users. Some users took to different platforms to avoid these interactions. Nancy, however, viewed these unwanted interactions as a basic component to each platform. However,

though she accepted this, she would alter the ability of other users to know she was available, as she viewed it as intrusive (i.e. Facebook chat: green light when online). Other users were more concerned with the ownership of their content. As stated, once uploaded the service provider owns the rights to the users' content. However, if the user is the creator of the content, how is it possible they cannot own their own content. One user provided the suggestion of Wikipedia as an example of how social media platforms can resolve ownership issues.

> George: "Well.... I think if they're not giving name, address and phone number and if it's just like what you like. I try to minimize that sometimes, in browser settings, do not track, but I assume they're going to do it anyways. I've heard, do you know it's true even if you've taken it yourself; they own the copyright to it?"
>
> Researcher: "Yes, they do"
>
> George: "I would change that, because usually if it's a picture that I've posted, I've taken it and it's really good. I would rather make no one have the rights to it than Facebook have the rights to it."
>
> Researcher: "Why do you not want Facebook to have it?"
>
> George: "They're a big conglomerate, they have enough. I've posted to Wikipedia does that count as a social media?"
>
> Researcher: "It can be, if it allows you to connect to someone."
>
> George: "Wiki is like my older ones. I used to use it a lot before now, I don't use it at all."
>
> Researcher: "In terms of pictures and information, if no one had a right to it, what do you think that would mean to you?"
>
> George: "I've posted a lot long time ago on Wikipedia. I would give it the least copyright as possible unless it's in a country where copyright is mandatory, then it's free for anyone to edit public domain."
>
> Researcher: "That's a lot different from how you feel now, why do you think at that point in your life, this doesn't really matter that much and now it does to you?"
>
> George: "Well I would still feel, if I were to post, I would want Facebook to have the same kind of thing where you could choose."
>
> Researcher: "The copyright?"
>
> George: "Yeah."
>
> Researcher: "Would you yourself want the copyright?"
>
> George: "Maybe. If it has me in the picture but otherwise, I'm really, I don't know, I read like these website about no copyright."

Here, the ability to choose whether the service provider or the user who created the content had the copyright was important. If the service provider had the copyright, the user cannot dictate how the provider uses it. The user can however dictate how others use their content and has some legal backing with regards to malicious use of their content. This suggestion was clearer in resolving the user to provider relationship.

> Tom: "Well, I know persistent identification is a trend, so when you log into Facebook, you can log into other sites like Uber and Tinder. So, wherever you go you have a persistent identity. I would change that if I could, but of course that's not realistic. I don't want my account on a dating app or a site where I can order pizza to be connected to my Facebook.

> I don't want to connect my gaming account. Those are different realms, they have different rules, they have different standards of what is appropriate and I see no reason to mix them. And it's an issue with privacy, as well; like you order pizza and then you get Facebook notifications about pizza places around you. I don't want to see that either."

Persistent identifications and ad preferences are similar in that the user has to log on to be able to use certain sites or be able to 'like' or share articles or interests. This allows platforms to tailor the ads shown on a user profile to the users behavior in sites not associated with Social Media. Other participants were aware of this form of identification however did not fully comprehend its meaning. As Harriet stated, it was not pleasant for her to encounter this function, however she continued her use. Tom did not see it this way, different platforms had different uses and rules and as such, to be identified persistently throughout the online realm was an issue in privacy and security. A user's preferences were known throughout, and though there is ease in use, for Tom it was not enough to warrant such an invasion.

Participants stated they would not change the function of social media. However, due to their concerns over privacy, the considerable issue was the service provider's right to know the information. Similar to the discussion of copyrights, a service provider is given a large amount of latitude with regards to user information; although the user provides the information, should the provider have a right to the information, to use, sell, etc.?

> Harriet: "I feel like the privacy settings are fine, before I wasn't mindful of it, but now I am. The privacy is just fine. I just get bored. Maybe I would change something, I would change because it's boring or the ads. They dynamic itself or how it works I wouldn't change."
> Researcher: "You wouldn't necessarily change how you use it, is there anything in terms of them using that information?"
> Harriet: "Yeah, I would change their right to know, that's why you have to be mindful of what you post, because even if you cancel your profile, FB will still have your photos [and] your information in there."

As much as individuals understand that the "Internet is permanent," service provider databases are as well. Even if a page disappears or is removed, if there is a database wherein which it still exists, the information will remain to be found at a later date. The database must be destroyed to remove all permanency of information. This is not realistic, thus the only way to circumvent the permanency is to control what will be permanent about a user online.

Chapter 5. Discussion: Risk in Reverse

"We don't have a choice on whether we *do* social media; the question is *how well we do it*" - Erik Qualman (*Socialnomics; What Happens in Vegas stays on YouTube*)

The current study's overall objective was to determine the appeal of social media and whether the appeal mitigated the lack of privacy on social media. I had hypothesized that the appeal of these platforms would not necessarily mitigate the limitations users have over how their information is dispersed. I posited that there was a higher value placed on privacy and security of information to users than connectivity or gratifications received from voyeurism or exhibitionism. My smaller studies indicated that there was an appeal in the ability to look at other users and those users were managing their social media through different rules of impression management and self-disclosure. These findings were consistent with my current study's findings; voyeurism and exhibitionism were appealing when using social media. Although they were engaging in impression management, users enjoyed the ability to self-present to others. Users also enjoyed the ability to look, (i.e. lurk), at other user's presentations of self-online. Users enjoyed engaging in this behavior, as *their true name* was not attached to their lurker-self. These findings are consistent with Calvert's (2000) theory of mediated voyeurism as it parallels real life gratifications to social media. The user is both voyeur and exhibitionist and is equally balancing these gratifications with the need to *control* the impression of themselves. Furthermore, from the findings and the overall discussion of social media surveillance, I am correct to state that this form of surveillance is more pervasive and intrusive than previous iterations, (e.g. camcorders, CCTV). The information provided is much more contextual and sheds more light on user behavior and everyday occurrences than previous technologies used. Moreover, individuals are more *open* due to the normalization of self-disclosure.

However, the findings indicate that although the appeal of social media was based in the ability to be both voyeur and exhibitionist, the treatment of social media by participants was of a group of individuals who were concerned by the issues in security or privacy online. Users' treatment of social media was based in controlling the flow of their information. They controlled how far-reaching their information was, to whom it was dispersed to and to which platform a part of their self was to be exhibited. Using Goffman (1959), I posited that each platform can be viewed as a stage with different audiences and different or similar claims about an individuals' self. The findings indicate that this assumption was correct in that users present varying degrees of self per

platform used. The more intimate the audience the more authentic the self-exposed. Additionally, these findings suggest that intimacy per Strahilevitz (2005) and Nissenbaum (2004) acts in conjunction to the management of impressions. Claims made about the self must be compatible to the real life self, but the real life self that is exposed, relies on the level of intimacy assigned to the platform.

Findings indicated that users were inherently more concerned with other users' use of their information than with service providers' use of information. Although findings show that the participants were aware and concerned about service provider use of their information, the actions engaged in by participants and discussions with participants indicated that the stratagems used by participants are geared toward the risk other users placed on their information. The service provider was a business, so there was a tacit understanding that given the service provided, the use of their information to do business was not exceedingly intrusive. Even those who cited this as an invasion continued to use the platforms. These findings led me to two distinct questions; what is "private" in today's society? The findings indicated that, for participants, privacy was a fluid term with no real definitive understanding within social media. I also wondered: what should we consider personal identifiable information? This was variable as well throughout my findings. The following is a discussion of these questions.

5.1. How private are you?

Previous studies have discussed the idea of radical transparency, where increased sharing has promoted a level of transparency between users that is unprecedented. This ideology is based on the foundation of openness and transparency of information, which is deemed beneficial for society. Society today is emboldened in the idea of "mediated public-ness (Thompson 2000 *in* Papathanassopoulous, 2015, p.2). As such, this has "facilitated the rise of 'the society of self-disclosure' (Thompson, 2000)" (Papathanassopoulous, 2015, p.2). Essentially turning once private spaces into "more public ones by making them more accessible to the outside world (Meyowitz, 1986)" (Papathanassopoulous, 2015, p2). Mark Zuckerberg as noted, is an advocate of sharing; that is the hallmark of his business. Mark Zuckerberg claimed in 2010 " that privacy was no longer a 'social norm'" (Joinson et al., 2011, p.34). Facebook runs as a space where transparency is rewarded. However, is Zuckerberg correct to state that privacy is no longer a social norm?

The findings indicate that this is a debatable claim. Zuckerberg's own behavior with regards to his own Facebook use makes his claim even more so debatable. The most intimate posts available on his Facebook are of announcements of relationship milestones, (i.e. engagement, wedding, birth of first child), and the standard family holiday pictures, (i.e. Halloween). Most posts on his public profile are of lectures or meetings he attends, charities or individuals he supports and promotes and discussions of issues relating to Facebook. As a public figure there is a level of privacy Zuckerberg must maintain to keep himself and his family safe. However, if at face value, looking through Zuckerberg's public posts, he does not live by this edict, then how could the ordinary user?

Privacy is still a concern for users; however, they are using platforms like Facebook, which champion transparency. Individuals are entering into a privacy paradox when participating in social media. The privacy paradox is related as when the "extensive concern about the safety of one's private data does not necessarily correspond to privacy-related behaviors such as reducing the accessibility of one's Social Web Profile, changing the privacy settings if possible (Aquisiti and Gross 2006; Tufekci 2008; Boyd and Hargittai, 2010) or limiting self-disclosure (Debatin et al. 2009)" *in* (Taddicken & Jers, 2011). This could be due to multiple issues, including, but not limited, to "a lack of problem awareness or media competence, such as ignorance of privacy settings and uncertainty about the audience (Debatin et al. 2009; Boyd and Hargittai, 2010; Aquisiti and Gross, 2006). Or it can be assumed that Social Web use offers advantages and gratifications that increase in direct proportion to the degree of self-disclosure" (Taddicken & Jers, 2011).

The findings indicated that participants within this study occupied such a paradox. Although the user placed restrictions, how far-reaching the dispersal of their information was unknown. For the most part, these participants were web-literate. However, this did not seem to matter as the rules and policies of using their social media were consistently changing without notification. Social media platforms are "public by default and private through effort (Boyd, 2010). Therefore partaking in Facebook's networked public, and trying at the same time not to be public, is not an oxymoron by an 'agentic act" (Livingstone, 2008, p.409) by means of which users protect their identity (Georgalou, 2016). To be private in a public sphere is difficult. Users are impeded by the vagueness of privacy settings or the inability to understand the settings. Therefore, their actual means of limiting information is through both the settings and terms of service available to them and their own decision-making processes. The user protects their privacy with the "adoption of various self-protective strategies" (Yao, 2011, p.112).

Privacy within the online realm is concerned with user information. It is the ability to "control what information about you is conveyed to others and for what purposes" (Henderson, 2012, p.232). However, on social media, users are controlling information to other *users* and not to the service provider. My findings suggest choice and control is limited within social media. Users possess much more control over how their information is dispersed to other audiences, but the most important audience is the service provider. Moreover, within the opt-out system of most social media platforms, users' default setting is exceedingly public. Users are pushed into the position of choosing what information to hide rather than what information to expose. Furthermore, the Internet is, by definition, public. There is an assumption of lack of privacy. However, the issue with the online realm is the permanency of the information dispersed (Papacharissi & Gibson, 2011, p.76). How private could a person be if their information is permanently online?

Within the understanding of privacy used within this thesis, these findings suggest that parts of the definition used are compatible to user's understanding of their privacy online. Users have selective control in limiting the accessibility of their information *to other users but not service providers.* These boundaries between the creator of content and the co-possessor are negotiated within limited confines. Between users, there is an understanding of appropriate and inappropriate behaviors, (e.g. negative, positive or neutral lurkers). However, between the service provider and the user, the negotiation is not realized. There is no mutual understanding of disclosure and control of dispersed information. It is a unilateral decision that leaves the user at a loss (Zuboff, 2015). Online privacy has predominately been viewed in interpersonal terms, as users consistently frame any violations in privacy as between users rather than between the user and the service provider. However, the relationship between user and service provider cannot be viewed within interpersonal terminology, (i.e. person to person versus person to entity). Therefore, although the privacy definition provided in Chapter Two is applicable to the overall discussion of privacy within this thesis, privacy viewed in terms of a transaction between service provider and user may be more useful in determining a user's expectation of privacy and information dispersal online. For the service provider, there must be a balance maintained where they can both gain profit from the user's information and limit user disquiet over the amount of control they have on the platform (Ziegele & Quiring, 2011). The service provider will utilize as much information as possible from a user's profile for the betterment of their profit margin. As such, although there is a goal to please (or appease) the user, limiting the amount of control the user has over user information benefits the service provider.

