

**Faculty of Humanities
Department of Internet Studies**

**Privacy in the Age of Facebook: Discourse, Architecture,
Consequences**

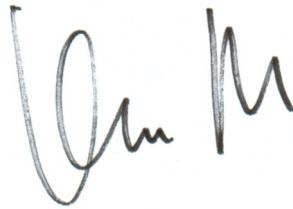
Katherine Sarah Raynes-Goldie

**This thesis is presented for the Degree of
Doctor of Philosophy
of
Curtin University**

January 2012

University Declaration

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgment has been made. This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

A handwritten signature in black ink, appearing to be 'J. M.', is written over a faint, light gray rectangular background.

Signature:

Date: January 31, 2012

Abstract

Privacy in the Age of Facebook: Discourse, Architecture, Consequences

Katherine Sarah Raynes-Goldie

Doctor of Philosophy, Internet Studies

Curtin University, Australia

Dr. Helen Merrick, Supervisor

Dr. Matthew Allen, Co-Supervisor

Dr. Philip Moore, Associate Supervisor

Most academic and journalistic discussions of privacy on Facebook have centred on users, rather than the company behind the site. The result is an overwhelming focus on the perceived shortcomings of users with respect to irresponsible privacy behaviours, rather than an examination of the potential role that Facebook Inc. may have in encouraging such behaviours. Aiming to counterbalance this common technological-deterministic perspective, this thesis deploys a multi-layered ethnographic approach in service of a deep and nuanced analysis of privacy on Facebook. This approach not only looks at both the users *and* creators of Facebook, it examines Facebook Inc. in the context of historical, cultural and discursive perspectives. Specifically, this thesis details how the company's privacy policy and design decisions are guided not simply by profit, but by a belief system which encourages "radical transparency" (Kirkpatrick, 2010) and is at odds with conventional understandings of privacy. In turn, drawing on Fiske's model of popular culture, users "make do" with the limited privacy choices afforded them by the site, while at the same time attempting to maximise its social utility. As this dynamic demonstrates, Facebook Inc. plays a critical, yet often overlooked role in shaping privacy norms and behaviours through site policies and architecture. Taken together, the layers of this thesis provide greater insight into user behaviour with respect to privacy, and, more broadly, demonstrate the importance of including critical analyses of social media companies in examinations of privacy culture.

Acknowledgements

As I reflect on my experience over the past few years, there are two aphorisms that come to mind. First, we plan and the universe laughs. And second, more than anything else, a PhD is about survivorship.

In addition to the rigour and challenge that already comes with a PhD, the universe kept throwing extra personal challenges at me. Sometimes I didn't know how I would finish. I could not have made it through, with my sanity (mostly!) and health intact, without the incredible support of my supervisors, family and friends. In particular, I am eternally grateful to Dr. Helen Merrick, for not only being an incredibly supportive, encouraging and inspiring supervisor, but also for being a wonderful friend who could always restore my sanity by having me over for european board games and a good chat. I'm equally thankful to Dr. Matthew Allen, who encouraged me to do a PhD all those years ago. Through all my obstacles, Matt was an amazingly understanding and supportive supervisor who continually pushed me to do excellent work. I am also grateful to have had the guidance of Dr. Philip Moore, a fellow Canadian downunder, under whose gentle and wise direction (and many flat whites at Gino's) I became an anthropologist.

I am indebted to everyone at Ryerson University's EDGE Lab in Toronto, in particular lab director Dr. Jason Nolan who adopted me into the lab as a Research Associate, giving me a quiet space to work (when I needed it most) and amazing people to brainstorm with, such as Melanie McBride and Noah Keneally (who deserves a special thanks for his smiles, encouragement and boundless positivity). Some of my key breakthroughs in this project came about thanks to working with Jason, who always got me thinking about things in a different way.

In addition to the amazing academic support I received, I am thankful to a number of individuals who took care of the rest of me. First and foremost, my dear friend, teacher, and healer, Martin Bogusz, whose selflessness, care and support got me through some of the toughest and most trying times over the past few years. I must

also thank my sister Alex Raynes-Goldie and Anne Leishman for showing me the awesomeness of yoga, which was one of the only things that kept me going towards the end of this project; Allan McSevich and Simone van Hattem, for showing me around downunder and being kindred spirits; Joy Scott, for supporting my family and whose endless smiles and laughter made my grandma a very happy lady; Stefanie Carmichael, a dear friend whose encouraging dispatches from the world's most dangerous places (plus Thailand) kept me motivated and smiling; and Margaret Maitland for being a friend to the end, Skype thesis buddy, and for never asking me when I was going to be finished. And last, but not least, my parents: Dr. Raymond Goldie whose own ethnographic work, *Inco Comes to Labrador*, helped me to learn how to become an anthropologist myself, and my mum, Jo-Anne Raynes, who saved me from an eleventh hour disaster. Twice.

I'd also like to thank Dr. Elaine Tay, for teaching me how to teach; Dr. Stewart Woods for his advice and guidance (and numerous sanity preserving eurogame sessions); Dr. Richard Forno for Twitter-enabled commiseration and encouragement; Delia Giggins, for her kindness and personal support. I owe a big thank you to Lindsay Shaddy and Cynthia Messenger for their support and guidance so early in my career, as well everyone else who supported, encouraged and inspired me throughout this process: Dr. Michele Willson, Dr. Alexandra Bal, Dr. Alice Marwick, Dr. Chu Chow, Christina Kostoff, David Fono, Claire Buré, Helen Li, Luke Walker, Pemma Muzumdar and Jaime Woo and everyone who participated in my research. I should also thank Shane Cusson, for accidentally inspiring me.

Finally, I would like acknowledge the financial support I received during the development of this thesis. First, for the grant graciously provided by the Center for Information Policy Research at the School of Information Studies, University of Wisconsin–Milwaukee which enabled me to present part of this thesis at the 2009 Association of Internet Researchers Annual Conference. I am also grateful to Cyber-surveillance in Everyday Life Workshop at the University of Toronto and the Office of the Privacy Commissioner of Canada for funding the development and presentation of parts of this thesis.

Table of Contents

<i>University Declaration</i>	i
<i>Abstract</i>	ii
<i>Acknowledgements</i>	iii
<i>Table of Contents</i>	v
Introduction	1
Summary	5
Chapter Summary	6
1 Methods and Rationale	11
Youth, the Privacy Paradox and Technological Determinism	11
Research Methodology	20
The Field	37
2 From ARPANET to Social Media	39
Brief History of the Internet	41
A Brief History of SNS	50
Internet Scholarship	54
Conclusion	59
3 Privacy, Surveillance & Social Network Sites	60
Understanding Contemporary Privacy Issues	62
Literature: Privacy, Youth and SNS	71
Framework: Contextual Integrity and Social Privacy	80
4 Opening Facebook	85
Facebook: the Company	86
Facebook: the SNS	90
The Evolution of Facebook	94
Privacy Architecture, Policies and Concerns	103
Conclusion	107
5 The History and Origins of the Discourse of Facebook	109
Overview	111

Technological Problems, Technological Solutions	112
1940s-1970s: Cybernetics	114
1960s and 1970s: The New Communalists and the Whole Earth Catalog	125
1980s and 1990s: Neoliberalism, Personal Computers and Virtual Communities	129
2000s: Cybernetic Totalism, Transhumanism and Web 2.0	137
Conclusion	144
6 Radically Transparent Sociality & the Architecture of Facebook	145
Mark Zuckerberg and Radically Transparent Sociality	148
Monetising Moral Goods	152
Case Study: Towards a Culture of "Openness and Authenticity"	157
Case Study: Friendship and Profiles	164
Rhetoric and Deployment	169
Conclusion	172
7 Radically Transparent Sociality in Everyday Life	173
Introduction	174
Theoretical Frames	176
Friendship	178
Lifestreaming	185
Loss of Identity Control	189
Creeping	191
Context Collapse	196
Management and Resistance	204
Conclusion	207
8 Rethinking Privacy in the Age of Facebook	208
Limiting Factors	210
Social privacy	216
Conclusion	223
Conclusion	226

<i>Appendix</i>	223
<i>Bibliography</i>	235

Introduction

In the spring of 2008, something new was happening in Toronto. As the ice and snow were melting and the air was getting warmer, Facebook was becoming a daily habit for many Torontonians. While not a revolution, Facebook's popularity demarcated an important gathering of momentum around the embedded, everyday use of the internet by individuals from across the demographic spectrum. More revolutionary, perhaps, was the privacy implications for the millions that would share their daily activities and personal communications through Facebook.

Starting around 1995, the internet began a swift ascent into popular awareness and usage (Turner, 2006). However, for a number of technological, social and cultural reasons, the spheres of online and offline were, relative to today, only slightly overlapping. But the late 2000s, the internet -- once considered solely the domain of mal-adjusted, socially awkward basement dwellers -- was becoming a routine part of the everyday social lives of Torontonians from all walks of life, basement dwelling or otherwise. As well as becoming more "normal" during this period, the internet also became increasingly physically and socially embedded. In Toronto, Facebook was an important part of this process.

Also beginning around 1995, references to the web began to appear in the physical world. Progressively, URLs were more commonly seen on delivery trucks, restaurant menus or television commercials. In the same manner in 2008, offline references to Facebook became apparent across Toronto. Mobile phone providers proudly proclaimed that access to Facebook was available on their latest devices. Smart Set, a popular women's clothing chain widely promoted its "fashion cubes" Facebook application. Some of Canada's banks followed suit, offering financial tools and advice through their newly launched Facebook applications. A walk through one of the city's university libraries usually revealed Facebook on multiple computer screens. References to Facebook could be regularly heard in conversations on the street or in bars or restaurants. One of Toronto's colleges even spoofed Facebook for its 2008 "Future of Learning" campaign. The apparent popularity of Facebook among Torontonians was also reflected in the quantitative data. In 2008, Facebook's second largest region-

al network was Toronto, right after London, UK. According to Facebook Inc.'s Canadian headquarters, by 2011, nearly half of all Canadians were on Facebook (Breikss, 2011). The mass uptake of Facebook in Toronto was an early glimpse of what would soon happen to the rest of the North America, and eventually most of the English-speaking developed world.

The popularity of Facebook during this time represented an important development in a larger, global trend. In less than twenty years, the internet had gone from a relatively obscure computer network, to mutually embedded in everyday life in the developed world (Haythornthwaite & Kendall, 2010, p. 1083). Relative to the first two decades of the 21st century, the internet of the 1980s and early 1990s was both logistically and discursively apart from physical reality. It was unusual to use the internet everyday and most people did not understand what it was or how it worked (Kessler & Shepard, 1997, p. 114). Indeed, what was once considered a "strange and uncharted place" inhabited by academics, gamers, government folk, nerds and assorted outsiders (Kessler & Shepard, 1997, p. 118), or worse still -- junkies, addicts and recluses (Baym, 2010a, p. 46) -- has now become a routine part of Western life. Nancy Baym, professor of Communication Studies and co-founder of the Association of Internet Researchers calls this process the "domestication" of technology (Baym, 2010a, p. 24).

Discursively, social media, especially social network(ing)¹ sites (SNS) like Facebook, exist in contrast from the popular media portrayals of the internet from the 1990s. Facebook users are not characterised as strange computer nerds with clandestine online lives and friends they have never met offline. Instead, users employ their "real" identities to seamlessly interact with people they already know in person. Relationships and activities are augmented through Facebook. Invitations to parties are sent out through Facebook, and photos of are posted in real time on mobile phones. Both practically and discursively, the use of Facebook has been accepted as a normal means of social interaction -- an acceptance that has likely contributed to the domes-

1. There is still debate about this term which I will explore in Chapter 2.

tication of the internet more broadly. At the time of writing, Facebook had 750 million users worldwide (Carney, 2011) and was the subject of an Oscar nominated film *The Social Network*, starring former boy band member Justin Timberlake and scored by Trent Reznor of *Nine Inch Nails*. Understandably, it is now difficult to conceptualise the internet as a domain solely for computer nerds. In this way, Facebook has been an important contributing factor to the domestication of the internet as an everyday social practice as well as facilitating a greater overlap of the online and off-line spheres.

An episode of *Nurse Jackie* (2011) from that same year serves to demonstrate this point. One of the narratives of the episode in question revolved around one of the main characters, Fitch Cooper, using Facebook on his iPhone throughout his day at work. Using the iPhone Facebook app, Cooper finds an old girlfriend. During his conversations with other staff, Cooper uses his phone to show pictures of her while he is talking about her. Throughout the episode he receives Facebook messages from her through his phone. Cooper later mentions that he is on Facebook to a patient, and she sends him a friend request after he leaves the room. Cooper then tracks her down in the hospital and says "I wanted to accept your friend request in person." He then holds up the phone and accepts it as she watches. The episode is a very literal portrayal of how SNS augment and extend existing relationships.

Perhaps the most important consequence of the internet's domestication has been an increasing assortment of digital privacy threats faced by an ever growing number of users. With these threats have come escalating public, academic and journalistic concern around online privacy -- a concern which had been mounting since the 2000 (Allen, 2000, pp. 1180-1181; Dourish & Anderson, 2006, p. 319; Rotenberg, 2011; Ryan, 2008, p. 30). One of the key components driving this concern has been Facebook Inc.'s² questionable privacy practices, which in addition to being described as radical and extreme (Dash, 2010; Kirkpatrick, 2010a), have consistently and increasingly pushed conventional privacy norms (Raynes-Goldie, 2010). Since 2009, these

2. I use Facebook Inc. to distinguish the company from Facebook the SNS.

practices have continually drawn a great deal of criticism from privacy activists and regulators (boyd & Hargittai, 2010). In 2010, likely buoyed by concern around Facebook's privacy practices, digital privacy had become a major political and social issue in the United States (Rotenberg, 2011), with hundreds of newspaper articles and television reports covering the issue (boyd & Hargittai, 2010).