The availability of privacy settings allows the user to perceive there is control over to whom and what they share online, however, the continuously changing features and privacy settings "circumvent their knowledge about privacy management and eventually make them share more content publicly than they intended to do" (Zeigele & Quiring, 2011, p.182). The newest feature of Snapchat is illustrative of this. Snapchat now allows users to indicate their locations on the platform and disclose this on a map tied to other users on the platform. The platform provides a chance to opt out of the feature when a user first opens up the feature, however it has become a popular new feature. The issue with this feature is that individuals are disclosing location information at all times. Therefore, if any other user looks through the map of users on their list, they can see where a user is located at any given time. This may be a godsend to the police force, however for the average user, it limits their privacy even more.

For the most part users choose whether or not to indicate their location when posting. However, with this feature, the service provider can track user location information and compile a list of a user's most frequented places and disperse that information to advertisers. A frequented brand can buy ad-space and have advertisements placed on the user's profile or on profiles similar to the user. Ironically, Snapchat is considered one of the more private social media platforms currently available. My findings indicate that the extent of privacy afforded to an online user is based on their own agency with regards to how they engage with a service provider. For a service provider, the transaction begins the moment information is given to the site. Any information given is information that can be utilized for profit unless otherwise stated. If a user requires more privacy online, the negotiation between themselves and the service provider is one where the service provider acts as a co-possessor of information without any duty to disclose where information is being shared. However, as stated, once an image is posted onto a platform it changes ownership from the user to the service provider. The same can be said for any other uploaded content. Thus, a user must decide within the limited means provided to them, what, how much, and what type of information they are willing to disclose. However, this can prove to be difficult as service providers create and encourage features like the above Snapchat map, to decrease limited disclosures by users. A user is left to decide what to disclose based on a limited understanding of how much information a service provider has, or can have, as seen in the above results. If an individual chooses complete privacy, social media is not a space they should participate in.

5.2. What is Personal Data?

My findings indicated that users had a perceived control over their personal information. Hoadley et al (2010) found that illusory control is important to an individual users' perception of privacy, where loss of control leads to a users' perception of an increased accessibility of their information. This correlated with my findings as participants moved platforms once they felt they were unable to completely control the dispersal of their personal information. For most users, ignorance was not bliss. Users are exceedingly ignorant to the practices used by the Social Media platforms they engaged in, however users were frustrated over their lack of knowledge, which left them unsatisfied with their level of privacy. The user is at a complete disadvantage as the system allows Social Media platforms to leave their producers/consumers in the dark (Zuboff, 2015). The user is then left to construct their own understanding of how to exist and engage online. Privacy and control over information are valued, but due to the users' disadvantage there is a lack of clarity of what personal information is and what data is dispersed. To be private included the ability to choose their audiences, choose the information disclosed, and the ability to control the level of attachment information had on an individual user. However, personal information was understood as identifiable information, which social media platforms state that they will not disclose. However, personal information or personal data is more than just an individuals' phone number or address. In fact, the information 'not shared' by service providers is just *contact information*. Which, for most users is given out in real life through resumes and other daily activities. The content of the posts users give is personally identifiable information, which seemed misunderstood by users; it was contradictory to say that providers data-skim and aggregate user data, but still post to a platform regardless of whether a "real" name was attached. The information given is still personal data that could be linked to a user.

Personal identifiable information is all user content; the issue is that users do not view this information as identifiable as it has not been *defined* to them as such. For users to subjectively define personal information as private it must be given those characteristics (Papacharissi & Gibson, 2011, p. 84). However, once information is supplanted on the realm of tradable goods, it takes on a public face rather than a private one. The information is "commercialized into the public realm, with little input from the individual in the process" (Papacharissi & Gibson, 2011, p. 84). As such, users are presenting their information with the indoctrinated idea that the information they are providing is *not identifiable data*. However, this is a false belief. Users are opening themselves up to two kinds of data breaches. The first type of data breach is the fact that other users can use the information provided online to hack onto affiliated user platforms, which is similar to

Frederick's understanding of the weakness of users, (i.e. social engineering). However, this is a smaller potential risk to what could happen with service providers. The second type of data breach concerns the service provider's databases. The aggregated information provided to service providers is kept within databases under the service provider's control. If user's interests, affiliations and attitudes, categorize the catalogued information service providers have, a veritable blue-print of whom an individual is readily available. For example, a user's political outlook can be determined by individual likes, shares and network affiliations; this information can be used to steer user voting to particular candidates through ad-space. Service providers could have a profile double or data double[1] of the user linked to online profiles the user is affiliated to. Individual actions are tracked based on what profiles and accounts the user links to online, so any activity a user engages in can be amalgamated to create their online double. Facebook, for example owns Instagram; users indicated within this study that the information provided to Instagram is different from that provided to Facebook; however, Facebook owns both databases. Thus, any information given can be aggregated to form one complete profile of the individual user. Depending on what periphery platforms service providers own, users' data double or doubles are available for service provider's use. Moreover, these data-doubles may be more consistent with individuals' real life self than the selves managed online by the user; making these doubles more valuable to third parties both malicious and otherwise.

Users are able to password protect their information, however they must opt-out of ad-space and tracking features on social media. Although their information can be protected from other users, it is not protected from their service provider. A user can close the door to their personal information online, however; they are not the only ones with the key to this information. If their service provider has the ultimate key, their information is vulnerable to being used and abused by other parties. Unlike email, where anti-spamming legislation has been enacted to curb the practice, social media service providers are not affected by such regulation with regards to user information. Individuals are adapting to these limits in privacy and surveillance by providing both justifications to their usage through the appeal of social media and through their treatment of social media. However, with little to no regulation over social media, these platforms are "continuously redefin[ing] what is legally considered private…as a result [users] personal data are often violated without [their] consent" (Odeomelam, 2015, p.575). It is assumed that users are

[1] A data double is "our vital/informational profiles that circulate in various computers and contexts of practical application" (Haggarty & Ericson, 2006, p.4). Essentially, a data double is an individual's online duplicate.

giving informed consent over the information uploaded. This is a false assumption. If users are unable to define what personally identifiable data is in relation to their social media use, informed consent has not been provided to service providers. Users must know exactly what information is being provided to third parties and their service providers to be able to make an informed decision over a) their participation on social media, b) the information dispersed by them on social media. Users do not have the complete picture to make informed decisions about their usage.

5.3. Normalizing Surveillance

Social media and the continuous advancement of technology have led to further development of surveillance technologies and surveillance behavior in society. The relation between privacy and security is a tenuous one, even more so within the age of social media. Security of information is not necessarily the same as having privacy of information. They are related but change in one does not necessarily mean change in the other (Henderson, 2012, p.234). If there is no definitive understanding of both privacy and identifiable information, the question of how to be safe online may be more appropriately placed in considering how secure an individual's information is. Security of information means that an individual's information is secure from different forms of risks, where the burden of protecting the information is placed on the service provider rather than the individual user. However, this would place the service provider at a disadvantage. Security of information may require opt-in services and detailed informed consent processes that would invariably affect the bottom-line for service providers. Instead, surveillance has become akin to security. Users can survey each other and police themselves without the need of the service provider to do so, thus, allowing service providers to continue their own surveillance without issue. Personal data, as stated within this thesis, is a commodity for social media service providers. For the past two decades "dataveillance…[a] kind of "watching" using not sight…but amassing details to create profiles" has been at the forefront for larger companies (Lyon, 2007). Social Media service providers are not the forbearers of the accumulation of personal data; however social media service providers have advanced this form of surveillance by normalizing 'sharing' to their users; people freely giving information is good for business.

By making the process of sharing normal, users are participating in their own surveillance and as well as acting as surveillers of other users. These behaviors act as justification to the appeal of social media and limits the concerns placed on social media by users. By being an active participant in surveillance, any infringement of privacy is negated as self-exposure and self-

disclosure by the individual removes the expectation of privacy. As such, participation in social media makes the role of the surveiller and the surveilled a guaranteed position taken on by users, removing liability from the service provider. It is therefore unremarkable that privacy issues concerning digital media focus more on the user-to-user interpersonal violations of privacy rather than user-to-service provider violations. Service providers do not necessarily categorize the dispersal of information, as discussed within this thesis, as a violation of user privacy. Moreover, the public character of social media and personal data on social media negates this characterization. Users are in compliance with surveillance and therefore in compliance with the public definition of their information. If social media is "accepted as legitimate and necessary then it is unlikely that anyone will question [it]," however this agreement to how service providers define and control social media usage is not based in knowledge of how much of their data is used (Lyon, 2007, p.164).

Users are trying to negotiate the use of their data by finding an agreement with their service providers that work for the user. However, the service provider is both changing definitions and the processes of how to use and perceive social media, compliance with social media practices becomes easier than negotiating with them. Social media is an omniopticon, where different levels of surveillance co-exist. Users are participating in a state of "continuous mutual surveillance where every user acts both as agent and subject" (Jensen, 2010 *in* Murmaa & Siibak, 2012). Users are able to "monitor other citizens' behavior through nonreciprocal forms of watching" (Humphreys, 2011, p.577). Moreover, users are voluntarily submitting to surveillance by corporations, (i.e. participatory Panoptican), where users are consenting to the "monitoring of their own behavior" (Humphreys, 2011, p.577). If there is a benefit to the user by using the service, compliance to surveillance is highly likely. My findings suggest this is the case for most users. The issue with compliance to this surveillance is that users are not told the complete story by service providers. Grenville (2010) notes that one of the first steps to engaging in an informed decision on how a user uses social media and what they disclose is *knowledge* (p.73). An understanding of how to classify the information they could disclose, where the information goes, and to whom it is used by, is important to a user's overall understanding of social media and social media service providers. Users in this study and previous studies showed an awareness of what it meant to participate but this awareness was superficial. The accessibility of their data and the use of their data for commercial purposes were far reaching. However, the perceived control over information leaves the users' personal identifiable information vulnerable, allowing for the surveillance of all. However, educating users and regulating the information dispersed online will

afford users the ability to see what data is used, how it is used, and what that data *means* to corporations using it. Accordingly, this could lead to a better outcome than the society Varian (2014) discusses that is numb to ubiquitous surveillance by corporations and the like (Zuboff, 2015). Agency, the ability to choose and decide is key to keeping a complete surveillance society at bay.

Chapter 6. Conclusion

"Social Media is not about the exploitation of technology but the service to community" – Simon Mainwaring

6.1. Implications

The current study provided many insights into how individual users perceive limits to privacy online. The appeal of social media lies in the ability to engage in the dual role of voyeur and exhibitionist for the user. Although the participants in this study had an awareness of the limits to security and privacy on Social Media, they considered the control they practiced online with regards to the managing of their social media enough to mitigate these concerns. However, participants could, in a limited sense, control *externally,* through the use of use of privacy settings, who looked into their profiles, however *internally (i.e. within the inner workings of the platform),* they lost the little control they had. Participants took a position where they accepted limited control over their information rather than full control. If I were to ask most participants, which would you rather have – Privacy or Social Media – it may be a harder question to answer than once thought.

Mark Zuckerberg fashioned his social network service under the helm of 'sharing.' He encourages all his users to think that 'We as users need to share more to others'. This may seem positive, as sharing has led to exposures of human interest incidents like the war in Iraq, the Gaza Strip, Aleppo and the Arab Spring. However, underscoring this is the fact that privacy online is relatively non-existent. Sharing has become the norm, thus surveillance in whatever form will be maintained and viewed as necessary. If users do not share it could be seen as suspicious, thus society would rather share *too* much than not share at all. Since we are all surveilling each other inclusive of corporations and the government, surveillance is viewed as a matter of fact. How much privacy is then appropriate to expect online? Moreover, is there a need for a definition that applies to the online world generally? For legal avenues, there should be some form of criteria used in applying such cases, however I posit this should be situated within real world consequences. Strahilevitz' (2005) states it should be based on the amount of reach the users' information could have, (i.e. how many expected users will the information get to), for Nissenbaum (2004), the context of the disclosures, however do they not come down to the same issue? What are the real life consequences of user disclosures and how do the disclosure(s) affect the user and those associated with the incident?

Within traditional privacy law, public disclosure of private facts does not require that the information provided to be concerned with legal or criminal avenues, “courts have broadly recognized newsworthiness” as a legitimate reason for user privacy to be impugned (p.149). The assumption is that a user “implicitly consents to sharing his information with others, regardless of the self-regulating privacy settings” (Breslawski, 2013, p.1286). Thus, any information “taken from public records meets the standard of public concern and therefore, there is no invasion of privacy by publishing it” (p.149). This view sees any claim to privacy as erroneous as the user voluntarily chooses to post online and thus should not be afforded the expectation. Regardless of whether a large majority of a user base views the content posted, the user has made accessible their “thoughts to ‘the public at large’” and the potential viewership nullifies any claims of privacy the user could have (*Moreno v. Hanford Sentinal Inc. 2009*, as cited in Lidsky & Friedel, 2012, p.244).