A common theme in both journalistic and academic coverage of online privacy to date has centred on the seemingly ignorant privacy attitudes and activities of young SNS users. In these accounts, one finds an implication that youth are privacy unconcerned or unaware simply because they are young. Such an implication was especially apparent in early accounts of MySpace, which rose to popularity with teenage users around 2006 before being overtaken by Facebook a few years later.³ Academically, this negative conception of youth privacy attitudes is best summarised in social computing professor Susan B. Barnes' privacy paradox. In Barnes' definition, "adults are concerned about invasion of privacy, while teens freely give up personal information" (Barnes, 2006). Broadly speaking, the privacy paradox describes an apparent discrepancy between privacy concerns and privacy behaviours (Utz & Krämer, 2009), which is not always specific to youth. As Helen Nissenbaum (2010) puts it "people appear to want and value privacy, yet simultaneously appear to not value or want it" (p. 104).

Another assumption running through these narratives is that SNS are only of interest to younger people. While teens and college students were the first demographic segment to integrate SNS into their everyday social lives, this adoption was preceded by adult usage. Historically, the first users of early SNS such as Friendster were certain segments of society, particularly subcultural groups or queer communities. danah boyd's work on the early SNS Friendster notes the early uptake of the site among of Burners (a subcultural community of people who attend the Burning Man festival in California) and gay men (boyd & Heer, 2006; Donath & boyd, 2004). Indeed, as I show in later chapters, the very first users of the internet were all adults: the re-

3. Even though MySpace and Facebook launched around the same time, MySpace reached mass popularity first in 2007, then began to lose ground to Facebook in 2009 (Stelter & Arango, 2009).

searchers, academics and engineers who created it for their own use. Further, despite the early popularity with SNS and youth, the use of SNS is quickly being adopted by adults as well.⁴ As emerging research on adult SNS users is showing, in some cases, the privacy behaviours of adults can put them at greater risk than their younger counterparts (Brandtzæg, Lüders, & Skjetne, 2010; Lenhart, 2009).

Summary

As adults begin to face similar privacy issues on SNS the explanations of youth privacy behaviours as youthful indiscretions or ignorance become problematised (Raynes-Goldie, 2011). Such an apparent disconnect serves as a launching point for this thesis. One of my initial driving questions was: "Are youth facing privacy risks because they are inexperienced or exhibitionists, or because of something else? If so, what is that something else?" This line of questioning lead me to ask: "What factors are not being considered with respect to privacy on SNS?" My first literature review for this thesis in 2007 revealed that almost all research in the field had exclusively employed user studies, while leaving SNS companies unexamined. My initial hypothesis, then, was that one of key unexamined factors was the technology being used, and the discourses behind it. Based on this, I formed my key research question: "What can be learnt about Facebook and privacy from a study that looks at *both* the company behind Facebook and its users. Specifically, what insights might be gained about the observations which lead to the privacy paradox, and more broadly, privacy for users of all ages?"

I took a different methodological approach than the majority of previous user-centric, online-only studies which implicitly treat technology as neutral. Such approaches leave unexamined motivations of social media companies and how those motivations might influence user behaviour. Informed by the models of Social Construction of Technology (SCOT) and Social Shaping of Technology (SST), I designed my study to take a recontextualised approach which examines both the users and the creators of Facebook. Since, according to SST, technology is socially embedded (Menser &

4. In 2009, 35% of American adults had a profile on an SNS site, which was four times more than 2006 (Lenhart, 2009).

Aronowitz, 1996), an equally socially embedded approach would be most appropriate. Accordingly, I deployed an ethnographic approach across a number of layers. First, I conducted a year long study of Facebook users between the ages of 20 and 30 in Toronto, Canada where I engaged in participation observations and interviews to gather data both from both physical and online interactions with and around Facebook. I then contextualised this data using archival/media research and historical textual analysis to examine Facebook Inc. My research and analysis encompassed the company's current activities as well as the historically-rooted technology culture from which it emerged.

Chapter Summary

Structurally, in line with my layered ethnographic approach, I examine Facebook and privacy using an similarly layered approach, with each layer building and extending on the last. The first layer is descriptive -- I provide a detailed overview of privacy, the internet, social network sites and Facebook with a specific focus on the perceived disconnect between privacy behaviours and attitudes amongst youth, also known as the privacy paradox. The second layer, based on archival/media research and textual analysis, is a historical overview of the technology culture of the Californian Bay Area which provided the necessary preconditions for Facebook. Critically, this layer also provides the historical lens through which privacy on Facebook can be made sensible. Accordingly, in the third layer I apply this lens to an examination of the privacy architecture and policies of Facebook. As I show, the application of this conceptual lens reveals a reflection of this technology culture within the discourse of Facebook -- a system of beliefs and values, which at its most basic level, embodies a push towards less privacy and more transparency. Often described as "radical transparency" (Kirkpatrick, 2010), it is a system of beliefs that is embedded into both the architecture and corporate culture of Facebook. The fourth layer combines participant observation and interviews with the work of John Fiske (1989) to examine the way in which 20-something users take up the use of the Facebook in their everyday lives. I show how Facebook's discursively-informed architectural choices have real life consequences for the privacy of users. Bringing everything together in the final layer, I provide a reexamination of privacy in the age of Facebook and what it means for

both youth and adults. Through this examination of the origins, manifestations and privacy implications of Facebook Inc.'s radically transparent architecture and corporate culture this thesis will show that privacy on Facebook implicates a variety of interconnected factors, choices and outcomes, thereby problematising the privacy paradox.

Chapter 1: Methods & Rationale

This chapter outlines my intellectual methods and research approach. I begin with an examination of the privacy paradox and the dominant narratives around youth and technology. Based on the drawbacks of these narratives, I propose an alternative approach based on the Social Shaping of Technology (SST) and Software Studies. In the second section of this chapter, I outline my research methodology. Overall, I argue for a recontextualised ethnographic approach that takes into account both users and developers as well as the online and offline spheres.

Chapter 2: From ARPANET to Social Media

Beginning with the early internet through until the launch of Facebook, I chart the development of the internet and social network sites in North America. I provide the history and scholarship of SNS, as well as an overview of key definitions of the term. I then contextualise this more recent research with an overview of early internet research and technological developments. Throughout the chapter, I pay particular attention to the principal factors which shaped the modern incarnation of the internet. The first of these factors is the domestication of the internet, combined with the increased overlap between online and offline identities and relationships. The second is the internet's shift as a non-commercial educational space to a commercial one. These two factors not only created the necessary conditions for the emergence of sites such as Facebook, but they also facilitated a number of privacy threats increasingly faced by social media users more broadly.

Chapter 3: Privacy, Surveillance & Social Network Sites

This chapter provides the contextual foundation for discussions of privacy and digitally mediated surveillance throughout the rest of the thesis. In the first section of

this chapter, I provide an overview of conventional models of privacy and how they are being conceptually and logistically challenged by the proliferation of digital and networked technologies. Specifically, by making them persistent, transferable, aggregateable, scalable, searchable, and cross-indexible, I show how the properties of networked technologies can make communication and personal information more prone to various forms of surveillance, thereby compromising privacy. Building on the cursory examination of SNS from Chapter 2, the second section of this chapter provides an overview of the literature for one of the key topics in SNS: privacy and youth. In response to the drawbacks of existing models as demonstrated throughout this chapter, I conclude with a privacy framework based on what I call social privacy and Helen Nissenbaum's (2010) heuristic of contextual integrity. This framework is then deployed throughout the rest of the thesis.

Chapter 4: Opening Facebook

In this chapter I chart the historical evolution of Facebook both as a company and as an social network site from 2004 until 2009, touching on the site's latest incarnation at the time of writing in 2011. Through a survey of the cultural, policy and design changes on Facebook, I provide the context for understanding how the belief systems within Facebook Inc. have shaped the site's privacy architecture over time -- a topic explored in detail in Chapter 5. Using a complaint filed against Facebook Inc. with the Privacy Commissioner of Canada as a framework, I conclude with an overview and cursory analysis of Facebook's privacy settings.

Chapter 5: The History & Origins of the Discourse of Facebook

Building on Chapter 4, Chapter 5 charts the historical development of the dominant ways in which technology, people, information and society can be put together in American technology culture. I chart how values and belief systems based on technological utopianism, cybernetics and libertarianism have co-evolved with the development of the personal computer and the internet. Overall, I show the origins of Facebook's values of openness, transparency, efficiency and authenticity -- all of which have come to shape the site's privacy design. In so doing, I provide a lens with which to make Facebook Inc.'s privacy choices and architecture sensible.

Chapter 6: Radically Transparent Sociality & the Architecture of Facebook

In Chapter 6, through archival, textual and media analysis, I show how the historically informed discourse of Facebook -- which I call radically transparent sociality -- is manifest in the revenue model, privacy architecture and policies of the site. To this end, I provide two case studies. In the first, I show how Facebook Inc. has strategically and systematically created a culture of openness on the site. In the second, I show how Facebook's Friendship feature merges social choices with privacy choices, thereby complicating both. Overall, I show how Facebook Inc. is attempting to push users into sharing more personal information with each other and with the company.

Chapter 7: Radically Transparent Sociality in Everyday Life

In Chapter 7, I connect the two previous layers of discourse and architecture with the lived experience of the participants in my ethnographic fieldwork. Drawing on John Fiske's (1989) model of popular culture, I analyse the intersection of Facebook and users as the space where users take up and negotiate openness, transparency, efficiency and connectedness within the context of their social lives and the privacy issues that ensue. I show how previously uncommon social privacy concerns, such as context collision, creeping and loss of identity management arise as a result of a disconnect between the beliefs and experiences of Facebook's users and creators. Overall, I show how the privacy challenges created by Facebook's radically transparent sociality call for a rethinking of the ways in which individuals might understand and enact privacy.

Chapter 8: Rethinking Privacy in the Age of Facebook

In this chapter, I bring together all the layers of the thesis -- the history, discourse, architecture and consequences of Facebook -- to reexamine privacy in the age of Facebook, particularly with respect to the privacy paradox. I show how radically transparent sociality might help to explain the observations that created the notion of the privacy paradox. In the first part of this chapter, building on the information presented thus far, I further analyse how a number of factors -- largely out of the hands of

users -- challenge meaningful privacy choices on Facebook. In the second part of this chapter, I further analyse social privacy both as a concept and as a privacy management strategy. In conclusion I show how, taken together, these factors suggest that the privacy paradox might not be a paradox at all.

Chapter One: Methods and Rationale

In this chapter, I present my methods and rationale. I have outlined in the introduction to this thesis the key questions which drive my interest in Facebook. As the launching point for this thesis was the privacy paradox, I begin with a deeper description and analysis of the privacy paradox and the discourses within it, particularly around youth and technology. Based on this examination, I then present my intellectual method which outlines the model by which I understand youth and technology throughout this thesis. In the second part of this chapter, I outline my research methodology, rationale, and description of my fieldsite. Overall, I argue for a recontextualised ethnographic approach that takes into account both users and developers as well as the online and offline spheres.

Youth, the Privacy Paradox and Technological Determinism

In this section, I unpack and examine youth and the related narratives of the privacy paradox and technological determinism. In order to contextualise this examination, I first provide a cursory overview of youth as SNS users, an overview which is then extended in Chapter 3. After analysing the privacy paradox and technological determinism, I conclude with an alternative perspective based on Software Studies and the Social Shaping of Technology (SST) which I use throughout my thesis.

Youth

The Commonwealth defines young people as those aged 15-29 (Commonwealth Secretariat, ND). In some countries, the upper limit of the age range can be as high as 35 (Curtain, 2001). Accordingly, in studies of youth and SNS, the term youth is generally used to describe individuals in their teens all the way up to 20-something university students. For example, in Barnes' (2006) privacy paradox study, the observations framing the study were with respect to teens, but the study she conducted was with undergraduate students. boyd's (2006a, 2007a) work on MySpace focused on teenagers, while Gross and Acquisti (2005) looked at undergraduate Facebook users.

Accordingly, as this thesis builds on and responds to this existing body of research, I use the Commonwealth definition of youth as aged 15-29.

Before delving into the privacy paradox, it is worth noting why studies on SNS and privacy thus far have primarily focused on youth. Even though such a focus implies that risky online privacy behaviours are tied to age, there is another factor that needs to be considered: it was primarily young people who were the early adopters of MySpace and Facebook (boyd, 2007a). As such, youth were not only the most obvious users to examine, they were also the first users to begin negotiating the novel privacy challenges and threats posed by social media. As adults begin to use SNS they are faced with similar challenges. Indeed, more recent research on adult SNS users shows, adults, in some areas, face greater privacy risks than their younger counterparts (Brandtzæg et al., 2010; Lenhart, 2009). Thus, even though this thesis is based on 20-something Facebook users, my findings should not be limited to youth.