Everything disclosed online is permanently held in online databases. Everyone online is accessible to others including corporations and the government. Therefore, in today’s world *reach*, (i.e. how far-reaching an audience is), context, newsworthiness, all means the same. Everyone is accessible, regardless of restrictions and therefore defining privacy under our traditional understanding of privacy within a space that is exceedingly public seems ineffective for both the law and general public discourse.

If we were to endeavor a look, collectively, at what an individual shares to whichever audience, all their information is available waiting for you, the requisite anonymous creeper to find. Within this thesis, participants, in their discussion of how they use social media and what they chose to post on social media, illustrated this. Due to the fluidity in their understanding of privacy online, more information than they wished to be available about them online seemed to be available. The issue with privacy in the online realm is that the common person has an antiquated idea of what privacy is. We are taught and have learned from the media that to be private online means to restrict any personal identifiable information. In all social media Terms and Conditions and FAQs, corporations state clearly that they will never give out any personal identifiable information. With that knowledge, participants within this study felt appeased. They acknowledge that these corporations are data skimming but this does *nothing*. The user will have more ads on their profile, but this can be easily mitigated by ad-blocks. However, this deflects from the key issue. The treatment of user data is based on the fact that users are not *owners* of their own content once uploaded. Schwartz’ (2005) discusses viewing personal data as individual property and as such treats the consumer as the owner of their online personal data rather than

the corporation. This theory correlates with Petronio's Communication Privacy Theory (2002), as it holds the creator as the owner of their content and information, in effect the decider of how to disperse said content. Although written prior to the upsurge of social media platforms, this proposition translates to the agreements between social media corporations and their consumers/producers. The model states that personal data should be considered in terms of property interests, where restrictions focus on how the data is used and transferred and who authorizes these actions. The model would "permit the transfer of personal data for an initial category of use (i.e. providing demographic information to *Facebook* for registration purposes), but only if the user is granted an opportunity to block further transfer or use by unaffiliated entities (i.e. *Facebook* providing the demographic information provided to third-parties like the government or *Wal-Mart*)" (Schwartz, 2005, p.1271).

Moreover, this model would also provide the consumer the option to opt-in to any added use or transfer of their personal data essentially prohibiting the "granting [of] one-stop permission for all use or transfer of their information" (Schwartz, 2005, p.1271). The premise of Schwartz' "user-transfer restriction" argument focuses on the metadata a user provides to a corporation that is transferred to third parties (Sparapani, 2012, p.1313). With regards to social media corporations Sparapani (2012) indicates that for the most part, the misuse of user information is executed by third parties and such regulations should focus on "deter[ing] third parties who are not explicitly authorized by consumers from accessing and using consumers' information" (p.1314). However, a full-scale implementation of this model would be difficult. Essentially, the model is giving consumers full discretion over their personal data regardless of where that information is. For some participants within this study, this would be ideal. Whatever metadata the social media platform has is not *owned* by the corporation but by the user, therefore providing the user the ability to *control* the dispersal of their personal information. Fuchs (2012), states opt-in policies are "favored by consumer and data protectionists" (p. 149). These policies favor the individual users' right to choose, either the information received by them as well as the information given by them. However, most corporations favor the "opt-out and self-regulation advertising policies in order to maximize profit", opt-in policies would be detrimental to both data surveillance and profits (p.149). Thus, by creating a space wherein the corporation for its own benefit, defines the understanding of personal identifiable information, allows the corporation to keep the user in a false sense of security.

As such, corporations' stating they do not give out personal identifiable information are self-serving. If there is any real concern over third parties receiving user information from service

providers, the user is unable to expect any recompense. They are the culprits in their own downfall. A cursory look through an individual users' profile provides important hints of their life. Moreover, audiences or followers linked to a user can provide more information about the user. Users need to consider that personal identifiable information is equivocal to Personal Identifiable Data, (i.e. the data aggregated by Social Media platforms, Google etc.). Any user with limited Internet skills can find information about a given user. They only have to look through one profile.

This implies that users need to be educated on what Personal Identifiable Data means. Personal identifiable information is terminology used by service providers defined in terms of contact information. Whereas, with in this thesis, Personal Identifiable Data is a term that looks to expands past the superficially defined personal identifiable information. If users truly want to control information dispersed without ending their participation on social media, there needs to be knowledge of the extent of what Personal Identifiable Data is. Based on the above interviews, a definition of Personal Identifiable Data needs to consider the fact that everything a user posts, comments, likes or shares online, for example, videos users watch and bookmark or save to view later, GIFs a user shares, people a user follows, people who follow the user, is personally identifiable data. Other users and corporations can investigate the pages the users follow, the school attached to a users' profile or even the friends attached to the profile. An individual user's data is everywhere. Restricting dispersal should mean more than restricting whom *views* the data. It should mean changing how an individual user disperses the information and what is dispersed. When posting, participants within this thesis asked questions like: "is this relevant," "is this appropriate," "is this interesting;" they consistently stated "I am not that interesting" or "I don't post anything I don't feel comfortable other people will see;" or "how much do I want to keep to myself." The real guide to restricting dispersal and maintaining a modicum of privacy online should *how much of my PID do I want out there?* This relies on how we define PID. As such, I created a definition of Personal Identifiable Data, which I believe provides guidance to users:

> *Personal Identifiable Data is any information online about an individual user that can inform other parties of the user's surroundings, workplace, family, or any such information that allows another user or third-party to locate or communicate with and/or observe the user (In Real Life or Online) without the latter's permission.*

If control is illusory and privacy online cannot be expected, individual users must control their posts using this designation. Control needs to occur outside the norm, not primarily in privacy settings but based on knowledge of how far reaching data can be and how much information an

individual has decided is acceptable to be permanently online. This will vary from user to user, however, decisions of this kind must be informed. Currently, they are not.

6.2. Limitations

6.2.1. Issues with the analytical approach used

There are issues with having theoretical influences and previous knowledge in the subject matter within the process of grounded theory as it could result in the researcher being "unable to consider alternative concepts for the phenomenon being investigated" as the claims made could be considered to have weight and could leave the researcher failing to "provide an original and grounded interpretation" (Wilson & Hutchinson, 1996 in Howard-Payne, 2016, p. 59). Moreover, as the researchers' previous knowledge may influence the subject matter, the researchers own background could "shap[e] the research at the expense of the problems of concern to informants" (Koch, 1994 in Heath & Cowley, 2004, 143). These are legitimate concerns a researcher may face when engaging with their research in the fashion proposed by Strauss & Corbin.

However, these concerns, in my view, were not limitations with regards to the subject matter at hand. Having previous knowledge or contact with the current subject matter studied is more an advantage than a disadvantage. General grounded theory bases some of its processes on being an objective party that may or may not be part of the population sampled. Glaserian-grounded theory prefers no relationship with the subject matter to allow for no bias (Glaser, 2002, p.23). However, all researchers come into studying any subject matter with some bias; it is the researcher who must place their bias aside and study their preferred topic in an objective manner. In the case of social media and technology as a whole, having *no* knowledge can be more of a detriment in undertaking a study than a benefit, due to the harsh learning curve a researcher would invariably shoulder. Specifically, a researcher must learn how to use the technology studied, its functions with regards to software as well as terminology attached to the technology as a whole. Attempting this during the data collection process could prove to be laborious, as the researcher would be playing catch-up. Attempting this prior to the data collection would undermine the process the researcher is following. Attempting this after the data collection period could prove to be an effort in patience or frustration. Without some cursory understanding of the technology studied, the researcher may not be able to completely comprehend his or her participants' insights into the subject matter and some interview time would be spent on the researcher asking perfunctory questions about a software or piece of technology rather than the more complex

questions concerning the interviewees thoughts, uses and overall perception of the technology or software studied.

If terminology were understood after the data collection, the availability of research subjects to answer more comprehensive questions would be in question. Moreover, if a researcher has had no contact with certain technology, there must be a reason behind his or her avoidance. There could be an underlying bias that speaks to why the researcher has had no contact, namely, a lack of interest or negative outlook on the technology, which could color how the research *discusses* the subject matter. That is not to say there would no bias with a researcher who uses the technology or software studied regularly. There will be some due to their positive outlook and the fact that the researcher makes the technology a part of their lives. Bias exists in both situations and in both cases the researcher can set aside whatever biases they may have to conduct good research.

In my case, I saw this as an opportunity. I use social media, but not on a regular or persistent basis. I am also part of a generation who grew up with exponentially advancing technology. Technology and innovation is part of the story of my life as it is for most Millennials. As such, my knowledge of technology, including social media, is due in part to environment and necessity. Any further understanding is due to interest in using social media. The advantage in knowing the terminology available and understanding it led to providing a better descriptive analysis of the subject matter studied.

Moreover, as stated, a good researcher can and will put aside any biases they may have to allow for good research. Furthermore, a good researcher can and will acknowledge any biases they may have and moreover be reflexive in the event that bias does color, influence or marginally interact with the subject matter studied. In this case, I was able to set aside my biases concerning the subject matter at hand, but I also saw having prior knowledge within the interview environment as beneficial. I was objective in making sure to disallow my bias to color the questions asked and allowed for participants to speak their truth. By having relative knowledge in the subject matter permitted an easier conversational environment within the interview; there was a relational aspect in discussion as by having knowledge in the social media used or being a user myself gave the interviewee a level of ease. I assumed that this ease was due to an assumption by the interviewee that any behaviors or activities or occurrences they may have experienced could have occurred to myself and thus, there was no judgment on my part. Without this relational aspect, conducting an interview with any profound data gained may have proved to be more difficult.

With regards to including theoretical influences within the study, which is some deviation to some grounded theory processes; having some theoretical influence or foundation can provide a more comprehensive understanding of the subject matter. Moreover, with a subject matter like social media, where theory building is relatively new, having some prior theory or theories that could aid in explaining the phenomenon, seemed reasonable, as it provided some guidance in how to interpret the data.

6.2.2. Sampling and Design Limitations

There are two key sampling limitations that should be discussed. At the start of the study, the hope was to have a larger participant pool from the lower-mainland secondary school used. Unfortunately, due to issues with ethics approval for the study, I was only able to meet with students from the chosen secondary school at the end of their school year. Moreover, during this period students between grades 7-10 were unavailable due to scheduled field trips. Thus, any comparison between younger adolescents to university students was somewhat limited. As discussed in my findings, the adolescent focus groups used were comparatively similar to university students. This may be due to similarities in age and understanding of social media. This was quite revealing in terms of the comparison of older high school students and university students because it is more commonly assumed that they would have a different outlook. However, I believe having a broader age group would have provided the study with a more complete outlook on what adolescents today consider when using social media and their perceptions on privacy in comparison to older individuals. 12-15-year-old students may have a completely different outlook to those 16-17 year old participants and older university students. I posit this different outlook in their decision-making process of posting and the length of use or experience may not inform their understanding of privacy. Adolescents are more likely to begin using social media at a younger age, however what they do use and how they use it may be completely different from that of older adolescents or adults. Therefore, it was unfortunate to have not been able to discuss these questions with the younger adolescents within the chosen school.

Finally, looking through the overall study, some changes to the questions asked could have led to a much more depth in understanding. Primarily, I would have discussed participants' understanding of Personal Identifiable Information at more length than I did during the interviews. Although enough data was gained to provide a preliminary understanding of their comprehension, further questions would have been beneficial. Furthermore, participants' understanding of reach could have been delved deeper within interviews. The participants did have an awareness of

reach and through examples there seemed to be a working understanding of how far reaching their information could become; however similar to my previous study on “Creeping” behavior, it was sometimes only when I provided them with an example of reach did they comprehend their own reach or audience. Restricting their information within the set controls has shown to be more of an illusory control, thus I would have liked to expand my questions to further the articulation of their views on reach and the control they had over this. Reach seems to be closely linked with their understanding of privacy, thus could prove illuminating to current literature.

6.3. Future Research

Future research should focus on how individuals understand personal identifiable information and how this relates to how individuals self-present on social media and how surveillance works online. We are a ‘sharing’ society, where privacy has become less and less obtainable. The consideration here is that any personal data online can be considered identifiable. It is a just matter of ‘looking” for the right information. Corporations cash in on this sharing sensibility and cloak and dagger the process by stating identifiable information will never be shared. However, everything on Social Media is identifiable information, therefore this statement is a misrepresentation of Social Media’s actual practices. This could link to users understanding of accessibility. It seems through the current study that users have an awareness of surveillance occurring, however is it a limited awareness due to limited knowledge or information available to them? This should be expanded upon within Social Media literature. Finally, our understanding of online privacy should be encapsulated in terms of our understanding of what the online realm is: boundless and in constant development. I do state there is no real privacy on Social Media, however this does not encapsulate the entire Internet. There may come a day where ‘spaces’ online could be considered private. Thus, a further understanding of what privacy could mean online situated within the definition and understanding of the online world would prove to be enlightening to current social media literature.