Moral Panics and the Privacy Paradox

As I touched on in the introductory chapter, running through the scholarship, public opinion and mainstream discourse about youth and digital privacy, is a narrative whereby young users are responsible when their privacy is violated. In much early academic literature on the subject, responsibility was implicitly or explicitly placed on young users with respect to privacy, suggesting that users do not care about their privacy because they are ignorant or indifferent (Albrechtslund, 2008; Gross & Acquisti, 2005). As Albrechtslund (2008) describes: "many people are puzzled and appear to be almost offended by the frankness in communication and, perhaps, carelessness that some people, especially youngsters, display with regard to their personal privacy." Within this narrative is an assumption of inappropriate privacy behaviour. As such, early investigations of SNS, youth and privacy tended to focus on the motivations behind the perceived "oversharing" (Hoffman, 2009) by young people despite seemingly obvious privacy risks. Together with Albrechtslund's observation, these narratives of "today's youth" (Nissenbaum, 2010, p. 227) suggest an undercurrent of ephebiphobia, or the "inaccurate, exaggerated and sensational characterization of young people" (Hoffman & Summers, 2000, p. 2).

In the mainstream media and public opinion, this conception of youth was exemplified in the 2006 moral panic which erupted around MySpace's teenaged users (Tufekci, 2008, p. 20). The panic was largely based on the idea that pedophiles could (and were) using SNS to sexually "prey" on teenage users, who, in turn, were seen as putting themselves in harm's way by sharing far too much personal information on their MySpace profiles (boyd & Jenkins, 2006; Marwick, 2008). Some commentators at the time characterised youth as exhibitionists with questionable morals who did not appreciate the benefits of privacy (such as Samuelson, 2006). Generational and age-based discrimination runs through these accounts, which assume that youth do not care about their privacy because of their inherent ignorance or immorality. As Marwick (2008) and Baym (2010a, pp. 25-30, 41-44) show in their respective historical surveys, such fear-based narratives of youth and new technologies have a long historical precedence (for example, the telephone or comic books). Such historical examples suggest fears are based more on culturally-entrenched ageism and technologically dystopian fears and less on the reality of the situation. In contemporary discourse, these narratives can be summarised by the privacy paradox.

As I began my fieldwork, the assumption within the privacy paradox that youth were privacy unconcerned or unaware became challenged (Albrechtslund, 2008; Lampe, Ellison, & Steinfield, 2008; Livingstone, 2008; Tufekci, 2008). These studies suggested that other factors needed to be taken into account, such as the benefits of publicity, or the motivations of social media companies (Beer, 2008; boyd & Hargittai, 2010; Brandtzæg et al., 2010; Stutzman & Kramer-Duffield, 2010; Utz & Krämer, 2009). In my own initial findings from my fieldwork, which I published in early 2010, found that youth did indeed care about privacy, but in a different way (Raynes-Goldie, 2010). Despite these findings, the narrative of the privacy paradox persists (boyd & Hargittai, 2010).

Uncritical Thinking About Technology

The MySpace moral panic -- which can more accurately be described as a "technopanic" (Marwick, 2008) -- reveals a second critical narrative which serves as

a launching point for this thesis. That narrative is technological determinism. According to social media researcher Alice Marwick, technopanics have three characteristics:

First, they focus on new media forms, which currently take the form of computer-mediated technologies. Second, technopanics generally pathologize young people's use of this media, like hacking, file-sharing, or playing violent video games. Third, this cultural anxiety manifests itself in an attempt to modify or regulate young people's behavior, either by controlling young people or the creators or producers of media products (Marwick, 2008).

As such, in their focus on new media forms, technopanics are inherently technological deterministic. That is, the source of the perceived moral decline of young people can solely be attributed to a new technology (Baym, 2010a, p. 41). Broadly, technological determinism is a belief about the relationship between technology and society whereby technology is believed to be the sole agent of human progress and change, regardless of any other factor in society. In this mode of thought, the influence of technology is a one way street: technology changes humanity (Baym, 2010a, p. 24). Technological determinism can manifest in two extremes -- utopian or dystopian. While the utopians argue that a new technology will bring about positive social change, the dystopians argue it will degrade society. Such immoderate responses to new technologies are not unique to digital technologies. One can find examples of this way of thinking as far back as the ancient Greeks, who experienced their own technopanic in response to the invention of the alphabet. In this ancient technopanic, they feared their oral tradition would be destroyed (Baym, 2010a, p. 25; Ong, 1982).

Technological determinism is not only a popular narrative within mainstream discourse (Smith & Marx, 1994), it also informs the way inventors, scientists and technologists conceptualise and described the technologies which they create. From the 1940s until the present day, the common thread running through the varied elements of American technology culture -- particularly that of Silicon Valley and the Californian Bay Area -- has been technological determinism, especially of the utopian varie-

ty. For example the 1990s saw a popular technological utopian view whereby the internet, by its very nature, could "level organizational structures, render the individual more psychologically whole, or drive the establishment of intimate, though geographically distributed, communities" (Turner, 2006, p. 3). This technologically utopian way of thinking can also be seen at Facebook Inc., where CEO Mark Zuckerberg apparently believes his site is making the world a better place (boyd, 2010; Lacy, 2008; Smith, 2007). Like Zuckerberg, many Silicon Valley technologists see what they create as having the power to overcome social, economic and political restraints to change the world for the better.

A related approach to technological determinism is technological neutrality. In 1980, political science professor Langdon Winner wrote "In our accustomed way of looking at things like roads and bridges we see the details of form as innocuous, and seldom give them a second thought" (Winner, 1980, p. 123). This is perhaps why, for almost 50 years, Robert Moses was able to embed his racist and classist beliefs into the public works of New York City. From the 1920s to the 1950s, Moses was the "master builder" of the city's infrastructure, which included roads, parks and bridges (Winner, 1980, p. 123). As Winner details, Moses designed many of his overpasses to be too low for buses, thereby preventing users of public transit -- who tended to lower income or racialised minorities -- from accessing many parts of the city. As the case of Robert Moses exemplifies, technology is not neutral. To varying degrees, technologies of all kinds reflect the ideologies -- both good and bad -- of their makers, and in turn, the social and cultural milieu which their makers inhabit. And yet, just like roads and bridges -- which are so domesticated that they are no longer thought of as technologies -- computing and communication technologies are treated as neutral. The more a technology becomes domesticated, the more innocuous and neutral it may seem (Baym, 2010a, p. 24).

While technological neutrality is not the same as technological determinism, they are similar in that both approaches tend to hamper critical reflection or investigation regarding the role of technology in social, cultural or economic change. In taking a technologically neutral perspective, the role of designers and their systems of belief -- such as technological determinism itself -- is left unchallenged and unexamined. In-

deed, given the influence on technological determinism on both the narratives around, and design of, new technologies, an approach that can unpack, question and understand the consequences of those technologies is essential. Such an approach is especially necessary with respect to understanding youth, Facebook and privacy. As I show in this thesis, the privacy policies and architecture of Facebook has been largely informed by technological utopianism which, in turn, has created unexpected privacy challenges for Facebook users. A technologically neutral approach would likely miss such a vital factor in understanding digital privacy threats and behaviours.

Despite this need for a critical examination, academic research on internet technologies often embodies an implicitly technological neutral stance. Software studies theorists such as Matthew Fuller (2003, p. 16) have noted that internet studies, cultural studies and related disciplines have been "held back from invading their conceptual domains of software by the myth of its own neutrality as a tool." Even though theorists such as Donna Haraway, Langdon Winner and Ed Kranakis have demonstrated that technology is politically, economically and socially shaped, critiques of SNS from this perspective remain few and far between.

This technologically neutral approach is reflected in an overwhelming research focus on users, especially in the study of SNS. Perilously, for studies of SNS and privacy, this method tends to overlook the role of SNS companies and the ideologies they both consciously and unconsciously embed in the technologies that they create (Beer, 2008). The result is that, in cases where privacy has been violated or where norms of privacy appear to be changing, the responsibility is often unfairly placed on users. Such one sided, user-focused studies tend to emphasise the "shortcomings on the part of the user" while overlooking the potential impact of discourses embedded in technology. In a sense, these arguments about youth are age-based determinism. (Albrecht, 2008) This one-sided perspective persists, even when users take actions to try and regain lost control. As a communication studies professor Nancy Baym (2010b, p. 399) has observed, the struggles over privacy and intellectual property between users and the individuals behind proprietary sites such Facebook have been "all but ignored in scholarship."

Indeed, Barnes' (2006) *A Privacy Paradox: Social Networking in the United States* is representative of the implicitly technological neutral, user-focused analyses. Writing about marketing, privacy and the safety of teenagers, Barnes critically notes that the purpose of SNS is to support information flow and "to advertise and promote brand recognition in consumers, especially teenagers." She also notes in a separate section that the illusion of privacy on SNS may partially be due to the sign-in feature. Despite these two observations, a clear link is not made between economic goals of the SNS providers and the privacy design of the site itself. In asking why there are privacy issues, the analysis stops at an observation of *how* the technology is designed, rather than *why* it was designed that way. Salient questions -- such how a revenue model based on the monetisation of personal information might shape the privacy design of an SNS -- are not being asked. Barnes' analysis, like much of the early literature in the field, does not problematise the social media design process or its critical role in privacy outcomes.

Ultimately, Barnes's technologically neutral approach results in a conclusion which portrays youth as privacy unconcerned or unaware. However, even research which has criticized this negative portrayal of youth often reflects some degree of implicit technological neutrality by focusing on users. danah boyd, one of the first SNS researchers, conducted groundbreaking work on SNS use among teenagers in the United States. She was one of the first to refute the negative portrayal of SNS use among teens, arguing that there are actually many benefits for youth who use MySpace and Facebook (boyd & Heer, 2006; boyd & Jenkins, 2006; boyd, 2006a). boyd has also argued against the belief that runs through Barnes' privacy paradox which holds that youth do not care about privacy (boyd & Hargittai, 2010). While this is an important issue, her approach focuses on the use of SNS rather than their production and design and the ideologies embedded within them. In a response to boyd and Nicole Ellison (2008), David Beer (2008) argues that such a focus on users "perpetuates an agenda" which frames SNS as democratic empowering spaces while ignoring the ideological influence of capitalism. In so doing, such approaches miss critical issues such as surveillance, privacy and equal access.

Ryan Bigge (2006) and Fred Scharmen (2006) further demonstrate how such user-focused approaches are problematic. While boyd identifies the political issues working against youth access to SNS, they argue, she misses the threats to youth posed by the discourses embedded in the design of the SNS themselves. As Bigge points out, boyd's work with Henry Jenkins (2006) does not ask question why it is so critical that youth have access to SNS, thereby "[eliding] the issue of when or why MySpace or Facebook membership became a necessity, rather than an option" (Bigge, 2006). Similarly, Scharmen states: "Boyd's central thesis is that teenagers are moving to MySpace and other online communities to produce identity and interact with each other publicly and privately in a venue that is outside of the control that adults exercise in the real space of a teenager's everyday life. I would argue that it is exactly *control* in the Deleuzian sense that these teenagers and other users of Myspace are submitting to" (Scharmen, 2006). As Bigge and Scharmen argue, boyd's work on teens and SNS, as with much of the prevailing research, does not ask the question of "why?" when it comes to the technology being examined. For example: why does MySpace have the features it does, or why does Facebook handle privacy in a certain way?

SCOT, SST and Software Studies

As the arguments of Beer, Bigge and Scharmen suggest, there is a need for internet studies and related disciplines to more commonly avoid technological neutrality by adopting approaches which examine the developers and designers, rather than just the users of a technology. Such an approach is necessary for understanding privacy in the digital age, particularly when the revenue models of many social media companies are at odds with conventional privacy values or when their privacy settings are informed by technological utopianism. For these reasons, my thesis examines Facebook both in terms of how it is used, as well as why and how it was made. In this section I provide an overview of the various alternatives to technological neutrality, concluding with the approach which I deploy in this thesis.

Perhaps the most well known alternative to technological determinism is the Construction of Technology (SCOT) model. Proponents of the SCOT approach argue that social contexts shape the creation of new technologies. These contexts include socio-

cultural influences, such as norms around gender and race, to monetary influences such as government or commercial interests and competitors (Baym, 2010a, pp. 39-40).

However, Winner (1993) shows that the SCOT approach also has a number of drawbacks. While SCOT examines the impact of social, economic or cultural factors on the *creation* of new technologies, it does not examine the *consequences* in those same areas. Likewise, SCOT focuses on immediate factors which influence the creation of a new technology, rather than historical ones. Such a narrow temporal scope does not take into account historically rooted belief systems, such as those that I examine in this thesis. Most critically, SCOT does it look at how individuals might be affected by a new technology. For example, SCOT ignores the role of users, who have some degree of control in how they actually take up a technology, often in ways unintended or undesired by its designers. Even though this appropriation by users or "function creep" (Raynes-Goldie & Fono, 2009, p. 205) can influence future iterations of that technology, it is a dynamic left unexamined by SCOT. Finally, Winner notes that SCOT does not take a moral or ethical stance in evaluating technology, which makes it prone to elements of technological neutrality.

Perhaps ironically -- since he himself was a technological determinist -- Canadian media theorist Marshall McLuhan provides a useful perspective here: "We change our tools and then our tools change us" (Onufrijchuk, 1993). Matthew Fuller's software studies -- the application of cultural studies to software -- takes a similar approach by acknowledging the relationship between technology and society. In so doing, his approach addressees some of the drawbacks of SCOT. Characterised by the work of Geert Lovink, Lev Manovich and of course Fuller himself, software studies is an emerging interdisciplinary field. The work of Manuel Castells, Steve Woolgar, Lawrence Lessig and N. Katherine Hayles are also reflective of this approach in their respective fields (Truscello, 2006). In his *Behind the Blip* (2003), Fuller outlines an approach which takes into account the iterative design process commonly used in contemporary software development. Software studies advocates for a perspective which examines the production of software in a manner which recognises the mutually influential relationship between its creation and use (Fuller, 2003). Through the

examination of the many layers of software and its production: the code, the features and interfaces, the design progress, and the organisational structure of the company producing it, Fuller deploys software studies to reveal how pieces of software -- such as word processors or search engines -- both reflect and influence different aspects of life, such as one's work practices or the act of writing.

Fuller's approach is similar to another model of the society/technology relationship called the Social Shaping of Technology (SST). In this model, technology, society, culture and economics are mutually implicative and influential. Unlike the linear causality of technological determinism, the SST model proposes that there are choices (conscious or otherwise) which are made when during the technology creation process. How these choices are made are influenced by society, and in turn, the resulting technologies have an influence on society (Williams & Edge, 1996). It is in this decision making process where ideologies become embedded in technologies, as evidenced by Robert Moses' racist and classist overpasses. Given the balanced and holistic approach of software studies and SST, it is these models which I deploy in my thesis project, both as methods to unpack technological determinism as well as broad lenses with which to examine my methodological approach. Taken together, the prevailing narratives of privacy paradox and technological determinism -- left unexamined by technologically neutral approaches -- call for a methodology that looks at users of SNS as well as the SNS companies themselves.

Research Methodology

In internet studies and related disciplines thus far, there has been a strong research and methodological focus on "highly virtual, online only experiences" (Haythornthwaite & Kendall, 2010, p. 1083). This early literature, however, generally is not reflective of the true nature of the online and offline spheres, which have always experienced a degree of overlap. Instead, the literature reflects an attitude among internet users and the public more broadly. As Baym (2010a, p. 30) describes, the use of the terms "real" and "virtual" to describe the offline and online worlds reflects a popular "deep seated presumption" about mediated sociality. Since, as I show in the next

chapter, there was empirical and logistical evidence to support this divide, scholars tended to agree.

Today, the offline and online spheres have become mutually overlapping to a degree where it is difficult to see where one stops and the other begins. Moreover, the common conception of the internet is no longer one where the online sphere is virtual and apart from the everyday. Smartphones, tablets and other internet-abled mobile devices have meant that the use of social media often takes place outside one's home, as an embedded part of everyday life. One's online identity, particularly on SNS, is commonly the same as one's offline identity, and is contextualised by one's job, friends, education and so on. These changes problematise these traditional internet research methodologies which inaccurately reinforced a firm delineation between online and offline, where the "real" everyday world is set apart from and the "virtual."

Such methodologies are particularly unsuited to the study of SNS, especially Facebook, which is designed to digitally augment the everyday social life of individuals in shared (offline) social networks. The physical world is the space in which Facebook is used, and thus, the site cannot realistically be understood in isolation. Studying Facebook using online-only methods removes it from its everyday social context, thereby potentially skewing findings. As David Machin (2002, p. 85) argues "human action is fundamentally social and contextual" and must be studied as such. In fact, since the early days of internet research, Canadian internet sociologist Barry Wellman has argued for a contextually embedded methodological approach in internet research (Wellman & Gulia, 1999; Wellman, 1997). Similarly, American privacy philosopher Helen Nissenbaum has applied this line of thinking to SNS. SNS, she argues, cannot be seen as having their own social contexts entirely apart from reality, rather, like the telephone, they are very much informed by the context of their use:

...one might conceive of the telephone system not as constituting a distinctive context, but as a medium for interactions occurring within diverse distinctive contexts, such as family, workplace and medical. Although of course the medium of social networking sites, generally, and design characteristics (configurations) of specific sites shape the

nature of interactions to some degree, these interactions are also governed by norms of respective social contexts and acquire significance from their occurrences within them (Nissenbaum, 2010, pp. 223-224).

Nissenbaum further underscores the need for an approach that recognises Facebook as an augmentation of physical social life, as well as within the context and discourse of its design. A methodology which fails acknowledge the embeddedness of Facebook in everyday, offline life does not just ignore one context (the offline), but the multiplicity of contexts that exist within it. Indeed, a contextualised approach is core to Nissenbaum's (2010) model of contextual integrity as a way of understanding and defining privacy violations in the age of social media ubiquity. Nissenbaum also hints at the importance of a site's design characteristics and configurations in shaping interactions. In this way, Nissenbaum's arguments further support the need for an approach that is not implicitly technological neutral.

Just as Facebook needs to be examined within the everyday context of its offline usage, that usage also needs to be studied within the context of the discourses which inform it. As Beer argued in his critique of predominant SNS research thus far:

When we ask about who are using SNS and for what purpose, we should not just think about those with profiles, we should also be thinking about capitalist interests, of third parties using the data, of the organising power of algorithms, of the welfare issues of privacy made public, of the motives and agendas of those that construct these technologies in the common rhetoric of the day (Beer, 2008, p. 526)

As Beer suggests, such an approach is particularly necessary when considering privacy and social media. Privacy and surveillance are highly politically and ideologically driven concepts and practicalities. How privacy is legally defined; how it is protected; and of course when and how it is violated can have a profound impact on individuals and societies. Within surveillance studies, the argument to examine the discursive or ideological context which inform the creation of new technologies is not a new one. Writing about surveillance technologies in 2001, Canadian surveillance researcher David Lyon argued:

When the problems of identifiable personal data arose, database designers did not immediately or automatically try to decouple data records from human identity. Why not? Because powerful economic and political interests would like to keep open the possibilities of using for secondary purposes personal data ostensibly collected for only one purpose. Recognizing those larger contexts -- the beliefs and ideologies by which organizations as well as ordinary people arrange their lives -- is vital to understanding how surveillance technologies are developed and used (Lyon, 2001, p. 26).

As I have shown, the predominant research methodologies employed in internet studies does not reflect the way the internet, especially SNS, is currently used or indeed, conceived. Facebook in particular cannot accurately be studied using online-only methodology, nor can its usage be accurately understood if individual, unconnected users are studied together. Since SNS are inherently used in the context of pre-existing social networks, studying connected individuals within those networks would likely yield more accurate results. Further still, technological determinism in internet studies continues to render invisible technological determinism and other ideologies embedded in social media. What is necessary here is the *recontextualisation* of social media in research methodologies. Facebook needs to be examined within the everyday physical and social context of its use as well as within the context of the discourses behind it. It is such a recognition that guides this thesis. Given my desire to study Facebook in a recontextualised way, I deployed a layered, ethnographic approach. For my user study I used participant observation and interviews. I then combined these findings with archival/media research and textual analysis of Facebook Inc. as well as the historical and discursive context which informed its development.

Ethnography as a Recontextualised Methodology

As an approach, ethnography is inherently about contextual and social embeddedness. In its truest form, ethnography is the study of situated meaning of a community or culture, of “situated action as it happens naturally” (Machin, 2002, p. 85). Tradi-

tionally, ethnography takes place in context -- in the natural settings where participants live and work. The ethnographer engages in participant observation in situ, rather than in asking participants to come to the researcher. In ethnography, the contexts in which the participants move through are as important as the participants and their comments and activities. Likewise, since technology is inherently socially embedded (Menser & Aronowitz, 1996), the most natural and obvious approach to the study of internet technologies, such as Facebook, is ethnographic.

It is through this contextualised approach that ethnography draws its power to bring out the hidden world, especially when ethnography is used to study technological systems such as SNS. Hine states that ethnography can "be used to develop an enriched sense of the meanings of the technology and the cultures which enable it and are enabled by it" (Hine, 2003, p. 8). Ethnography allows researchers to see how meaning is embedded, how ideologies run through systems such as Facebook and how meaning plays out. It acknowledges that the world is not found in our words, rather it is found in between our words and within our practice. It recognizes the human disposition towards knowing, without knowing what is known. As Philip Moore, one of my thesis supervisors relayed to me: "Words are not culture. They are manifestations of culture. But we can only get to the culture through the words. The important question is 'What sort of world (or system) makes these words possible?'" Through this approach, ethnography teases meaning from culture and makes sense of the world.

Another strength of an ethnographic approach is that it does not rely on words alone, or words outside of context. Self-reports can often be faulty because people are often unaware of their own internal motivations (Machin, 2002, pp. 81-82). This issue with self-reporting was evidenced in a 2006 study of Facebook usage which employed user surveys as a primary data collection tool. In this study, users reported that their own usage was drastically different from that of everyone else. Users provided socially acceptable reasons for their own use of Facebook (such as finding friends), while portraying the motivations of their peers in a negative way (such as self-promotion) (Acquisti & Gross, 2006).

Finally, as internet ethnographer Christine Hine argues in her *Virtual Ethnography*, ethnography renders problematic technologies which have become invisible through domestication, thus opening them up for enquiry (Hine, 2003, p. 64). Again, to use the words of renowned Canadian media theorist, Marshall McLuhan "We don't know who discovered water but we know it wasn't a fish. A pervasive medium is always beyond perception" (Ing, 2008, p. 3). Indeed, since social media has become pervasive, the defamiliarisation afforded by an ethnographic approach is especially critical.

Despite its strengths, however, the use of ethnography does not automatically ensure a contextualised research methodology. As mentioned, most internet research -- including those using ethnographic approaches -- has been almost exclusively online. The use of ethnography in this way has been called cyberanthropology, or the anthropology of cyberculture and computer mediated anthropology (Ryan, 2008, p. 27). As the "cyber" in name suggests, cyberanthropology is the study of cyberspace, which is, by definition, frames the internet as apart from the offline world. The early cyberanthropology of the 1980s and 1990s examined networked technologies such as MUDs, MOOs and Usenet. Sherry Turkle was one of the pioneers in this field, studying online identity formation and subcultures long before the internet became a household word (Turkle, 1997; Turkle, 2004). While Turkle's work did frame the internet as apart from the everyday (largely as a result of her focus on online fantasy/game spaces), it is important to note that she did engage in trailblazing physical participant observation of groups formed online, such as pizza parties held by Boston MUDders (Turkle, 1994).

Seminal works such as *Cybersociety, a collected volume of essays on computer networks and community* (1995) and Howard Rheingold's *Virtual Community* (2000) critically reframed cyberspace as a place where community and culture could and certainly did exist. This recognition ran counter to prior work done in the field of computer mediated communication (CMC), which framed networked communication as a communication tool which was studied on temporary networks in laboratories, rather than in the context of everyday use. While *Virtual Community* and *Cybersociety* did the important work of showing that the internet was worthy of

ethnographic study, it still reentrenched online culture as apart from everyday offline culture.

The online/offline divide in internet ethnography existed both in terms of what was studied *and* how it was studied. Especially in the early days of internet research, the core methods of data collection -- for example, participant observation and interviews -- were usually conducted entirely online. The archival nature of many internet technologies, such as Usenet, allowed ethnographers to "lurk" and study events that have happened in the past, rather than as they happen. It also meant ethnographers could get by without building a relationship with study participants. Even though the internet facilitates this form of decontextualised ethnography, cyberanthropology and internet ethnography's status as true ethnographic approaches been called into question (Hine, 2003).

Even in the early days of the internet, a methodology founded on the online/offline tended to miss the then somewhat subtle overlap between the online and offline spheres. Take, for example, friendships made between players in MOOs (Parks & Roberts, 1998), or face-to-face gatherings of people who had met on the WELL (Rheingold, 2000). These examples serve to show that while an offline/online overlap was not as apparent as it is today with Facebook, a strict divide between the "real" and the "virtual" -- indeed, even the use of such terms -- has never been entirely accurate.

Some pioneering researchers such as Nancy Baym challenged the prevailing decontextualised approach by engaging real time with participants, conducting face to face interviews and email exchanges (Baym, 1995a; Baym, 1995b). In 2000, Christine Hine, another pioneer in the field of internet ethnography, began problematising the online/offline divide. One of the core questions in her *Virtual Ethnography* was "is 'the virtual' experienced as radically different from and separate from 'the real'? Is there a boundary between online and offline?" (Hine, 2003, p. 8) She concluded that "abandoning the offline/online boundary as a principled barrier to the analysis allows for it to be traversed (or created and sustained) through the ways in which connections are assembled" (Hine, 2003, p. 62).

Hine's approach was of particular inspiration to the ethnographic approach deployed in this thesis, as was that of Daniel Miller and Don Slater. In the same year as Hine's *Virtual Ethnography*, Miller and Slater (2000) published a groundbreaking ethnography which studied the internet as situated in its particular, everyday use in Trinidad and Tobago. In their opening chapter, they proclaimed "... contrary to the first generation of Internet literature -- the internet is not a monolithic or placeless "cyber-space"; rather it is numerous new technologies, used by diverse people, in diverse real-world locations. Hence, there is everything to be gained by an ethnographic approach, by investigating how Internet technologies are being understood somewhere in particular" (Miller & Slater, 2000, p. 1).

Another groundbreaking study which influenced my approach was carried out by Keith Hampton and Barry Wellman (1999) in the late 1990s and early 2000s. The study used ethnographic methods to study Netville, Canada's first wired suburb, gathering data both online and off. Hampton lived in the suburb, just outside of Toronto, as a participant-observer for over a year. Their research was guided by a desire to study community both online and offline -- a innovative approach which, as I have shown, is still uncommon today.