References

Amadeo, R. (2015). Google officially ends forced Google+ integration: First up YouTube. *Arstechnica.* Retrieved from: https://arstechnica.com/gadgets/2015/07/google-officially-ends-forced-google-integration-first-up-youtube/

Angwin, J. (2014). Dragnet nation. New York: Henry Holt and Company.

Baruh, L. (2010). Mediated voyeurism and the guilty pleasure of consuming reality television. *Media Psychology*, *13* (3), 201-221.

Bagdasarov, Z., Greene, K., Banerjee, S.C., Krcmar, M., Yanovitzky, I., Ruginyte, D. (2010). I am what I watch: Voyeurism, sensation seeking and television viewing patterns. *Journal of Broadcasting & Electronic Media, 54* (2), 299-310.

Boyd, D. (2014). It's complicated: The social lives of networked lives. New Haven: Yale University Press.

Boyd, D. & Ellison, N. (2008). Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication*, *13,* 210-230.

Breslawski, T. (2013). Privacy in social media: To tweet or not to tweet? *Touro Law Review, 29*, 1283-1304.

Buffardi, L.E., & Campbell, W.K. (2008). Narcissism and social networking websites. *Personality and Social Psychology Bulletin, 34* (10), 1303-1314.

Calvert, C. (2000). Voyeur nation: Media, privacy, and peering in modern culture. Colorado: Westview Press.

Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedural canons, and evaluative criteria. *Qualitative sociology, 3*(1),

Constine, J. & Cutler, K. (2012). Facebook buys Instagram for $1Billion, turns budding rival into its standalone photo app. *TechCrunch.* Retrieved from: https://techcrunch.com/2012/04/09/facebook-to-acquire-instagram-for-1-billion/

Constine, J. (2015). A year later $19Billion for Whatsapp doesn't sound so crazy. *TechCrunch.* Retrieved from: https://techcrunch.com/2015/02/19/crazy-like-a-facebook-fox/

Cross, M. (2013). Social media security: Leveraging social networking while mitigating risk. Waltham: Syngress.

DeWall, C.N, Buffardi, L.E, Bonser, I., & Campbell, W.K. (2011). Narcissism and implicit attention seeking: Evidence from linguistic analyses of social networking and online presentation. *Personality and Individual Differences, 51*, 57-62).

Ellison, N., Steinfeld, C., Lampe, C. (2006). Spatially bounded online social networks and social capital: The role of Facebook. Proceedings from *Annual Conference of the International Communication Association (ICA),* June 19-23, 2006, Dresden Germany.

Everett, C. (2010). Social media: Opportunity or risk? Computer Fraud & Security, 2010 (6). 8-10

(2016) Page Post Metrics. *Facebook Help Centre.* Retrieved from: https://www.facebook.com/help/336143376466063/

Ferrucci, P., Edson T.C. (Jr.), Duffy, M. E. (2014). Modeling reality: The connection between behaviour on reality TV and Facebook. *Bulletin of Science, Technology & Society, 34*(3-4), 99-107.

Fogel, J. & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behaviour, 25,*153-160.

Fuchs, C. (2012). The political economy of privacy on Facebook. *Television & New Media*, *13* (2), 139-159.

Georgalou, M. (2016). 'I make the rules on my wall': Privacy and Identity management practices on Facebook. *Discourse & Communication, 10* (1), 40-64.

Gentile, B., Twenge, J.M., Freeman, E.C, Campbell, W.K. (2012). The effect of social networking websites on positive self-views: An experimental investigation. *Computes in Human Behaviour, 28*, 1929-1933.

Gill, P., Stewart, K., Treasure E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal,* 204 (6), 291-295.

Glaser, B. (2002). Conceptualization: On theory and theorizing using grounded theory. *International Journal of Qualitative Methods, 1*(2), 23-38.

Goffman, E. (1956) Self-Presentation *From The Presentation of Self in Everyday Life*. In Lemert, C. Branaman, A. (1997) (pp.21-26). *The Goffman Reader.* USA: Blackwell Publishers Inc.

Goldfarb, R. (Ed.) (2015). After Snowden: Privacy, secrecy and security in the information age. New York: Thomas Dunne Books.

Grenville, A. (2010). Shunning surveillance or welcoming the watcher? Exploring how people traverse the path of resistance. In Zureik, E. *Surveillance, Privacy and the Globalization of Personal Information: International Comparisons*. (Pp.70 – 85). Montreal & Kingston, Canada: McGill-Queens University Press.

(2016). About us. *Instagram*. Retrieved from: https://www.instagram.com/about/us/

Haggarty, K.D, & Ericson, R.V. (2006). The new politics of surveillance and visibility. *In* R. V. Ericson & K. D. Haggerty (Eds.), *The new politics of surveillance and visibility* (pp. 3–25). Toronto: University of Toronto Press.

Heath, H., & Cowley, S. (2004). Developing a grounded theory approach: A comparison of Glaser and Strauss. *International Journal of Nursing Studies, 41*(1), 141-150.

Heyman, R., De Wolf, R. & Pierson, J. (2014). Evaluating social media privacy settings for personal and advertising purposes. *Info*, 16(4), 18-32.

Hoadly, C.M., Xu, H., Lee, J.J., & Rosson, M.B. (2010). Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Research and Applications*, *9*, 50-60.

Howard-Payne, L. (2016). Glaser or Strauss? Considerations for selecting grounded theory study. *South African Journal of Psychology, 46*(1), 50-62.

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication, 61*, 575-595.

Joinson, A., Houghton, D., Vasalou, A., & Marder, B. (2011). Chapter 4: Digital crowding: Privacy, self-disclosure, and technology. In Trepte, S. & Reinecke, L. (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* (pp.33-46) New York: Springer.

Keenan, T. (2014). Technocreep: The surrender of privacy and the capitalization of intimacy. New York: Greystone Books.

Kemp, S. (2015). Digital, social, mobile in 2015:We are social's compendium of global digital statistics. *We are Social.* Retrieved from: http://wearesocial.net/tag/statistics/

Kemp, S (2016). Special reports: Digital in 2016. *We are Social.* Retrieved from: https://wearesocial.com/uk/special-reports/digital-in-2016

Kramer, N. & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. In Trepte, S. & Reinecke, L. (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* (pp.127-142). New York: Springer.

Kowalski, S.P., Krattiger, A. (2007). Confidentiality agreements: A basis for partnerships. In *Intellectual property Management in Health and Agricultural Innovation: A Handbook of Best Practices*. (Eds.) A Krattiger, R.T. Mahoney, L. Nelson, et al. Davis, USA: PIPRA.

Lyon, D. (2007). Surveillance studies: An overview. Cambridge: Polity Press.

Lidsky, L. & Friedel, D. (2012). Legal pitfalls in social media usage. In Noor Al-Deen, H.S. & Hendricks, J.A. (Eds.), *Social Media: Usage and Impact*. (pp.237-253). Toronto: Lexington Books

Marguilis, S. (2011). Three theories of privacy: An overview. In Trepte, S. & Reinecke, L. (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* (pp.9-18). New York: Springer.

McNamara, K. (2009). Publicising private lives: Celebrities, image control, and the reconfiguration of public space. *Social & Cultural Geography, 10* (1), 9-23.

McNealy, J. (2012a). Chapter 15: The realm of the expected: Redefining the public and private spheres of social media. In Noor Al-Deen, H.S. & Hendricks, J.A. (Eds.), *Social Media: Usage and Impact* (pp.255-270). Toronto: Lexington Books.

McNealy, J. (2012b). The privacy implications of digital preservation: Social Media archives and the social networks theory of privacy. *Elon Law Review, 3,* 133-160.

Munar, A. (2010). Digital exhibitionism: The age of exposure. *Culture Unbound, 2,* 401-422.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119-158.

Odemelam, C.E. (2015). Adapting to surveillance and privacy issues in the era of technological and social networking. *International Journal of Social Science and Humanity, 5* (6), 572-577.

Papacharissi, Z. & Gibson, P. (2011). Chapter 7: Fifteen minutes of privacy: Privacy, sociality, and publicity on Social Networks. In Trepte, S. & Reinecke, L. (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* (pp.75-90). New York: Springer.

Papathanassopoulos, S. (2015). Privacy 2.0. *Social Media & Society,* 1-2.

Panek, E. (2014). Left to their own devices: College students' guilty pleasure media use and time management. *Communication Research, 41*(4), 561-577.

Pena, J., & Brody, N. (2014). Intentions to hide and unfriend Facebook connections based on perceptions of sender attractiveness and status updates. *Computers in Human Behaviour, 31,* 143-150.

Pitkanen, O. & Tuunainen, V.K. (2012). Disclosing personal data, socially: An empirical study on Facebook users' privacy awareness. *Journal of Information Privacy and Security, 8*(1), 3-29.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. New York: W.W Norton & Company.

Schulman, Y. (2014). In real life: Love, lives and identity in the digital age. New York: Grand Central Publishing.

Schwartz, P. (2005). Privacy Inalienability and the regulation of spyware. *Berkley Technology Law Journal, 20*(3), 1269-1282.

Smitha, N. (2013). Facebook metrics defined: Impressions. *Simply Measured.* Retrieved from: https://simplymeasured.com/blog/facebook-metrics-defined-impressions/#sm.000oij9lj105ue7jvi923hen575i4

Sparapani, T.D., (2012). Putting consumers at the heart of the social media revolution: Toward a personal property interest to protect privacy. *North Carolina Law Review, 90*, 1309-1325.

Strahilevitz, L. (2005). A social networks theory of privacy. *The University of Chicago Law Review, 72*, 919-988.

Taddicken, M. & Jers, C. (2011). The uses of privacy online: Trading loss of privacy for social web gratifications? In Trepte, S. & Reinecke, L. (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* (pp. 143-158). New York: Springer.

Tassi, P. (2013). Google Plus Creates Uproar Over Forced YouTube Integration. *Forbes.Com,* Retrieved from: *https://www.forbes.com/sites/insertcoin/2013/11/09/google-plus-creates-uproar-over-forced-youtube-integration/#6e4de0881f07*

(2016). "The History of Social Networking." *Digital Trends.* Retrieved From: https://www.digitaltrends.com/features/the-history-of-social-networking/

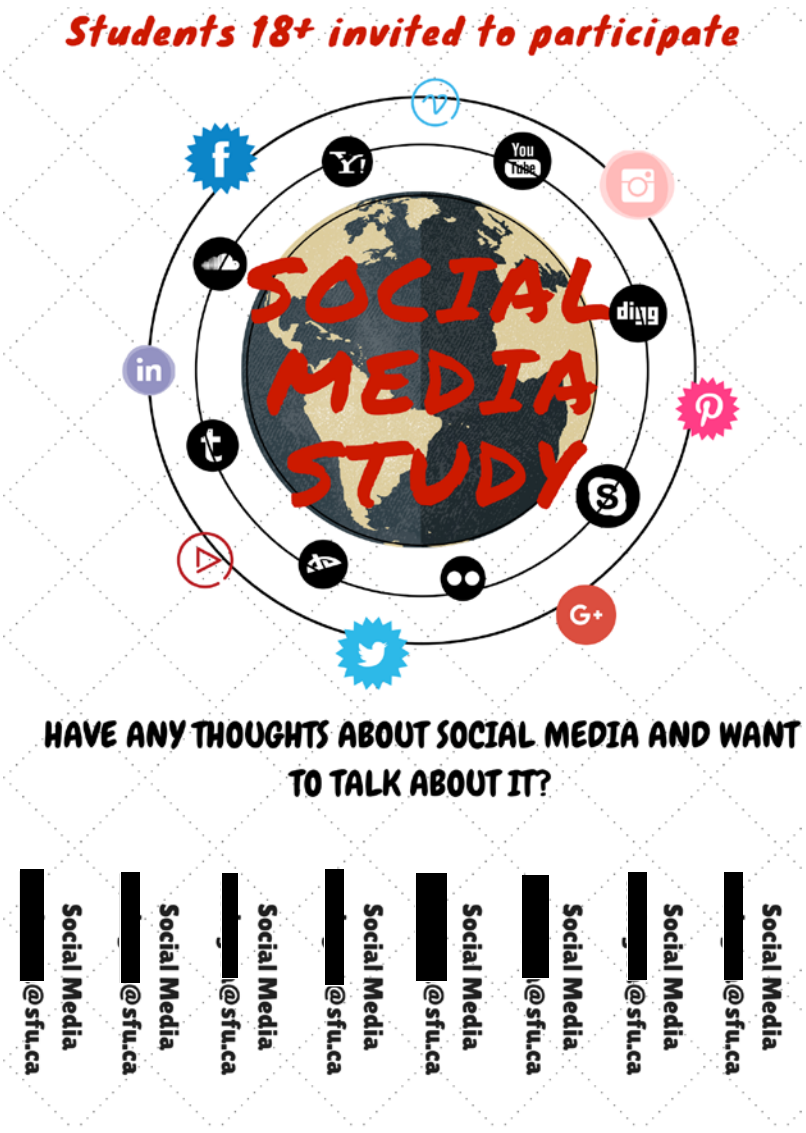
Qi, M. & Edgar-Nevill, D. (2011). Social networking searching and privacy issues. Information *Security Technical Report, 16*, 74-78.

Wang, S.S. (2015). To unfriend or not: exploring factors affecting users in keeping friends on Facebook and the implications on mediated voyeurism, *Asian Journal of Communication, 25 (5), 465-485.*

Ziegele, M. & Quiring, O. (2011). Privacy in social network sites. In Trepte, S. & Reinecke, L. (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* (pp.175- 190). New York: Springer.

Appendix I.

Poster



Email Recruitment

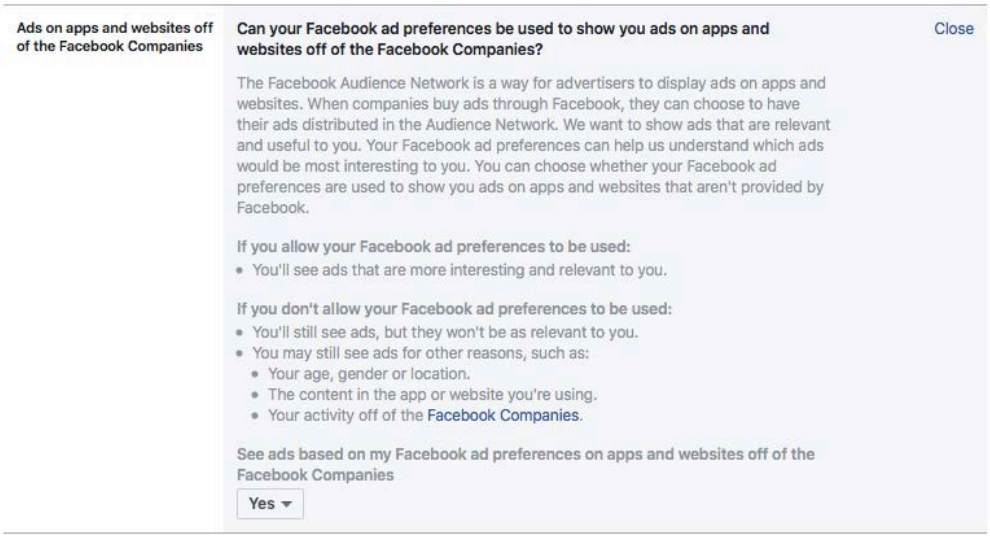
SIMON FRASER UNIVERSITY SCHOOL OF CRIMINOLOGGY RECRUITMENT INFORMATION SHEET

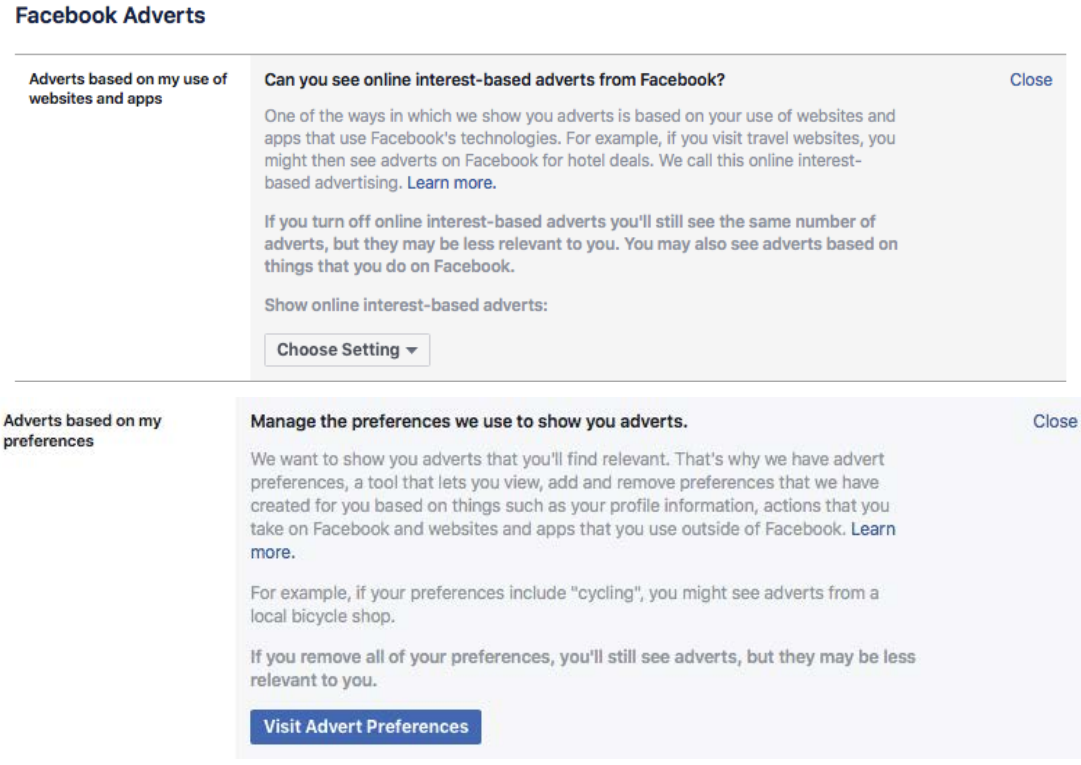
Appealing to the Masses: The Allure of Social Media Anna Ndegwa (BSocSc.) and Dr. Ted Palys (Ph.D.) from the School of Criminology at Simon Fraser University (Burnaby) are conducting a research study.

I am inviting you as a possible participant in this study because as a user of social media, you may have insight as to why social media is so prevalent in everyday-life. Specifically, either because you are part of a demographic that grew up using social media or were part of its rise, any insight provided would be of interest to the overall research topic. Your participation in this research study is voluntary. The study is being conducted to learn more about why individuals use social media and if there are varying degrees of appeal within that use. I am inviting individuals such as you who have an interest in discussing social media as a phenomenon and as a tool of the everyday. As this study's research questions are not sensitive in nature, there is minimal risk in you participating in this study. If you volunteer to be a part of this research study, you can participate either in a focus group or a singular interview based on your availability. Questions will be geared towards social media and its appeal to individual users. The interviews and focus groups will be recorded with your permission. You can stop being in this study at any time during the interview or focus group and afterwards. If you have any concerns about your rights as a research subject and/or your experiences while participating in this study, you may contact Dr. Dina Shafey, Associate Director, Office of Research Ethics at [redacted]sfu.ca or 778-[redacted].

If you would like to take part in this study, please contact Anna Ndegwa (BSocSc.): email: [redacted]@sfu.ca

Appendix II.


Ads on apps and websites off of the Facebook Companies
Can your Facebook ad preferences be used to show you ads on apps and websites off of the Facebook Companies?
Close
The Facebook Audience Network is a way for advertisers to display ads on apps and websites. When companies buy ads through Facebook, they can choose to have their ads distributed in the Audience Network. We want to show ads that are relevant and useful to you. Your Facebook ad preferences can help us understand which ads would be most interesting to you. You can choose whether your Facebook ad preferences are used to show you ads on apps and websites that aren't provided by Facebook.
If you allow your Facebook ad preferences to be used:
You'll see ads that are more interesting and relevant to you.
If you don't allow your Facebook ad preferences to be used:
You'll still see ads, but they won't be as relevant to you.
You may still see ads for other reasons, such as:
Your age, gender or location.
The content in the app or website you're using.
Your activity off of the Facebook Companies.
See ads based on my Facebook ad preferences on apps and websites off of the Facebook Companies
Yes


Facebook Adverts
Adverts based on my use of websites and apps
Can you see online interest-based adverts from Facebook?
Close
One of the ways in which we show you adverts is based on your use of websites and apps that use Facebook's technologies. For example, if you visit travel websites, you might then see adverts on Facebook for hotel deals. We call this online interest-based advertising. Learn more.
If you turn off online interest-based adverts you'll still see the same number of adverts, but they may be less relevant to you. You may also see adverts based on things that you do on Facebook.
Show online interest-based adverts:
Choose Setting
Adverts based on my preferences
Manage the preferences we use to show you adverts.
Close
We want to show you adverts that you'll find relevant. That's why we have advert preferences, a tool that lets you view, add and remove preferences that we have created for you based on things such as your profile information, actions that you take on Facebook and websites and apps that you use outside of Facebook. Learn more.
For example, if your preferences include "cycling", you might see adverts from a local bicycle shop.
If you remove all of your preferences, you'll still see adverts, but they may be less relevant to you.
Visit Advert Preferences

Facebook Pixel Information

https://www.facebook.com/business/a/facebook-pixel

https://www.facebook.com/business/help/952192354843755

https://www.facebook.com/business/a/online-sales/custom-audiences-website#u_0_2

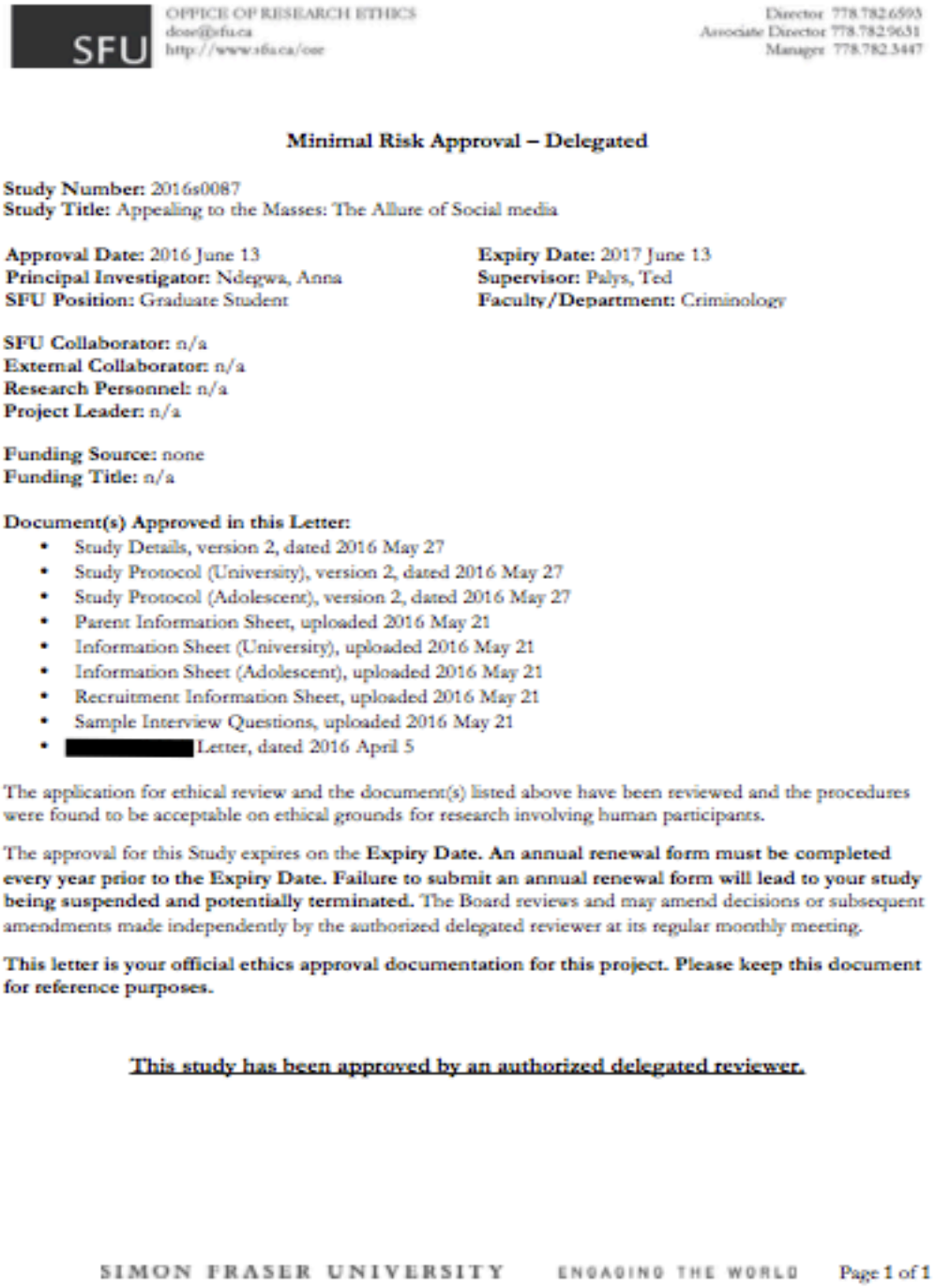
https://www.facebook.com/business/a/lookalike-audiences

https://www.facebook.com/business/a/pixel-best-practices

https://www.facebook.com/business/a/add-pixel-standard-events

Appendix III.