More recently, Alice Marwick (2010) conducted an ethnographic study of Web 2.0 and technology culture in Silicon Valley for her PhD thesis. Even though her thesis was published after I had finished my fieldwork, her subject matter and approach were quite helpful in informing aspects of my thesis. A few years earlier, danah boyd was of the first to employ ethnographically-inspired methods to study teenage users of MySpace and Facebook (boyd, 2008c). However, given the many constraints of working with American teenagers, she notes that she was unable to be a true participant-observer (boyd, 2008c, p. 80). Instead of studying users in the field, her method used interviews across a large number of unconnected users. While such an approach gathers a large number of data points from a wide variety of users in a variety of contexts, it is not suited to capture the localised, in situ use of SNS, thereby making it difficult to examine how groups of users in a given social network use an SNS with each other.

boyd's research also calls to attention an important distinction within ethnographic approaches. An ethnography of users -- which can be used to describe boyd's approach -- can be distinguished from an ethnography of an SNS. The latter is an ethnography of a system (or culture, or space, or context) which can be deployed to expose and examine the discourses and philosophies embedded in a system, such as Facebook (as is the case in my research). A system ethnography covers all aspects of the system: users and designers, online and offline (without making an artificial distinction between the two), and the relationships between all of them. In this way, a systems ethnography addresses many of the drawbacks of earlier online ethnographic approaches.

Study Design: Users

In 2000, Hine called into question online-only data collection methods by asking:

In an offline setting, we might expect an ethnographer to have spent a prolonged period living in their field site. We would expect them to have observed, asked questions, interviewed people, drawn maps and taken photographs, learnt techniques and done what they could to find out how life was lived from the point of view of the participants...[but] how can one live in an online setting? Do you have to be logged in 24 hours a day, or can you visit the setting at periodic intervals? (Hine, 2003, p. 21)

Hine's line of questioning highlights the logistical and practical difficulties which hindered a truly embedded and contextualised ethnography of the internet in the 1980s and 1990s. Even in 2000, it still required a conscious effort and choice to be online. Users had to dial up when they wished to use the internet, and often paid by the minute or hour. Always on, unlimited internet or access- anywhere wifi were uncommon. Moreover, mobile phones did not yet offer internet access. Taken together, these factors meant that being online still required physically sitting in front of a computer. And yet, as Miller and Slater showed, it was still possible to study internet use in this way, using traditional (offline) ethnographic methods.

By 2008, Hine's question "How can one live in an online setting?" had been answered. The pervasiveness of Facebook in Toronto among young people meant that logistically, I could carry out a study in the same way that Hine had described traditional ethnographers had done it -- living in the field site; taking photographs; and asking questions. The manner in which Facebook augments everyday social and physical life meant that my participants were living a life online, just as much as they were offline. Thus, not only was a recontextualised ethnography logistically possible, it was necessary for an accurate picture of the field site. Such an approach which calls for the merging online and offline has since been supported by others (such as Rogers, 2009).

To this end, I chose a reflexive ethnographic (or autoethnographic) approach. Historically, ethnography is done from the perspective of a neutral, unbiased observer. However, my personal perspective is just as political and therefore is as biased as my participants or anyone else. In her Master's thesis which deployed autoethnography to study SNS, Jennifer Ryan (2008) argues "From the phenomenological point of view, the truth of ethnography lies in the interpretation of lived experiences, and is always partial" (p. 34). Similarly, as autoethnographer Stacy H. Jones (2005) describes, reflexive ethnographies recognize the impossibility of a "careful, faithful and authoritative cataloguing of the exotic other" and embracing of the potentials of "partial, reflexive and local narrative accounts" (p. 766).

In addition to being reflexive, my ethnographic approach was one of the system of Facebook, rather than simply just users. This meant that I was not aiming to create an exhaustive list of the specific and different ways in which people use and understand Facebook with respect to privacy but rather to delve further into the meanings behind those behaviours and what they might mean for society at large. Using archival/media research and textual analysis of the company behind Facebook, I combined specific user behaviours with the context, history and discourse of Facebook Inc. The generality that I was seeking was not a collection of specific user behaviours, but rather what those behaviours reveal about the design of Facebook and in turn, what that might mean for the future of privacy. As C. Wright Mills pointed out in *The Sociological Imagination* (1959), personal problems can often reflect on larger public

issues and help us to understand them. Put another way, the personal is the political (Jones, 2005).

Other than actual, hands on experience, one of the best ways to learn ethnography is by reading as many as possible (boyd, 2008a, p. 28). Thus, I drew both internet ethnography as well as conventional, contemporary ethnography, such as Sherman's *Class Acts* (2007); Geertz's *Deep Play: Notes on the Balinese Cockfight* (2000) and Wolf's *A Thrice Told Tale* (1992). I also drew on seminal, classic ethnographic works such as Evans-Prichard's *Witchcraft, Oracles and Magic Among the Azande* (1973).

Informed by these foundational works, I designed a contextualised, reflexive ethnography study of Facebook which examined social context, physical context, and -- combined with archival and textual research -- historical and discursive context. To accomplish this recontextualisation in my participant recruitment, I drew on the work of March and Fleuriot's (2006) "friendship groups" and Bumgarner's (2007) "urban tribes." Based on these models, I chose a group of participants who were already acquainted and were using Facebook together. To recruit participants, I began with group of six early adopters who already had a rapport with me and each other. I then used snowball sampling (Brown, 2005; Noy, 2008) to grow this core group based on organic social introductions throughout the project. This approach ensured that I was able to study a network of socially connected individuals in a way that realistically reflected the way Facebook was used as an SNS by participants. Further, in using a group rather than individual unconnected users, my fieldwork could be carried out in physical social situations as well as Facebook. The final core group was 10, with 7 more participants beyond that. This smaller group beyond the core group was either made up of participants who were less involved, or whose stories/experiences were used more for contextual or background purposes and thus were not mentioned specifically in this thesis. The participants mentioned in this thesis, along with some demographic/personal information are listed in the Appendix.

I began my fieldwork in January, 2008 in Toronto, Canada. My primary modes of data gathering during this phase were participant observation as well as formal and informal interviews. For the first six months I was physically located in Toronto, and

was conducting my fieldwork with participants in person, through text messages as well as online through Facebook, email, IM. I spent time with participants as a group as well as individually, and did a number of formal, recorded interviews with each in order to clarify and extend the issues or trends that I was observing. I also requested my participants invite me along to whatever social events they were attending. I would occasionally bring other participants to these social events. The Toronto fieldwork component not only allowed me to establish a strong connection with my participants, it also gave me the opportunity to document the larger context of what was happening in the physical environment. To this end, I spent any time that I was not with my participants in the neighbourhoods in which they lived (largely the downtown of the city), on public transit, the streets and at the malls. I took note of conversations I overheard where people were discussing Facebook. I photographed signs and advertising related to Facebook, as well as situations where people were using Facebook in public. I also attended numerous tech community events, such as CaseCamp.

For the second six months of the study, as I began the analysis of my findings, I continued to communicate with my participants exclusively through Facebook, email and IM. This exclusively online component enabled me to extend the length of the study within the constraints of the project. With a strong rapport established, many of my participants would send me updates from their lives or the latest Facebook-related happenings in Toronto, such as new advertising campaign mentioning Facebook. As I remained in contact with participants as I analysed my data, this second phase of my fieldwork allowed me to ask for clarification on comments that were made. Overall, this ongoing dialogue and mutual reflection by myself and participants, I was able to delve more deeply into the issues as they emerged in my analysis.

Study Design: Facebook

There exists a significant access barrier for ethnographers wishing to conduct fieldwork inside social media companies. For a variety of reasons, such as protecting the latest feature from the competition, it is difficult for researchers to gain the access required for in depth ethnographic work. For example, while working on another re-

search project, I was invited to a lunch meeting at Google's Toronto offices. Before I could go beyond the lobby, I was required to sign a non-disclosure agreement as well as agree to wear a name tag identifying me as a visitor so that employees would "know not to talk about secret things" in front of me. This perhaps explains why, to the best of my knowledge, there has been no ethnographic work on the companies behind social media.

In contrast, users are generally do not have an agenda or mandate to protect the reputations of the company who produces their SNS of choice. As such, they are more willing to participate in ethnographic research by sharing their experiences and activities openly. Conversely, the fieldwork involved in an ethnography of Facebook Inc. would pose quite a challenge, both in terms of getting access and being allowed to publish findings. Even replacing fieldwork with a series of interviews would not yield useful ethnographic results. The Facebook employees with whom I would want to speak (such as Zuckerberg) would likely be media trained and would give canned answers. Further, as I have noted, ethnography works best in context and through behaviour and observation. Ethnography acknowledges that people are not very good at self-reporting, especially in cases where they have a vested interest in keeping certain details private. Thus, even with access, I could not simply ask Zuckerberg about where he derives his beliefs, or what his real goals are and expect answers that would be useful to my study.

For these reasons, I chose to utilise archival and media research combined with textual analysis of the public, written commentary of the developers and key employees at Facebook Inc. I was guided by Danuta Reah's (1998) guide to textual analysis and Fred Turner (2006), whose archival research of the California Bay Area technology culture provided much of the foundation for this thesis, both in form and content. Given that the purpose of this phase of my research was to avoid the metanarrative of technological determinism that runs through much internet scholarship, my approach was also informed by the work of Langdon Winner (1980, 1993), Matthew Fuller's software studies (2003) as well as the SST (Williams & Edge, 1996). Tying together both aspects of my thesis, my understanding of the relationship between users and designers was shaped by John Fiske's (1989) theory of popular cultural production.

This model acknowledges that, despite an unequal power relationship with the site's creators, users still have some degree of autonomy and power within the constraints of Facebook's designs and policies.

I conducted my research and analysis of Facebook Inc. over a four year period (2007-2011), partially in tandem with my user ethnography. My primary sources included interviews with Facebook employees (particularly Zuckerberg); press statements; and official posts on the Facebook blog. I also tracked changes to Facebook's Terms of Service, privacy settings, general features and overall design. I was particularly interested in how Facebook Inc. described and framed its activities and how that may have changed (or remained static) over the course of the site's existence. My goal was to discern any patterns that might be triangulated across numerous materials over a number of years. To this end, I paid particular attention to early materials, such as articles in the *Crimson* (Harvard's student paper) and a 2005 interview with Zuckerberg at Stanford University (Stanford University, 2005). These earlier accounts had the added benefit of being more revealing, since Zuckerberg and Facebook Inc. were both relatively young and were not yet facing scrutiny from the public, regulators and so on.

In 2007, I obtained court documents from ConnectU's case that same year against Facebook Inc., which were published in the now defunct online magazine aimed at Harvard alumni, entitled *02138* (O'Brien, 2007). These documents included partial transcripts of Zuckerberg's testimony in court; part of his application to Harvard; and a letter he wrote to the Harvard administration regarding the disputed founding of Facebook. Also included were copies of incriminating blog posts written by Zuckerberg while working on a precursor to Facebook called Fashmash, circa 2003. Facebook Inc. went to court to have these documents removed from the internet (Goldstein, 2007) -- a demand which appears to have been met, as they are no longer available. In addition to background information about Facebook Inc.'s early days, these documents provided insight into the attitudes and behaviour of Zuckerberg.

To augment these primary materials, I continually monitored and gathered information from secondary sources, including academic publications, mainstream news out-

lets, books and technology blogs. I paid particular focus to *Inside Facebook*, *TechCrunch*, *ValleyWag* and *GigaOM*. I followed the blogs of other academics studying Facebook and SNS, such as Michael Zimmer, Alice Marwick, Fred Stutzman and danah boyd. As I progressed in my research, I built up a network of informants who would also send me relevant news and journal articles as well as blog posts.

When I began this project in 2007, in depth published work on Facebook Inc. was almost negligible, save for Karel Baloun's (2007) self-published account of his time at Facebook in 2005. Since then, a number of journalistic accounts have been released, including Sarah Lacy's, *Once You're Lucky, Twice You're Good* (2008); Ben Mezrich's *The Accidental Billionaires* (2009) and David Kirkpatrick's *The Facebook Effect* (2010a), which was based on an unprecedented number of extensive interviews with Zuckerberg and other key employees. What is notable about all these works, excluding that of Mezrich, is that they were written by individuals who are supporters of Facebook Inc. Baloun even went as far as to compare Zuckerberg to a Greek god in the pages of his account. For this reason, I was careful to balance out these works with other primary research sources and materials.

In addition to textual analysis, I attended SXSW Interactive 2008, which is one of the most important technology conferences. The year I attended, the conference was keynoteed by Zuckerberg. I was present at both the keynote and a number of Facebook sponsored parties, including an event for developers which Zuckerberg appeared at, giving me the opportunity to talk with him about the privacy architecture on his site.

Historical and Discursive Context

In order to deepen this examination of the recent history of Facebook, I also conducted a broader, historical examination of the culture from which it emerged. As I have noted, a key component of a recontextualised internet ethnography is an investigation of not just users, but also of the creators of the internet technologies under examination. As with all technologies, Facebook did not develop in a vacuum, devoid of cultural, social or economic influence. Nor is Facebook a singularity which emerged unexpectedly. As I detail in the next Chapter, Facebook is not only the latest iteration

in a series of social network sites, but exists as part of a larger legacy of computer mediated communication technologies stretching as far back as the late 1970s. These technologies co-evolved with a particular way of thinking about technology, people and society which is pervasive in American technology culture, even to this day. Drawing on Foucault's (1972) definition, this historically rooted system of beliefs is best described a "discourse."⁵ Within this discourse are particular elements which clash with traditional understandings of privacy. These elements can be seen not just in Facebook, but in Google as well. In order to understand this discourse, and by extension Facebook's privacy architecture and policies, one must understand the history from which the discourse has emerged. To this end, in Chapter 5, I chart the historical development of American technology culture through historical accounts and analyses such as Turner's (2006) *From Counterculture to Cyberculture*; Hayles' (1999) *How We Became Posthuman*; Pickering's (2010) *The Cybernetic Brain*; Barbrook's (2007) *Imaginary Futures* and Markoff's (2006) *What the Dormouse Said*; as well as key historical works, such as Norbert Wiener's (1950) *The Human Use of Human Beings*. Taken together, this historical overview provides a critical lens with which to make sensible Facebook Inc.'s privacy choices.