REB: ETHICS REVIEW DOCUMENTS



SFU

OFFICE OF RESEARCH ETHICS
dore@sfu.ca
http://www.sfu.ca/ore

Director 778.782.6593
Associate Director 778.782.9631
Manager 778.782.3447

Minimal Risk Approval – Delegated

Study Number: 2016s0087
Study Title: Appealing to the Masses: The Allure of Social media

Approval Date: 2016 June 13
Principal Investigator: Ndegwa, Anna
SFU Position: Graduate Student

Expiry Date: 2017 June 13
Supervisor: Palys, Ted
Faculty/Department: Criminology

SFU Collaborator: n/a
External Collaborator: n/a
Research Personnel: n/a
Project Leader: n/a

Funding Source: none
Funding Title: n/a

Document(s) Approved in this Letter:

- Study Details, version 2, dated 2016 May 27
- Study Protocol (University), version 2, dated 2016 May 27
- Study Protocol (Adolescent), version 2, dated 2016 May 27
- Parent Information Sheet, uploaded 2016 May 21
- Information Sheet (University), uploaded 2016 May 21
- Information Sheet (Adolescent), uploaded 2016 May 21
- Recruitment Information Sheet, uploaded 2016 May 21
- Sample Interview Questions, uploaded 2016 May 21
- [redacted] Letter, dated 2016 April 5

The application for ethical review and the document(s) listed above have been reviewed and the procedures were found to be acceptable on ethical grounds for research involving human participants.

The approval for this Study expires on the **Expiry Date. An annual renewal form must be completed every year prior to the Expiry Date. Failure to submit an annual renewal form will lead to your study being suspended and potentially terminated.** The Board reviews and may amend decisions or subsequent amendments made independently by the authorized delegated reviewer at its regular monthly meeting.

This letter is your official ethics approval documentation for this project. Please keep this document for reference purposes.

This study has been approved by an authorized delegated reviewer.

SIMON FRASER UNIVERSITY ENGAGING THE WORLD Page 1 of 1

PDF 1: Initial Minimal Risk Approval

SFU OFFICE OF RESEARCH ETHICS
dore@sfu.ca
http://www.sfu.ca/ore

Director 778.782.6593
Associate Director 778.782.9631
Manager 778.782.3447

Annual Renewal Approval

Study Number: 2016s0087

Study Title: Appealing to the Masses: The Allure of Social media

Annual Renewal Date: June 14, 2017

Expiry Date: 13 June 2018

Principal Investigator: Anna Ndegwa

Supervisor: Ted Palys

SFU Position: Graduate Student

Faculty/Department: Criminology

SFU Collaborator: n/a
External Collaborator: n/a
Research Personnel: n/a
Project Leader: n/a

Funding Source 1: n/a
Funding Title 1: n/a

Document(s) Approved in this Application:

- Annual Renewal Report

The approval for this study expires on the **Expiry Date. Failure to submit an annual renewal form will lead to your study being suspended and potentially terminated.** If you intend to continue to collect data past the term of approval, you must submit an annual renewal form at least 4 weeks before the expiry date.

This letter is your official Annual Renewal Approval documentation for this project. Please keep this document for reference purposes.

The annual renewal for this study been approved by an authorized delegated reviewer.

PDF 2: Annual Review Approval

2016s0087

SIMON FRASER UNIVERSITY SCHOOL OF CRIMINOLOGY
MASTER STUDY DETAILS

Appealing to the Masses: The Allure of Social Media

Principal Investigator: Anna Ndegwa, Graduate Student, School of Criminology
Contact: [redacted]@sfu.ca or 604-[redacted]
Faculty Supervisor: Dr. Ted Palys, Professor, School of Criminology
Contact: [redacted]@sfu.ca or 778-[redacted]

Project Number: 2016s0087

Study Details:

This research involves interviews and focus groups conducted with two different samples: (1) adolescents at a private school in Vancouver; and (2) adult university students. Although my interests in both run parallel, the populations involve slightly differing ethical issues, such that some documents pertain to both samples, and some to one study or the other. The following table shows which files are associated with which sample population:

Study Documents and the Sample(s) each is Associated With

Document Name	Study Component
Ndegwa_MasterStudyDetails2015-2016	Both
Ndegwa_StudyChecklist-2015-2016	Both
Ndegwa_InterviewSampleQuestions-2015-2016	Both
Ndegwa_StudyProtocolUniversity-2015-2016	University
Ndegwa_InformationSheetUniversity2015-2016	University
Ndegwa_RecruitmentInformationUniversitySheet-2015-2016	University
Ndegwa_StudyProtocolAdolescents2015-2016	Youth
Ndegwa_AdolescentInformationSheet2015-2016	Youth
Ndegwa_ParentInformationSheet2015-2016	Youth
[redacted]LetterofAmenability	Youth
Ndegwa_CPIC/VulnerablepersonsCPIC	Youth

Overall, the goal of my research is to understand how individuals in these two sample groups perceive social media and why they use social media; considering the issues with regards to security and privacy that are tied to its use. As stated in the above-mentioned documents, I will be interviewing these sample groups and will anonymize (providing pseudonyms to participants) the data gathered during the transcription process. All recordings will be destroyed once interviews are transcribed. Please see the attached documents for a complete synopsis of the proposed research. With regards to secondary data (previous mini studies I conducted), I received a minimal risk approval from my course instructors (Dr. Ted Palys – CRM862 and Dr. Sheri Fabian – CRM864). During the course of each mini study I made clear to my participants that I may, in the future, use the data collected for future research (conference presentations and thesis), which they consented to. I am the steward of the aforementioned secondary data.

Version 2 May 27, 2016

PDF 3: Master Study Details

SIMON FRASER UNIVERSITY SCHOOL OF CRIMINOLOGGY

RECRUITMENT INFORMATION SHEET

Appealing to the Masses: The Allure of Social Media

Anna Ndegwa (BSocSc.) and Dr. Ted Palys (Ph.D) from the *School of Criminology* at Simon Fraser University (Burnaby) are conducting a research study.

I am inviting you as a possible participant in this study because as a user of social media, you may have insight as to why social media is so prevalent in everyday-life. Specifically, either because you are part of a demographic that grew up using social media or were part of its rise, any insight provided would be of interest to the overall research topic. Your participation in this research study is voluntary.

The study is being conducted to learn more about why individuals use social media and if there are varying degrees of appeal within that use. I am inviting individuals such as you who have an interest in discussing social media as a phenomenon and as a tool of the everyday.

As this study's research questions are not sensitive in nature, there is minimal risk in you participating in this study.

If you volunteer to be a part of this research study, you can participate either in a focus group or a singular interview based on your availability. Questions will be geared towards social media and its appeal to individual users. The interviews and focus groups will be recorded with your permission.

You can stop being in this study at any time during the interview or focus group and afterwards.

If you have any concerns about your rights as a research subject and/or your experiences while participating in this study, you may contact Dr. Dina Shafey, Associate Director, Office of Research Ethics at [redacted]@sfu.ca or 778-[redacted].

If you would like to take part in this study, please contact

Anna Ndegwa (BSocSc.): email: [redacted]@sfu.ca

PDF 4: REB Recruitment Information Sheet

Sample Interview Questions

1. Why do you think social media has become so popular within your social circle?
2. What are your thoughts on the different forms of social media out there?
3. What's the most frequented form of social media you use? Explain why
4. Are there other forms of social media that you find interesting but you yourself don't use, why?
5. *What about these forums of social media do you think is appealing?*
6. How do you decide what you will share online?
   (Within this could ask why share that particular content? - I have asked this question in the previous study in Sheri's class and my interviewee's discussed this in a way that was more like a 'revelatory moment for them)
7. Within the forms of social media you use, how do you use them?
   Do you use specific forms for specific reasons?
   Are there other ways to use these forms of social media external to its primary/initial use
8. Can you think of situations where you became worried that your identity or information wasn't safe? (If stories from the media come up ask them about this)
   Explain/what are your thoughts on these types of situations?
9. What are your thoughts on the popular types of content being shared on social media currently?
   (Maybe here ask what types of content do they think is popular online- prior to asking #9)

   (From prior study the interviewees discussed the issues they had with some types of popular content like insta-models or issues with 'trolling', which segues into #10)
10. What do you think/feel about anonymous liking/sharing of content? (Here connects to popularity of content – the sharing/liking of media by individuals that the user doesn't know – here users from the previous study discussed the good and the bad of anonymous sharing – like social stalking or becoming 'viral')
11. Is there anything within the social media realm you would change?
12. Why do you continue using social media? (- I put this question here because some of the questions though not explicit end up having a discussion about the pitfalls of using social media etc.)

PDF 5: Sample Interview Questions (Ethics Review)

OTTAWA POLICE SERVICE
SERVICE DE POLICE D'OTTAWA

Working together for a safer community
La sécurité de notre communauté, un travail d'équipe

CRIMINAL RECORDS CHECK

This search is not intended for individuals seeking a volunteer and/or employment position with children or vulnerable person(s).

FORM #308/Rev. May 2010

PRINT CLEARLY. THIS WILL BE USED TO MAIL YOUR FORM BACK TO YOU.

ANNA NDEGWA.
[redacted]
< First Name, Middle Name, Surname
< Unit/Number, Street
< City, Province
< Postal Code

[redacted]

I hereby certify that the information provided above is true and correct to the best of my knowledge and belief. I hereby authorize the Ottawa Police Service to conduct such searches as are deemed necessary to obtain the information required to complete this Criminal Records Check and disclose such information to me.

SIGNATURE OF APPLICANT: [redacted]

Signed this date: 05/MAY, 201 5

(BY APPLICANT)

A Police Criminal Records Search may provide the following information obtained from the Canadian Police Information Centre (C.P.I.C)

- Outstanding entries (i.e. charged & wanted persons)
- Records of criminal convictions, as the records exist on the date of search
- Findings of guilt where a pardon has not been granted

VOID *without* Ottawa Police seal

FOR POLICE USE ONLY

☑ **This is to confirm that no criminal convictions nor outstanding charges have been found in the Canadian National Repository of Criminal Records as a result of a search based on the above name and date of birth. The search has not been confirmed by fingerprints.**

☐ **This is to notify that there may be criminal convictions associated to the above name and date of birth, the existence of which can only be confirmed by the RCMP based on fingerprints.**

☐ **This is to notify that there may be outstanding charges associated to the above name and date of birth.**

Date Completed (yy/mm/dd): 15/05/05

(BY POLICE)

Signed: [redacted]

POLICE AUTHORIZING SIGNATURE

PDF 6: CPIC (Vulnerable Persons Check)

SIMON FRASER UNIVERSITY SCHOOL OF CRIMINOLOGY

STUDY PARENT INFORMATION SHEET

Appealing to the Masses: The Allure of Social Media

Anna Ndegwa (BsocSc) and Dr. Ted Palys (Ph.D.), from the *School of Criminology* at Simon Fraser University, are conducting a research study.

Your child was selected as a possible participant in this study because as a user of social media, they may have insight as to why social media is so prevalent in everyday-life. Specifically, either because they are part of a demographic that grew up using social media or were part of its rise, any insight provided would be of interest to the overall research topic. Your child's participation in this research study is voluntary.

This research will form part of my MA thesis, and may also be reported in conference presentations, articles and/or books. The information gained in the study could be of use to social media corporations, research on social media users and research on social media as a phenomenon.

Why is this study being done?

The study is being conducted to learn more about why individuals use social media and if there are varying degrees of appeal within that use. I am inviting individuals such as your child who have an interest in discussing social media as a phenomenon and as a tool of the everyday.

What will happen if my child takes part in this research study?

If you agree to allow your child to participate in this study, we would ask him/her to:

- They can either decide to participate in one focus group based on their availability or be available for one singular interview.
- During the study, questions will be geared towards social media and its appeal to individual users
- Your child as a participant will have a chance to provide insight and opinions to these discussions

- The interviews and focus groups will be recorded due to the open-ended nature of these discussions

An example of an interview question: What do you do on the social media platforms you use?

How long will my child be in the research study?

Participation will take about *one to two hours over a period of one day. This date will be specified by the school and will not interfere with your child's education.*

Are there any potential risks or discomforts that my child can expect from this study?