Situating Myself

Further supporting my rationale in choosing a reflexive ethnography was that it would allow me to leverage, rather than falsely hide, my own background and experience as an early adopter of Facebook and member of Toronto's technology community -- a community also shared by a number of my participants. I first went online as a teenager in 1994, so the internet played a pivotal role in my coming of age. It was a place where I could experiment with my identity and find my voice. I spent many Friday nights causing trouble on Internet Relay Chat (IRC) with my high school friends or chatting with strangers on ICQ. My own experience watching the internet become mainstream, both informed and inspired this thesis. The night *The Social*

5. Writing about the prevailing and resistive discourses of teen motherhood, Iara Lessa (2006, p. 285) summarises Foucault's (1972) definition of discourse as "systems of thoughts composed of ideas, attitudes, courses of action, beliefs and practices that systematically construct the subjects and the worlds of which they speak."

Network (the Hollywood film about the creation of Facebook) premiered, I wrote the following on my blog:

In 1997, when I was a nerdy teenage girl sitting in my basement talking to my nerdy internet friends on IRC and ICQ, I never ever would have thought one day I would be seeing a Hollywood movie about the creation of anything to do with the internet... Back then, the internet was like my private, secret thing. I got a weird twinge the first time I overheard the 'cool girls' in the hallway whispering about how they were talking to boys they liked on ICQ. I realised it wasn't just mine anymore. I still get this twinge whenever I'm reminded just how mainstream socializing online has become (even that phrase seems so outdated) – like today.

To me, the internet I experienced in the 1990s was inherently private because very few people I knew "in real life" (as I often thought of it then) were online. Due to this privacy through obscurity, I could share my innermost secrets with strangers on my LiveJournal without facing negative judgement or rejection from my peers. For my teenaged self, this was therapeutic and liberating. My high school was a strict, conservative all-girls school which was very academically focused -- an environment I found stressful and oppressive. The internet provided a world outside of this enclosure, where I could talk to people with an outside perspective. It helped me to stay grounded and gain self-confidence.

As Facebook and similar sites evidence, in many ways, the internet of the 1990s no longer exists. Except perhaps in online game spaces, it more difficult to talk to strangers without it seeming unusual.⁶ Angst-filled teenagers can no longer post things without fear of their parents or teachers finding it. The way I use the internet now is very different. I am very careful about what I share because that information is very much tied to my personal life and professional reputation. At the same time, I

6. For example, adding someone on Facebook who you do not know usually results in a message asking who you are. Such activity is even against the site's Terms of Service.

have access to a great deal of information about my friends and colleagues -- information that they have also probably carefully curated. This dynamic greatly changes my experience of privacy and sociality in everyday life. It was this change in the way I experienced and used the internet -- especially in my social life -- that started me on this investigation which has now become the focus of this thesis.

The Field

Noting that it was common for individuals to be users of multiple social media platforms, my original study design was to include whatever tools my participants used, whether it be Facebook, MySpace, Twitter, Flickr or so on. However, after a few weeks it quickly became apparent that while this ecosystem model was true, study participants (and Torontonians at large) were using Facebook overwhelmingly more than anything else. Penny, one of my participants, reflected what I observed:

I realised it wasn't just me [who was using Facebook a lot] -- it was all of Toronto. It was in the news more. I definately realised it was something I was contributing to. I used to have 100 friends and then I had 300. It was just very fast, and it was a lot of people who were new to Facebook and we just started to use it in all sorts of different ways.

At the time Penny made this observation, Toronto had the second largest regional Facebook network, second only to London, UK.

Prior to starting my fieldwork, I was living in Perth, Australia, where my fellow university students were all still using MySpace. My time living in Perth reinscribed the relative uniqueness of what was going on in Toronto in 2007/2008. Indeed, a few months after I returned to Australia (late 2008) I noticed the same exponential uptake of Facebook that I witnessed in Toronto, an uptake that quickly went global. As I write this, Facebook has over 750 billion users worldwide (Facebook, ND). Staying true to an ethnographic approach, I followed the data and quickly refocused exclusively on Facebook.

There are a number of elements that likely contributed to the mass uptake of Facebook in Toronto. Not only is Toronto Canada's largest city, but it has also been described as "Canada's high tech hub" where new technologies, especially SNS, have quickly proliferated (City of Toronto, 2011, p. 6). In 2007, according to Bryan Segal of comScore (2008), Canadians viewed the most online content (videos, blogs and so forth) and spend the most time using social media of all the G7 countries. Toronto's highly educated population combined with its three universities (Ryerson University, the University of Toronto and York University), were likely a factor in the relatively quick and early adoption of Facebook -- particularly since Facebook was then aimed at a university audience. The large student population provided a base for when Facebook opened to the public. Toronto is also home to Facebook Inc.'s Canadian offices, which are located downtown at Bay and Bloor.

Toronto also has Canada's largest gay population, and is home to one of the largest pride parades in the world (along with San Francisco, USA and Sydney, Australia). As danah boyd noted in her research on early SNS, Friendster, subcultural communities, especially LGBTQ communities, are often the first early adopters of new social technologies (boyd, 2007c). This was anecdotally supported by one of my queer participants, who told me that gay men in Toronto were the first to adopt online dating well before it became accepted by the straight community. Indeed, the higher than statistically average number of queer participants in my study (4 out of 13) might be due to (or at least reflective of) the early uptake of Facebook by LGBTQ communities. Overall, Toronto in 2008 was an ideal place to conduct an ethnography of Facebook.

Chapter Two: From ARPANET to Social Media

Facebook is both shaped and enabled by the history of the internet, social media and, most specifically, social network sites. In this chapter, I provide an overview of the development of this group of technologies from the early days until the present. Given the interdisciplinary nature of both the discipline of Internet Studies as well as the internet itself, a truly comprehensive historical overview would prove quite challenging. As I show throughout the next few chapters, the development of the internet -- both technically and discursively -- implicates a wide variety of disciplines and movements, from Cold War science, Human Computer Interaction (HCI) and artificial intelligence to the New Age, the New Left and the New Communalists. Thus, while this overview is broad, it provides the necessary foundation for the deeper historical examination of more specific aspects of the development of the internet in the following chapters. Overall, my goal in this chapter is to summarise and synthesise the large body of existing literature in order to frame and contextualise my primary research in the underexamined areas in the literature -- namely, the origins and implications of Facebook Inc.'s radically transparent architecture and corporate culture.

As I touched on in the introduction to this thesis, the approach which I take in this chapter is one which acknowledges that the ways in which the internet is described and experienced are often more discursive and than actually-existing. Moreover, the narratives, as I show in later chapters, were often created and promoted by a small group of influential technologists and thinkers in the Bay Area of California. As Allen (2001) has written about Web 2.0 and the historicity of the internet, metaphors -- such as the the online world as a cyberspace; a virtual "frontier" as set apart from the "real" offline world -- were pervasive in early accounts of the internet. Regardless their accuracy, these metaphors were reflected (and perhaps even influenced) in the way the internet was experienced. For this reason, I attempt to the disentangle the narratives and experiences of those using the internet; researching the internet and evangelising the internet by providing an overview in this chapter that looks at evolution of the internet technologically, discursively and academically.

With this in mind, this chapter pays particular attention to two key factors that not only played an important role in shaping today's privacy landscape, they also created the necessary conditions for the existence of Facebook. The first is the shift from the internet as an educational and academic space to a commercial one. In his book *The Future of the Internet* (2009, p. 8), Jonathan Zittrain, an American professor of internet law, charts the shift from the early "generative" internet to today's commercial, "appliancized" internet (pp. 8). This early internet was created researchers, academics and engineers for their own purposes, purposes which were best supported by an organic, inherently innovative, and open internet. Accordingly, these principles were baked into the generative internet. As a consequence, the internet was not originally built to protect privacy, nor serve commercial ends. As Zittrain describes, even though the generative internet lacked a revenue model or master guiding plan, it was successful largely due to a culture of openness, efficiency, cooperation and sharing, all enabled by the mutual goodwill, respect and trust of its users. This culture shaped the architecture of the generative internet. While the goals, purpose and userbase of the internet changed as it became commercial, the generative architecture remained fundamentally the same -- a change which has important implications for privacy.

The second set of factors examined in this chapter are the domestication and mass uptake of the internet combined with the increasing overlap of the online and offline spheres -- two related processes that not only enabled the creation of Facebook, but, as I show in Chapter 6, were also leveraged and accelerated through the site's creation. Metaphorically, the increasing online/offline overlap can be conceived as two connected spheres drawn on a piece of paper -- much like a Venn diagram -- with the two spheres gradually moving together.⁷ As I noted in the introduction to this thesis, the online and offline spheres have never been entirely separate. However, since the invention of the internet, these two spheres have gradually moved closer together, a process which accelerated in the 1990s. As the 2000s developed and momentum gathered around use of the internet, these spheres became increasingly overlapped and the internet and the physical world could be seen as cross-colonising each other.⁸

7. Thanks to Matthew Allen for this analogy.

8. The final stage in this overlapping will be when humans interact with computers using mental

Today, at least in developed countries, use of social media and the internet as part everyday life reflects a near overlap between these two spheres. For example, As Zhao et al. (2008) describe, relationships on SNS are "anchored" in the physical world, meaning that individuals engage use them to engage with individuals with whom they have existing, physical relationships. These sorts of relationships do not fit into the "online relationship" category (Beer, 2008) -- a common category in early internet research -- rather they are more accurately described as extensions or augmentations.

As the existence of this purely online category suggests, and as I show in this chapter, early popular and academic discourse around the internet commonly portrayed the online and offline as two entirely distinct worlds. This discursive framing existed despite the continual existence of at least some overlap. Even though it was not entirely accurate, it was a mode of representation that was influential in the way the internet and its implications were understood and investigated. While there was some logistical truth to these categories, the reality was not so cut and dry.

Touching on these key themes throughout, I chart the development of the internet and social network sites in North America. I begin with an examination of the history and changing perceptions of the internet from the 1960s until today, with particular focus on the development of SNS. With this historical examination as a foundation, I then examine the prevailing themes and areas of research in the literature thus far. My overall goal is to lay the contextual foundation for the rest of the thesis by connecting how the changing nature of the internet plays a critical part in creating the necessary conditions for Facebook and the privacy threats it creates.

A Brief History of the Internet

In this section I chart the development of the internet technologically and socially. I show how, through a number of technological, social and cultural changes, the internet shifted from a non-commercial network for researchers, by researchers to a ubiq-

rather than physical interfaces, as imagined by the early adopters of augmented reality such as the University of Toronto engineering professor and self-proclaimed cyborg, Steve Mann.

uitous social space for everyone. I pay specific attention to the increasing domestication, commercialisation and online/offline overlap -- all of which are crucial factors in the development of today's SNS and privacy landscape.

Early 1980s

Today's internet originally grew out of an American-funded network called ARPANET. Developing in the late 1960s and 1970s, ARPANET was as a closed, non-commercial network designed to connect academics, scientists and other researchers at universities and research centres across the United States (Griffiths, 2002). The invention and subsequent adoption of a standardised protocol called TCP/IP (transmission control/internet protocol) allowed for the connection of other global research networks with ARPANET (Leiner et al., 2009), giving birth to the internet in 1983 (Griffiths, 2002).

The early internet remained relatively obscure for a number of reasons. In addition to it being officially off-limits to anyone outside of the research community, the early internet was largely incomprehensible to the non-technically minded. The difficult nature of the internet was not simply as result of the technology being in its infancy, but also because of the individuals who had designed it. At the time, the main users of the internet were the same people who were building it: American and British computer scientists, engineers and researchers (Baym, 2010a). Thus, the design of the internet reflected their backgrounds and ways in which they understood the world. As Richard Griffith's (2002) describes:

At this stage, the Internet is still quite a forbidding place for the uninitiated. Access commands to find data range from the complicated to the impenetrable, the documentation available is mostly (highly) scientific and the presentation unattractive (courier script, no colour), finding stuff is a pain in the neck and transfer times are relatively slow.

Perhaps the most prohibitive aspect of ARPANET and the early internet was that they

both required users to interact entirely with and through text. Thus, the internet of the 1980s and early 1990s can be described the "textual internet" (Baym, 2010a, p. 13). Perhaps unsurprisingly, the most important and influential technology of the time leveraged the strength of text as an established means of communication. Electronic mail, now simply known as email, was the initial "hot" application of the internet (Leiner et al., 2009, pp. 24-25), a role that continues to this day. Email "provided a new model of how people could communicate with each other, and changed the nature of collaboration, first in the building of the Internet itself... and later for much of society" (Leiner et al., 2009, pp. 24-25). By 1973, the primary use of the internet was for for this purpose (Elon University School of Communications, ND). The "phenomenal success of email" in the 1980s was one of the key factors that helped to push the adoption of the internet well beyond its creators' original expectations and intended use, sparking fears that the system would eventually collapse due to sheer volume (Griffiths, 2002). In a sense, email can be seen as the original social technology.