As the research question is not sensitive in nature, there is minimal risk in their participation in the study. If anything, the study may reduce risk for the students because of the opportunities the discussion will provide to talk about strategies people use to manage and protect their personal information on social media.

Are there any potential benefits to my child if he or she participates?

The insights your children share will enhance our understanding of the phenomenon of social media and how and why adolescents use them. After the study is complete, I will make a summary of the results available to the school and any students who are interested.

Will information about my child's participation be kept confidential?

Your child's confidentiality will be respected within this study. Any information that could be associated with a particular child will never be released without child and parental consent. Furthermore, everyone who participates will be provided with a pseudonym, anonymizing them within the study. The interviews and focus groups will be recorded, however once transcribed, these audio recordings will be destroyed. The transcripts will be kept on a secure USB and will be stored in a secure location. With regards to participation in focus groups: I encourage all participants to respect each other's confidentiality. However, I cannot control what participants do with the information discussed, so you and your child should consider that when deciding whether to participate in a focus group or interview.

What are my and my child's rights if he or she takes part in this study?

- You can choose whether or not you want your child to be in this study, and you may withdraw your permission and discontinue your child's participation at any time.
- Whatever decision you make, there will be no penalty to you or your child, This decision will not have any negative consequences to the education, employment or other services to which your child is entitled to or presently receiving.
- Your child may refuse to answer any questions that he/she does not want to answer and remain in the study.

Who can I contact if I have questions about this study?

If you have any questions, comments or concerns about the research, you can talk to the primary researcher. Please contact:

Anna Ndegwa (BSocSc): email: [redacted]@sfu.ca

Complaints/Concerns

If you have any concerns about your child's rights as a research subject and/or their experiences while participating in this study, you may contact Dr. Dina Shafey, Associate Direct, Office of Research Ethics at [redacted]@sfu.ca or 778-[redacted].

You will be given a copy of this information to keep for your records.

SIMON FRASER UNIVERSITY SCHOOL OF CRIMINOLOGY

ADOLESCENT (Ages 13-17) INFORMATION SHEET

Anna Ndegwa (BSocSc) and Dr. Ted Palys (Ph.D.) from the *School of Criminology*, at Simon Fraser University.

You were invited as a possible participant in this study because as a user of social media, you may have insight as to why social media is so prevalent in everyday-life. Specifically, either because you are part of a demographic that grew up using social media or were part of its rise, any insight provided would be of interest to the overall research topic. Your participation in this research study is voluntary.

This research will form part of my MA thesis, and may also be reported in conference presentations, articles and/or books. The information gained in the study could be of use to social media corporations, research on social media users and research on social media as a phenomenon.

Why is this study being done?

The study is being conducted to learn more about why individuals use social media and if there are varying degrees of appeal within that use. I am inviting individuals such as you who have an interest in discussing social media as a phenomenon and as a tool of the everyday.

What will happen if I take part in this research study?

Please talk this over with your parents before you decide whether or not to participate. We will also ask your parents to give their permission for you to take part in this study. But even if your parents say “yes” you can still decide not to do this.

If you volunteer to participate in this study:

- You can either decide to participate in one focus group based on your availability or be available for one singular interview.
- During the study, Questions will be geared towards social media and its appeal to individual users
- You as a participant will have a chance to provide insight and opinions to these discussions
- The interviews and focus groups will be recorded due to the open-ended nature of these

discussions

How long will I be in the research study?

Participation in the study will take a total of about *one hour to two* hours*.*

Are there any potential risks or discomforts that I can expect from this study?

As the research question is not sensitive in nature, there is minimal risk in you participating in the study.

Are there any potential benefits if I participate?

The insights you share will enhance our understanding of the phenomenon of social media and how and why people use them. After the study is complete, I will make a summary of the results available to the school and any students who are interested.

Will information about me and my participation be kept confidential?

Your confidentiality will be respected within this study. Any information that might identify you personally will never be released without your consent. Furthermore, everyone who participates will be provided with a pseudonym (fake name). The interviews and focus groups will be recorded, however once transcribed, these audio recordings will be destroyed. The transcripts will be kept on a secure USB and will be stored in a secure location. With regards to participation in focus groups: I encourage all participants to respect each other's confidentiality. However, I cannot control what participants do with the information discussed, so you should consider that when deciding whether to participate in a focus group or interview.

What are my rights if I take part in this study?

You may withdraw your assent at any time and discontinue participation. This decision will not have any negative consequences to the education, employment or other services to which you are entitled or presently receiving. You may refuse to answer any questions that you do not want to answer and remain in the study.

Who can answer questions I might have about this study?

If you have any questions, comments or concerns about the research, you can talk to the primary researcher. Please contact:

Anna Ndegwa (BSocSc.) Email: [redacted]@sfu.ca

Complaints/Concerns

If you have any concerns about your rights as a research participant and/or your experiences while participating in this study, you may contact Dr. Dina Shafey, Associate Direct, Office of Research Ethics at [redacted]@sfu.ca or 778-[redacted]

You will be given a copy of this information to keep for your records

STUDY INFORMATION SHEET

Appealing to the Masses: The Allure of Social Media

Anna Ndegwa (BSocSc.) and Dr. Ted Palys (Ph.D.) from the *School of Criminology* at Simon Fraser University (Burnaby) are conducting a research study.

You were invited as a possible participant in this study because as a user of social media, you may have insight as to why social media is so prevalent in everyday-life. Specifically, because you are part of a demographic that either grew up using social media or were part of its rise, any insight provided would be of interest to the overall research topic. Your participation in this research study is voluntary.

This research will form part of my MA thesis, and may also be reported in conference presentations, articles and/or books. The information gained in the study could be of use to social media corporations, research on social media users and research on social media as a phenomenon.

Why is this study being done?

The study is being conducted to learn more about why individuals use social media and if there are varying degrees of appeal within that use. I am inviting individuals such as you who have an interest in discussing social media as a phenomenon and as a tool of the everyday.

What will happen if I take part in this research study?

If you volunteer to participate in this study:

- You can either decide to participate in one focus group based on your availability or be available for one singular interview.
- During the study, questions will be geared towards social media and its appeal to individual users
- You as a participant will have a chance to provide insight and opinions to these discussions

- The interviews and focus groups will be recorded due to the open-ended nature of these discussions

How long will I be in the research study?

Participation will take a total of about an hour to two hours maximum of your time once you have confirmed your participation.

Are there any potential risks or discomforts that I can expect from this study?

With regards to potential risks, I do not see there being anything in this study that could pose a risk or be harmful to you. As the research question is not sensitive in nature there is minimal risk in you participating in the study. Furthermore, as the facilitator, if sensitive topics do come up in discussion and participants express discomfort, I will endeavor to steer the discussion back to topics at hand, if the former are not in some way related to the research question.

Are there any potential benefits if I participate?

Though the study may not directly benefit you, the insight you share may in the future provide an understanding to the phenomenon of social media. Social media is a popular platform and for the most part researchers have yet to tap into why social media holds such an appeal to a variety of people. You could help in understanding this.

Will information about me and my participation be kept confidential?

Your confidentiality is respected within this study. Any information that might be identified will never be released without your consent. Furthermore, everyone who participates will be provided with a pseudonym, anonymizing them within the study. The interviews and focus groups will be recorded, however once transcribed, these audio recordings will be destroyed. The transcripts will be kept on a secure USB and will be stored in a secure location. With regards to participation in focus groups: I encourage all participants to respect each other's confidentiality. However, I cannot control what participants do with the information discussed, so you should consider that when deciding whether to participate in a focus group or interview.

What are my rights if I take part in this study?

- You can choose whether or not you want to be in this study, and you may withdraw your consent and discontinue participation at any time.
- Whatever decision you make, there will be no penalty to you. The decision will not have any negative consequences to the education, employment or other services to which you are entitled or presently receiving.
- You may refuse to answer any questions that you do not want to answer and still remain in the study.

Who can I contact if I have questions about this study?

If you have any questions, comments or concerns about the research, you can talk to the primary researcher. Please contact:

Anna Ndegwa (BSocSc.): email: [redacted]@sfu.ca

Complaints/Concerns

If you have any concerns about your rights as a research subject and/or your experiences while participating in this study, you may contact Dr. Dina Shafey, Associate Director, Office of Research Ethics at [redacted]@sfu.ca or [redacted]

You will be given a copy of this information to keep for your records

PDF 7: Study Protocol Adolescents

2016s0087

Appealing to the Masses: The Allure of Social Media

Principal Investigator: Anna Ndegwa, Graduate Student, School of Criminology

Faculty Supervisor: Dr. Ted Palys, Professor, School of Criminology

Project Number: 2016s0087

Study Objectives:

There are over 2 billion social media users worldwide. Their ease of use, convenience and the services they provide have become indispensable to users, but at what price? Theorists such as Zuboff [1] describe social media as the epitome of the contemporary surveillance economy, where terms of service establish that, in exchange for use of the platform, individuals supply personal information that becomes the property of the platform, and which the site can then aggregate and sell to other corporations, or simply use internally to personalize the ads you are offered, thereby increasing your likelihood of clicking on an ad, with each click contributing to the wealth of the social media platform.

In a previous study, I focussed on *how* individuals manage their social identities – their presentation of self – on social media. My results indicated that although individuals understood the loss of privacy their sharing of information allowed, and would often try to circumvent this, they also accepted that they have no control how their content is disseminated once uploaded; despite being identifiable and often involving intensely personal information, the terms of service make clear the information, once posted, and sometimes even after being ostensibly "deleted," is the property of the platform and not the user. The current study strives to find out more about *why* users continue to use these sites if lack of control is the underlying caveat.

Study Design:

Research Question: The proposed research will study users' perception of these sites and the fascination they and other users have with these sites. Specifically, my research question is as follows: *What exactly is the appeal of these sites that users accept an agreement that holds them at a disadvantage?*

Sample: High school students are a highly appropriate sample for this research. Students are adolescents who have grown up in a digital world. Social media could be said to be the most widely used form of media by this particular demographic and it is rare to find anyone of this age group who is not connected to more than one social media site (social media sites include platforms for the exchange of personal information with one's defined community of contacts or "friends," e.g., Facebook, Twitter, Instagram, Snapchat). There will be at least 3 focus groups and up to 10 one-on-one interviews conducted. The focus group groupings will be dependent on the availability of interested parties.

Recruitment:

[1] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30,* 75-89.

I have been in contact with a lower mainland semi-private high school. The administrators are amenable to having the study conducted at their organization. The school chosen has its own internal processes with regards to studies conducted at the school and have chosen to allow for the study to be conducted (see [redacted]LetterofAmenability2016.pdf).

Students will be provided with an information sheet (see Ndegwa_AdolescentInformationSheet2015-2016.docx) and an information sheet for their parental guardians (see Ndegwa_ParentInformationSheet2015-2016.docx) detailing the study. In conjunction with the school administrators, we will schedule an appropriate date and time(s) where students who have chosen to participate will complete the study. The interviews will be conducted at the school during school hours at times chosen by the institution to minimize conflict with the students' academic and extracurricular schedules.

Data Gathering Procedures:

Focus group discussions and semi-structured interviews will be the primary methods of data collection. Participants will include individuals between the ages of 13-17. The composition of focus groups/singular interviews will be decided based on the scheduled interview date and time(s) by the school administrators and myself. Specifically, students interested in singular interviews will have particular allotted times where they can participate in the study and students interested in participating in focus groups will be provided with separate allotted times for their participation in the study. All interviews and focus groups will be conducted at the high school and will vary between 45 minutes to 60 minutes.

The Consent Process:

In accordance with Section 5 (1-11, 17-18) of the Simon Fraser University Research Ethics Policy (R20.01), informed consent will include the following affordances to participants:

1. A summary of the purpose of the study through an information sheet (see Ndegwa_ AdolescentInformationSheet2015-2016.docx/Ndegwa_ParentInformationSheet2015-2016.docx) provided to the individuals prior to the commencement of either focus group or singular interview
2. An assurance that participants can withdraw from the study at any time. Refusal to participate or withdrawal/dropout after agreeing to participate will not have an adverse effect or consequences on the participants, their employment or education.
3. If they choose to withdraw at any time, the participants' information will be removed from the study and destroyed. The removal of their information will be done as follows:
    a. If the participant was part of a singular interview:
        i. If the interview has yet to be transcribed, I will destroy the recordings (i.e. delete electronic copies) and any notes made from the interview will be shredded securely.

ii. If the interview has been transcribed and audio recordings destroyed forthwith, I will shred both transcripts and notations from the interview securely.

b. If the participant was part of a focus group:

i. If the focus group has yet to be transcribed, I will transcribe the focus group but leave out instances where the participant speaks. I will then destroy the audio recordings, as is procedure.

ii. If the focus group has been transcribed:

1. I will shred any initial hard copy transcriptions of the focus group interview

2. I will review the electronic copy transcription of the focus group interview, remove every instance of speech of the participant, and proceed with the version excluding their participation.