As I will discuss in depth in later chapters, the 1970s and 1980s were also a time when computers, in contrast to their early conception as cold, dehumanising devices, became increasingly portrayed and treated as personal, human-friendly devices (Turner, 2006). This perceptual change did not simply arise naturally in tandem with the miniaturisation of computers from huge room-sized mainframes to smaller, desk sized PCs. Rather, this changing view of computers was largely due to a rhetorical framing of computing and networking technologies in as social and revolutionary tools which could help humanity overcome a multitude of problems (Turner, 2006). The confluence of these factors facilitated the internet's gradual acceptance into the mainstream, beginning slowly in the 1980s when the internet was still very experimental and was hardly known beyond the research and technology communities from which it emerged.

1980s and early 1990s

By the end of the 1980s, the internet was moving from the realm of the relatively obscure to the subcultural. University students and computer hobbyists were now

joining the ranks of new internet users (Baym, 2010a). More early social technologies, such as Internet Relay Chat (IRC) emerged and began to gain popularity.⁹ Governments also begin to see the importance of the internet, and in 1994 the US government launched a website for the White House (Elon University School of Communications, ND).

This period also saw the acceleration of the internet's domestication-- particularly around the early 1990s -- a shift facilitated by two critical factors which significantly reduced the technology's high entry barriers. The first of these factors was the invention of the World Wide Web by Tim Berners-Lee in 1991, followed by the creation of the first web browser in 1993 (Elon University School of Communications, ND). The invention of the web marked a shift from the textual internet to the graphical internet, whereby accessible and intuitive graphical interfaces eventually replaced the prohibitive text-only interfaces of the early internet. Like email, the web became the internet's second "killer app."

The second critical factor which enabled the mainstream adoption of the internet occurred in 1995, when the last formal barrier which prevented commercial traffic was removed (Kesan & Shah, 2001). Since the internet had originally been built by governmentally-funded agencies for the exclusive use of researchers, academics and scientists, commercial use of the internet had been officially prohibited until 1991, the year the National Science Foundation (NSF) in the United States began granting private computers access to its backbone (Griffiths, 2002). In 1995, the NSF finally ceased its funding of the internet backbone in 1995 while simultaneously opening up internet access to all (Baym, 2010a).

Prior to 1995, the prohibition of commercial traffic had the unintended consequence of fostering the creation of walled networks such as Delphi, CompuServe and AOL (Zittrain, 2009) which provided online services to those who could not get on the internet. These walled online services were generally more facile than the internet,

9. Created for use on the internet in 1988 by Jarkko Oikarinen, IRC is still used by millions of people around the world (Mardham-Bey, 2012).

thereby attracting a less technical, more general audience. In 1995, when the doors were opened for unfettered commercial activity, these private networks could now connect their services to the internet, thereby becoming internet service providers (ISPs) for thousands of users who had an entirely different online experiences, expectations and background than the technically-minded creators and early adopters of the internet (Baym, 2010a). In this way, the internet quickly gained a large number of new users, with many more now able to easily join through AOL or CompuServe. Most importantly, this shift paved the way for commercial sites aimed at a general audience, including Facebook 10 years later.

Even as the internet became more commonly used, throughout this period, the internet was commonly seen as quite separate from the offline world. This perception, although somewhat overstated, was supported by technical and logistical realities which meant early internet (the online world) was often experienced as contextually separated from (offline) everyday life. As I have shown, the early internet was still relatively slow, and hard to use, and thus was only appealing to a very niche audience. Getting on the internet was a conscious and often expensive undertaking. Likewise, since most of the population in developed countries were not yet online, many online communities and networks formed around interests rather than existing geographic networks or shared locations (Ryan, 2008, p. 28). Online identities and relationships were not as commonly anchored in the physical as they are today, particularly on SNS (Zhao et al., 2008). For these reasons, the internet was commonly seen as a space apart from the everyday both discursively and technologically.

Mid 1990s to 2000

The mid 1990s saw the internet begin its rapid and exponential rise into public use and discourse (Turner, 2006, p. 1). The now increasing amount of commercial use combined with the growing popularity of the user-friendly, graphical web -- launched four years prior -- further accelerated the internet into popular use. As internet researcher Matthew Allen describes, the web played an important part of the domestication of the internet by making it more like more familiar, commercial media:

Prior to the web, the Internet was constructed according to the aesthetic and functional conventions of computing. Part of the attractiveness of the web was that it relocated online life to the normative space of traditional media design, thus making it culturally (not just technically) more accessible. (Allen, 2011, p. 8)

Part this increasing accessibility could be attributed to the internet's increasingly commercial use. No longer only created by technologists, for technologists, the new commercially-created internet technologies were created by companies with a vested interest in mainstream accessibility.

In addition to the web, email remained a popular reason for people to get and stay online (Baym, 2010a, p. 13). Other user-friendly technologies began to emerge, such as the first instant messenger (IM) in 1996, called ICQ (Boneva, Quinn, Kraut, Kiesler, & Shklovski, 2006), followed by the first SNS, SixDegrees, in 1997. As these early social technologies helped the internet become part of everyday life, the spheres of online and offline became further overlapped. References and connections to the internet were now more common in the physical world. As two technologists described in 1997:

We have often mused to ourselves about what regular people (aka civilians) must think of the Internet and those of us who use the 'net everyday. When the Internet was a secret within the academic and R&D community, the popular literature didn't give it a second thought. But now that we see URLs everywhere (on the side of ambulances, say, and at shopping malls), Web addresses as common as 800 numbers, advertisements for Internet services appearing in Newsweek and on Super Bowl commercials, online real-time news events, and common criminals going online (not to mention new online-specific crimes), it is clear that the Internet has arrived as a popular icon (Kessler & Shepard, 1997, p. 114).

Like today, popular representations of the internet both reflected as well as shaped the way the internet was perceived. In 1995, the release two Hollywood films featuring somewhat fictionalised versions of the internet -- *Hackers* and *The Net* -- showed that the internet had both reached a critical point in public perception, but at the same time was still largely misunderstood. Moreover, they both reinforced the common perception that the internet was entirely apart from reality. Relying on metaphor rather than technical reality, both films portrayed the internet as a literal cyberspace that was fantastical, mysterious and even dangerous. Three years later, *You've Got Mail* reflected the cracks in the stark online/offline divide. Playing on this divide, film's plot centres around the budding online romance of two protagonists, who communicate through IM and email using pseudonyms. Unbeknownst to the pair, they actually know and despise each other in the physical world. In this way the internet is both apart, yet not entirely separate from their lived reality. Even though they see their online interactions as "virtual" or not "real," their activities still have very real consequences for their social lives.

You've Got Mail also reflects some of the logistical realities that supported the perceived apartness of the internet. The protagonists speak of "going online," a conscious effort which requires sitting down at a computer and dialing in with a modem, rather than the seamless and perpetual connectedness enabled by smartphones and wifi ten years later. The film, as an ideological vehicle for an AOL branded, walled-garden version of online space, also reflected the increasing commercial interest in and use of the internet.

Some of the more hyperbolic proponents of the internet also reflecting and perhaps also fuelled this perception of a strict online/offline dichotomy. Within these technologically deterministic narratives, the internet was separate and uninfluenced by pre-existing "offline" ideologies. Offline meanings of identity, gender, sexuality and race could apparently be erased, reworked or would manifest differently in the online world (Hine, 2003). As John Perry Barlow -- one of key figures in shaping the discourse around the internet -- proclaimed in 1996, "We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth" (Barlow, 1996). This way of thinking was echoed in popu-

lar discourse, as exemplified by the MCI commercial that ran during the 1997 Superbowl, which proudly announced: "There is no race, there are no genders, there is no age, there are no infirmities, there are only minds. Utopia? No, the Internet" (Baym, 2010a).

Another key shift during this time period was the increasing commercialisation of the internet. As noted, the NSF officially began allowing commercial traffic in 1995, a change which would enable a gradual yet drastic change in the culture, use and indeed the very nature of the internet, particularly with respect to privacy. As Zittrain (2009) argues, the internet was not designed to protect privacy as such a thing was inefficient and counterproductive when it came to information sharing, which was the driving goal behind the creation of the internet. Indeed, privacy was also deemed unnecessary given the shared goals and backgrounds of the early creators of the internet. Privacy was seen as an issue on the social layer of the internet, not the technical layer. Much like a co-operative, users were seen as equal participants rather than customers, and as such, Zittrain argues, would respect the network and other users. The assumption that users would not be destructive and would respect each other's privacy was reflected in the very architecture of the internet, for example the ability (at least in the early days) for users to remain anonymous or use a pseudonym, or the equal treatment of all data on the network, regardless of sender or content.

As Zittrain's account of the history of the internet shows, the beliefs of the early internet engineers and scientists shaped its architecture. The well-educated scientists, researchers and engineers who created the internet had a shared background which valued efficiency, logic, and innovation -- values which all became embedded in the internet, even as it became commercial. The result is that the architecture of the internet -- redundancy, persistence of data, and default openness, features meant to support educational, non-commercial use -- has now become a challenge for everyday privacy.

In contrast to the early days of the internet, the majority of today's internet users are just that: users. They do not participate in the create the technologies that they use. The power dynamic has shifted. A small number of individuals -- those working at

social media companies such as Facebook Inc. -- hold a degree of power over users. As I show in Chapter 5 and 6, the values embedded in the internet have reworked and reinvoked to support Facebook Inc.'s goals, which reflect a largely different attitude than that of the internet's creators. While espousing the values of the generative internet, Facebook Inc. has built a site that, architecturally, is at odds with these values. As Zittrain describes, today's increasingly "appliancized" internet is characterised by walled, proprietary services, devices and networks (such as Facebook) which impose top down authority and control (Zittrain, 2009, p. 8). While these networks are easier to control and regulate when it comes to privacy, security and illegal activity, they also make it easier for those in control to exploit and monetize the privacy of users.

2000s: Web 2.0 and Social Media

Throughout the 1990s and early 2000s, the commercialisation of the internet continued, as did the growing overlap between of the online and offline spheres. By 2004, the internet could be considered a normal part of everyday life in developed countries. As Baym argues, it "had become almost invisible" (Baym, 2010a, p. 48). By the time I began this project in 2008, the norm of always-on internet connectivity through cable and DSL in Canada's urban centres in concert with the growing prevalence of Blackberries and other smart phones saw individuals seamlessly checking their email or IMing with friends throughout the day, in a spare moment at the bus stop or during a lull in activity at work. Contrast this use of the internet with that of the mid 1990s, when checking one's email still required consciously and intentionally sitting down at a desktop computer, dialling up one's ISP and then waiting to get connected.

Most importantly, with respect to this thesis, the 2000s saw the rise of SNS and social media more broadly. Given the focus of my thesis on Facebook, I dedicate the next section to the examination of the definition, history and scholarship of social network sites.

A Brief History of SNS

In this section, I continue my historical examination of the internet with a specific focus on the development of early SNS and the creation of the necessary conditions for mass uptake of Facebook. I begin with various scholarly definitions of SNS. I then provide a brief history of SNS. Throughout this historical examination of the internet, I have examined the gradual overlap between the online and offline spheres as a process intertwined with the normalisation, domestication and commercialisation of the internet. These processes, ultimately, created the necessary climate for the existence of Facebook. Likewise, with respect to the popularisation of SNS, there are two essential components of these larger processes which were necessary for the mainstream success of SNS and indeed Facebook more broadly. I conclude this section with a discussion of these two factors.

Social Network Sites Defined

While Facebook Inc. defines itself as a "social utility" which "helps people communicate more efficiently with their friends, family and coworkers" (Facebook Inc., 2011), most academic scholarship defines Facebook as a social network(ing) site (SNS). Despite this consensus, the definition of SNS can still be rather slippery. According to Alessandro Acquisti and Ralph Gross (2006, p. 2), who were among the first to study Facebook, "an online social network is an Internet community where individuals interact, often through profiles that (re)present their public persona (and their networks of connections) to others." SNS have also been called social network communities (Stutzman, 2006). However, the most authoritative description of SNS comes from danah boyd and Nicole Ellison (boyd & Ellison, 2008), who propose a definition of SNS based on three key features. In their schema, SNS are "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." boyd and Ellison also propose that researchers use the term "social network sites" rather than "social networking sites" -- two terms that are often used interchangeably. Even though social networking site is used more commonly (and had twice as many Google hits in early 2012) boyd and Ellison argue that there

is a critical difference which is demarcated by their term. The term "social networking" implies that new connections are being formed. On the other hand, they argue, the term "social network site" more accurately reflects the actual usage of what it describes. That is, the building and maintenance of existing contacts by users. Facebook Inc.'s own definition of a social utility also reflects this focus on existing relationship maintenance over the creation of new ones.

Responding to boyd and Ellison's (2008) definition, Beer (2008) argues against what he sees as their implicit segregation of online and offline life in their research approach, especially with respect to social interactions and friends. Just as their distinction between social networks and social networking suggests, with SNS in the mainstream and embedded in everyday life, this online/offline distinction is no longer applicable. Beer points out that is not longer so easy to distinguish between online and offline nor between a "Friend" (online) and "friend" (offline). With the mass adoption of SNS, they are more often than not the same person.