4. That all data will be kept in a secure off campus location only known to me to maintain confidentiality and that all audio recordings will be destroyed once transcribed to ensure confidentiality. Moreover, all electronic versions of transcriptions will be documented within a password-protected document. I will be asking participants if they consent to being recorded prior to the start of the interview as well as within the recorded interview. If participants choose not to be recorded, I will record their interview using notations in a Word document. I will make this document an encrypted password-protected document to maintain confidentiality. Difficulty will occur if a focus group participant does not consent to being recorded. As such, it may not be prudent for them to be a part of such a discussion if other participants have consented to being recorded. Thus, if a focus group participant does not consent to being recorded at the time of the focus group discussion, I will ask the participant to consent to a singular interview instead. Participants also will be provided a pseudonym to further ensure anonymity within the study.

5. Confidentiality for focus group participants is limited due the researcher having no control over whether or not participants of focus groups will discuss the information, though not sensitive in nature, outside of the study. Focus group participants will be informed of this fact, but will be encouraged to honour the confidentiality of other participants nonetheless. They also will be assured that the researcher will do everything in her power to maintain confidentiality.

6. My senior supervisor, Dr. Ted Palys, will have access to the tapes and transcriptions to verify the interviews and ensure the transcripts are properly anonymized. Contact: [redacted]@sfu.ca or 778-[redacted]

7. Any complaints/concerns should be directed to Dr. Jeff Toward, Director of the Office of Research Ethics, at [redacted]@sfu.ca or 778-[redacted]

8. The option for the participants to be further contacted by the researcher. This option is due to the possibility of a follow-up interview with any added questions I may have that relate to the initial interview or focus group. Focus group participants will not need to engage in another focus group discussion; a singular follow-up interview will be conducted specifically on their individual disclosures.
9. The School will be provided the option of receiving the study results and disseminating them.
10. I will provide my information if the participant chooses to contact me if they have any questions concerning the study and if they have any other discussion, they believe is relevant to the study.
11. In accordance with R20.01 S 5.17, I will be obtaining oral consent at the beginning of each interview/focus group from participants. Verbal consent provides a highest level of confidentiality for my participants.

Focus Group Procedure:

All focus group participants, prior to the group discussion, will be provided with information sheets summarizing the purpose of the study and discussing confidentiality and withdrawal (see Ndegwa_AdolescentInformationSheet2015-2016.docx). I will verbally review the information sheet. Due to the nature of the focus group, I will explain that, although I will maintain their confidentiality for the purpose of the study, there is no guarantee that the other participants will do the same. However, I will encourage participants to preserve the confidentiality of other participants and if they do need to discuss the study with other individuals outside of the focus group to do so in general terms. If they do have questions concerning confidentiality, I will answer them fully and honestly. Prior to recording, I will confirm with all participants their consent to participate and to be recorded.

Since focus groups offer a different dynamic to singular interviews, I will have sample questions to guide the discussion, however the interview is intended primarily to be semi-structured (see Ndegwa_InterviewSampleQuestions2015-2016.docx). I will facilitate discussion, but will allow for the free flow of conversation. If the discussions move too far away from topic, I will guide participants back to the topic at hand.

Individual Interview Procedure:

Similar to the focus group procedure, I will begin the interview process by providing the individual participant with an information sheet summarizing the purpose of the study and discussing confidentiality and withdrawal (see Ndegwa_AdolescentInformationSheet2015-2016.docx). I will verbally review the information sheet. The singular interviewee has the prerogative to discuss their interview with others, however I will stipulate that I will maintain their confidentiality for the purpose of the study. If they do have questions concerning confidentiality, I will answer them fully and honestly. Similar to the focus group, prior to recording, I will confirm with the participants their consent to participate and to be recorded.

Similar to the focus group, I will have sample questions that will guide my interview (see Ndegwa_InterviewSampleQuestions2015-2016.docx), but again the interview is in a semi-structured format.

Data Compilation and Destruction:

Both sets of interviews will be transcribed and anonymized with pseudonyms for any personal or place names. Until transcription, data will be kept on a password protected USB key. After the interviews have been transcribed, and my senior supervisor has verified the accuracy and anonymization of the transcription, the original recordings will be destroyed. The interviews do not deal with particularly sensitive information in any event, and the anonymized transcriptions will be of no risk to anyone and will be retained indefinitely.

Benefits to Participants:

Potential benefits to the participants could include an opportunity to provide individuals with an opportunity to discuss with others their views on what has become a staple of everyday life. It might offer them a broader grasp of what social media means to them. The study allows them to be introspective of why they use social media and why it holds an appeal to them on a singular level and if they are similar to others in some way. I will not be providing any monetary remuneration for this study.

Designation of Study:

Although the study will be sampling a population that is characterized as vulnerable, the study itself is best characterized as 'minimal risk'. There is no foreseeable risk to participants, as the topic in question does not concern a vulnerable area of discussion or a sensitive issue. Overall, the risk to participating is no greater than risks to their everyday life. Furthermore, with regards to working with vulnerable populations, I have a current vulnerable persons criminal record check that I will provide to the school administrators (see Ndegwa_CriminalRecordsCheck2015-2016.pdf.)

[1] N.B: If the withdrawal of any participant during or after interviews or focus groups affects the data collected, this will be noted as a minor limitation to my study.

2016s0087

Appealing to the Masses: The Allure of Social Media

Principal Investigator: Anna Ndegwa, Graduate Student, School of Criminology

Faculty Supervisor: Dr. Ted Palys, Professor, School of Criminology

Project Number: 2016s0087

Study Objectives:

There are over 2 billion social media users worldwide. Their ease of use, convenience and the services they provide have become indispensable to users, but at what price? Theorists such as Zuboff [1] describe social media as the epitome of the contemporary surveillance economy, where terms of service establish that, in exchange for use of the platform, individuals supply personal information that becomes the property of the platform, and which the site can then aggregate and sell to other corporations, or simply use internally to personalize the ads you are offered, thereby increasing your likelihood of clicking on an ad, with each click contributing to the wealth of the social media platform.

In a previous study, I focussed on *how* individuals manage their social identities – their presentation of self – on social media. My results indicated that although individuals understood the loss of privacy their sharing of information allowed, and would often try to circumvent this, they also accepted that they have no control how their content is disseminated once uploaded; despite being identifiable and often involving intensely personal information, the terms of service make clear the information, once posted, and sometimes even after being ostensibly "deleted," is the property of the platform and not the user. The current study strives to find out more about *why* users continue to use these sites if lack of control is the underlying caveat.

Study Design:

Research Question: The proposed research will study users' perception of these sites and the fascination they and other users have with these sites. Specifically, my research question is as follows: *What exactly is the appeal of these sites that users accept an agreement that holds them at a disadvantage?*

Sample: University students are a highly appropriate sample for this research. Students are young adults, have grown up in a digital world, and it is rare to find anyone of university age who is not connected to more than one social media site (social media sites include platforms for the exchange of personal information with one's defined community of contacts or "friends," e.g., Facebook, Twitter, Instagram, Snapchat). There will be at least 3 focus groups and up to 10 one-on-one interviews conducted. The focus group groupings will be dependent on the availability of interested parties.

[1] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30,* 75-89.

i. If the interview has yet to be transcribed, I will destroy the recordings (i.e. delete electronic copies) and any notes made from the interview will be shredded securely.

ii. If the interview has been transcribed and audio recordings destroyed forthwith, I will shred both transcripts and notations from the interview securely.

b. If the participant was part of a focus group:

i. If the focus group has yet to be transcribed, I will transcribe the focus group but leave out instances where the participant speaks. I will then destroy the audio recordings, as is procedure.

ii. If the focus group has been transcribed:

1. I will shred any initial hard copy transcriptions of the focus group interview

2. I will review the electronic copy transcription of the focus group interview, remove every instance of speech of the participant, and proceed with the version excluding their participation.

4. That all data will be kept in a secure off-campus location known only to me, and all audio recordings will be destroyed once transcribed to ensure confidentiality. Moreover, all electronic versions of transcriptions will be documented within a password-protected document. I will be asking participants if they consent to be recorded prior to the start of the interview as well as within the recorded interview. If participants choose not to be recorded, I will record their interview using notations in a Word document. I will make this document an encrypted password-protected document to maintain confidentiality. Difficulty will occur if a focus group participant does not consent to being recorded. As such, it may not be prudent for them to be a part of such a discussion if other participants have consented to being recorded. Thus, if a focus group participant does not consent to being recorded at the time of the focus group discussion, I will ask the participant to consent to a one-on-one interview instead. Participants also will be provided a pseudonym to further ensure anonymity within the study.

5. Confidentiality for focus group participants is limited due to the researcher having no control over whether or not participants of focus groups will discuss the information, though not particularly sensitive in nature, outside of the study. Focus group participants will be informed of this fact, but will be encouraged to honour the confidentiality of other participants nonetheless. They also will be assured that the researcher will do everything in her power to maintain confidentiality.

6. My senior supervisor, Dr. Ted Palys, will have access to the tapes and transcriptions to verify the interviews and ensure the transcripts are properly anonymized. Contact: [redacted]@sfu.ca or 778-[redacted]

7. Any complaints/concerns should be directed to Dr. Jeff Toward, Director of the Office of Research Ethics, at [redacted]@sfu.ca or 778-782-6593
8. The option for the participants to be further contacted by the researcher. This option is due to the possibility of a follow-up interview with any added questions I may have that relate to the initial interview or focus group. Focus group participants will not need to engage in another focus group discussion; a singular follow-up interview will be conducted specifically on their individual disclosures.
9. The option to provide their contact information to receive study results. If participants are amenable, they can provide their information or contact me separately through the email I provide. Any contact information provided will remain confidential. There will be no identifying information provided other than the contact information they choose to provide.
10. I will provide my information if the participant chooses to contact me if they have any questions concerning the study and if they have any other discussion, they believe is relevant to the study.
11. In accordance with R20.01 S 5.17, I will be obtaining oral consent at the beginning of each interview/focus group from participants. Verbal consent provides a highest level of confidentiality for my participants.

Focus Group Procedure:

All focus group participants, prior to the group discussion, will be provided with information sheets summarizing the purpose of the study and discussing confidentiality and withdrawal (See Ndegwa_InformationSheet2015-2016.docx). I will verbally review the information sheet. Due to the nature of the focus group, I will explain that though I will maintain their confidentiality for the purpose of the study, there is no guarantee that the other participants will do the same. However, I will encourage participants to preserve the confidentiality of other participants and if they do need to discuss the study with other individuals outside of the focus group to do so in general terms. If they do have questions concerning confidentiality, I will answer them fully and honestly. Prior to recording, I will confirm with all participants their consent to participate and to be recorded.

Since focus groups offer a different dynamic to singular interviews, I will have sample questions to guide the discussion, however the interview is primarily semi-structured (See Ndegwa_InterviewSampleQuestions2015-2016.docx). I will facilitate discussion, however, I will allow for the free flow of conversation. If the discussions move too far away from topic, I will guide participants back to the topic at hand.

Individual Interview Procedure:

Similar to the focus group procedure, I will begin the interview process by providing the individual participant with an information sheet summarizing the purpose of the study and discussing confidentiality and withdrawal (see Ndegwa_ InformationSheet2015-2016.docx). I will verbally review

the information sheet. The singular interviewee has the prerogative to discuss their interview with others, however I will stipulate that I will maintain their confidentiality for the purpose of the study. If they do have questions concerning confidentiality, I will answer them fully and honestly. Similar to the focus group, prior to recording, I will confirm with the participant their consent to participate and to be recorded.

Similar to the focus group, I will have sample questions that will guide my interview (See Ndegwa_InterviewSampleQuestions2015-2016.docx), but again the interview is in a semi-structured format.

Data Compilation and Destruction:

Both sets of interviews will be transcribed and anonymized with pseudonyms for any personal or place names. Until transcription, data will be kept on a password protected USB key. After the interviews have been transcribed, and my senior supervisor has verified the accuracy and anonymization of the transcription, the original recordings will be destroyed. The interviews do not deal with particularly sensitive information in any event, and the anonymized transcriptions will be of no risk to anyone and will be retained indefinitely.

Benefits to Participants:

Potential benefits to the participants could include an opportunity to provide individuals with an opportunity to discuss with others their views on what has become a staple of everyday life. It might offer them a broader grasp of what social media means to them. The study allows them to be introspective of why they use social media and why it holds an appeal to them on a singular level and if they are similar to others in some way. I will not be providing any monetary remuneration for this study.

Designation of Study:

The study is best characterized as 'minimal risk'. There is no foreseeable risk to participants, as the topic in question does not concern a vulnerable area of discussion or a sensitive issue. Overall, the risk to participating is no greater than risks to their everyday life.