Beer also disagrees with boyd and Ellison's proposal that researchers use the term social network sites in lieu of social networking sites as the term *networking*. Beer argues that this term is too broad and means too many things, thus losing the nuance which separates sites such as Facebook from YouTube or Last.fm, which according to boyd and Ellison's definition, would fall into the SNS category. Indeed, the characteristics that define a social networking site (profile, public listing of Friends) are becoming standard functionality across a wide range of web services, as users increasingly expect to be able to see what their Friends did, bought or looked at, and if they liked it (Needleman, 2008). Twitter (microblogging), LiveJournal (blogging communities), LibraryThing (book sharing) -- all have the core elements of SNS, even though they are not aimed exclusively at connecting people the way Facebook is. Even the online bookseller, Amazon, now has user profiles and the ability to add Friends as "Interesting People."

Privacy philosopher Helen Nissenbaum's definition of SNS further reinforces the slippery, broad nature of SNS: "Social networking sites constitute a sub domain of the larger software ecosystem, frequently called Web 2.0, a loose class of Web sites

dedicated to creating and maintaining socialities, groups and networks" (Nissenbaum, 2010, p. 59). Given the multiplicity and slippery nature of the term SNS, I will distinguish between SNS from sites that have the social elements of SNS, such as YouTube, but are not exclusively for social purposes by classifying them as social media. Put simply, all SNS are social media, but not all social media sites are SNS. Social media is also a clearer term that is becoming more commonly used in lieu of Web 2.0.

A Brief History of Social Network Sites

In North America, sites that fit boyd and Ellison's (2008) definition of SNS have existed from as far back as the 1990s. The first SNS was SixDegrees, which launched in 1997, followed by LiveJournal in 1999. As Gross and Acquisi (2006) summarise:

Although the concept of computer-based communities dates back to the early days of computer networks, only after the advent of the commercial Internet did such communities meet public success. Following the SixDegrees.com experience in 1997, hundreds of social networks spurred online, sometimes growing very rapidly, thereby attracting the attention of both media and academia.

However, SNS did not begin to garner widespread attention until the launch and subsequently rapid rise in the popularity of Friendster in 2003 among a number of significant yet niche groups (boyd & Ellison, 2008; Eisner, 1985). Even though it framed SNS in a negative light, the MySpace moral panic in 2006 (Marwick, 2008) reflected SNS's ascent to mainstream discourse. While Friendster and MySpace were popular among certain segments of the population, such as teenagers, gay men and a number of other subcultural groups (boyd & Ellison, 2008), Facebook was the first SNS to appeal to a broad demographic.

Early SNS were based around the then novel ability to publicly articulate one's relationships with others. This articulation was accomplished through the other key component of the service: the profile page. In addition to displaying pictures and personal

information about themselves, users can display a clickable list of “Friends,” which allows users to browse each others networks. Social networks have always existed both online and off, but this was the first time such networks were formalised, made artifactual and navigable (boyd, 2005).

MySpace and Facebook built on the success of Friendster by taking the next step by responding to the desire of users to do more than simply list their friends (boyd & Ellison, 2008). MySpace became more appealing to teenagers than Friendster because, unlike Friendster, it allowed users to design their profile pages; connect with whomever they wanted and use whatever identity they wished (boyd & Ellison, 2008). Similarly, Facebook added new and compelling ways for users to interact with each other, such as the ability to tag friends in photos or play Scrabble with family members.

Overall, Facebook grew out of the mainstream adoption of SNS started by Friendster, MySpace and other early SNS. Combined with the domestication of the internet more broadly, these earlier sites paved the way for Facebook by helping to normalise and create an understanding around their use.

Network Effects and Anchored Identities

In addition to the commercialisation and domestication of the internet combined with an increasing overlap between the online and offline spheres, there are two important and interrelated components within this process which are worth examining. These components were necessary for, and part of the development of, SNS as part of everyday social life.

The first of these components are network effects. Like fax machines, the value of the internet is relative to its number of users. The more users a network has, the more useful it becomes to all users (Schauer, 2005). The second factor is the physical "anchoring" of digital identities and relationships (Ladd, 2009; Zhao et al., 2008). In the early, textual days of the internet it was uncommon to use one's full name. Instead, users employed pseudonyms, often referred to as handles, screen names or nicks.

With the increasing use of social media and SNS came the increased use of "real," legal names. This is, of course, not to say that nicknames and identity play no longer take place online. While there are still forums and other spaces online where users use pseudonyms, the norm on SNS like Facebook and Twitter are to use one's full name (Zhao et al., 2008). As Kirkpatrick (2010a, p. 12) describes: "On Facebook it is important today to be your real self as it was when the service launched at Harvard in February 2004. Anonymity, roleplaying, pseudonyms and handles have always been routine on the web... but they have little role here [on Facebook]..." In the same way, individuals using nonymous, anchored identities use SNS to extend and build on pre-existing relationships (boyd, 2006b). In other words, relationships that are anchored in the physical world.

SixDegrees, the first SNS, provides a good case study for understanding these components. SixDegrees ceased operation at the end of 2000. According to boyd and Ellison (2008), the founder of SixDegrees believes that the site's failure was a result of it being ahead of its time. As boyd and Ellison (2008) argue "While people were already flocking to the Internet, most did not have extended networks of friends who were online." The result was that the network effects were not yet strong enough to make SixDegrees compelling and useful.

As the failure of SixDegrees suggests, and as I examine more fully in Chapter 4, a key factor contributing to Facebook's success was timing. Facebook was not the first SNS, nor is it the most well designed. Because of the Facebook's initial popularity with university students, the company was able to better leverage critical shifts in the way the internet was used. As I show in the following chapters, as Facebook Inc. built its influence over a number, it increasingly pushed the boundaries of internet use -- particularly around privacy -- even further.

Internet Scholarship

In this chapter thus far, I have provided a historical examination of the internet, with a focus on the factors essential for the development of SNS, in particular, Facebook. Building on this historical context, this section lays out a chronological examination

of the key themes and areas of research in internet studies and related disciplines. As an area which has garnered so much attention that it can be considered an area of study unto itself, I also provide a cursory examination of the key themes in SNS research -- a summary which will be fleshed out fully in the next chapter.

As in the introduction to this chapter, the concepts which are used to describe the internet both in popular culture and by academics -- such as the notions of offline/off-line or real/virtual -- can often be more discursive than actually-existing. Accordingly, this section examines the evolution of key research on the internet, with an eye for how the approaches might have contributed to less than accurate narratives around the realities of the internet.

CMC and Impoverished Social Cues

Just as the internet was essentially unknown outside of research and technology communities throughout the 1980s, it was also largely unexamined in the social sciences and humanities. The research focus during this period was "computer conferencing" and computer mediated communication (CMC). CMC, which became a field of scholarship in itself, was primarily concerned with the effects of computer-based communication in organisational contexts (see for example Rice & Love, 1987; Kiesler, Siegel, & McGuire, 1984; Sproull & Kiesler, 1986). CMC's quantitative, functionalist research approach was founded on a model in which technology influenced or determined interaction between users. CMC also framed networked computers as impersonal tools rather than as facilitators of social spaces or community platforms. As such, communications on computers were studied using face-to-face communications as a comparative benchmark. As such, a large focus of these studies concerned the impacts of the impoverished social cues which were perceived to be a feature of text-based communication. This model of networked communication was echoed in popular discourse well into the early 2000s. A story from 1993 on the internet by the Canadian Broadcasting Corporation described the internet thusly:

Computer communication is not much like human communication, there's no body language, no intonation, no facial expression... so the isolated communicators of cyberspace have come up little signs made out of punctuation marks. They're called emoticons. They go at the end of sentences as graphic explanations (CBC News, 1993).

The most influential research during this time was conducted in experimental laboratory settings using custom computer conference systems (Hine, 2003). Unlike the internet or other early networks such as BBSes (bulletin board systems), these laboratory computer networks were not persistent communities. Thus, such an approach has been criticised for not reflecting “an accurate picture of the reality of virtuality” (Sudweeks & Simoff, 1999, p. 38). Indeed, such a user-focused decontextualised approach reflects an implicit technological determinism (Hine, 2003), which, as I noted in the introduction, continues in internet studies and related fields, such as Human-Computer Interaction (HCI) (Fuller, 2003).

Virtual Communities and Online Identities

As awareness of its existence grew throughout the 1990s, the internet also became of increasing interest to humanities and social science researchers. Counter to early CMC research which treated computer networks as tools, rather than social spaces, this phase of internet research painted a different picture. In 1993, through his seminal book *The Virtual Community*, Howard Rheingold became instrumental in reframing the internet as social and community space unto itself. Unlike the CMC research studies which had users interacting with each other across temporary networks, Rheingold showed -- through his experiences on an early online community called the Whole Earth 'Lectronic Link (or the WELL) -- that electronic communication could facilitate supportive, vibrant and authentic communities.

As the title of the *The Virtual Community* suggests, the internet of the 1990s was still portrayed as a virtual space, where online communities existed distinctly from physical communities (Rheingold, 2000). Virtual text-based communities on MUDs, MOOs, IRC and Usenet were seen as spaces apart from reality where play and

exploration (especially around one's identity) could occur and the constraints of the physical or "real" world could be overcome (Turkle, 1997). In addition to virtual community, this virtual or online identity was also a key area of study. Sherry Turkle (1997) and Amy Bruckman (1992) looked at identity play in the fantasy environments of MUDs and MOOs while Daniel Chandler (1998) examined identity creation and articulation on personal homepages. This research focus on gender play, multiple identities or "cyberspace"-only identities reinforced scholarly perceptions of the internet as apart and separate from reality.

At the same time, the alternymity allowed by the internet as identified in this research -- that is, the ability for individuals to create distinct, disembodied identities for themselves online -- reflected a clear and real disconnect between the online and offline worlds. Even though alternymity was, and still is, a valid example of a way in which the internet can be distinct from real life, its occurrence was overemphasised by many researchers in the 1990s (Baym, 2010a). Overall, there was a stark and somewhat overstated divide between the "virtual" or online world and the "real" or offline world.

Social Network Sites

In later chapters, I look at SNS more deeply with respect to privacy. In this section, I aim to provide broader overview of the other key themes in SNS that are relevant to understanding privacy on Facebook. Since my study concerns Canadian users, my focus here is on North American research on English speaking sites.¹⁰ Overall, aside from privacy, most research on SNS has focused on various elements of identity, reputation and impression management and the nature and structure of online Friendships¹¹ and Friendship networks (boyd & Ellison, 2008).

10. See (boyd & Ellison, 2008) for a comprehensive overview of international SNS and SNS research.

11. I use "Friendship" to distinguish the feature on SNS from "friend" in the conventional sense. As Beer (2008) notes, there is now very little difference between online and offline relationships. Who one is Friends with online is generally the same as who one is friends with offline. Distinguishing between the two based on the somewhat overstated online/offline dichotomy, Beer argues, serves to further reinforce it. However, Friendship is still a core SNS feature which is functionally different than offline friendship. For example, Facebook Friendship grants a user ongoing and automatic information

SNS research has continued the traditional focus in internet studies on identity. As I will examine in later chapters, identity, especially with respect to reputation management, is a critical part of privacy for users of SNS. Some key works in this area include Alice Marwick's (2005) examination of identity, power and authenticity on Friendster, Orkut and Myspace; Fred Stutzman's (2006) study of identity sharing behaviour on Friendster, MySpace and Facebook; Hugo Liu's (2008) identity and taste performance on MySpace. danah boyd, one of the first researchers to study SNS has looked at identity and SNS from a number of perspectives, such as her examination of identity performance on Friendster with Jeffrey Heer (2006).

Like identity, online relationships and communication represent another common area of internet research which has continued with the study of SNS. The nature of SNS has presented new research possibilities. For example, the ability to easily gather large datasets has led to a significant number of studies which analyse the network structure of online connections and relationships (boyd & Ellison, 2008). Friending, or the act of adding a "Friend" to one's list of publicly articulated friends, was non-existent until the invention of SNS. Friendship, then, represented a new area for examination. For example, the functional meaning of friending mixed with pre-existing meanings of friendship has led to a new meaning with new norms and protocols (boyd, 2006b; Fono & Raynes-Goldie, 2006). As I examine in depth in a later chapter, Friendship is also a form of privacy or access control.

Thus far, the majority of North American SNS research has been carried out by American researchers. However, there is some important and relevant research being done in Canada, especially with respect to Facebook. The Facebook research group at the University of Guelph has completed a number of studies that examine identity, information disclosure and privacy on Facebook.¹² Other Canadian SNS research of note includes Leslie Regan Shade's focus groups with young women who use SNS (2008) as well as her co-authored research with Nicole Cohen on gender, privacy and

access between two users. It is on this difference that I base my distinction.

12. See their website for a list of publications <http://www.psychology.uoguelph.ca/faculty/desmarais/>

commodification of Facebook (2008). Valerie Steeves' work on the difference between the legal definition of privacy expectations versus what young people's expectations while using Facebook (2008) is also significant.

Conclusion

In this chapter, I laid the historical and contextual groundwork for an examination of Facebook and privacy. I showed how the internet became more accessible and more pervasive. Network effects encouraged more users to join and share more content. Individuals became comfortable using their offline identities online, especially on social media sites where this has become the norm. The online and offline spheres became nearly overlapping. At the same time, the internet has become a highly commercialised space, where users must pay to participate -- either directly through subscription fees or indirectly through targeted advertising and data collection and mining.

This domestication, overlap and commercialisation are three key factors which created necessary conditions Facebook. Moreover, the confluence of these factors has lead to the key privacy issues facing social media users today. As I will show in Chapter 7 and 8, the increasing overlap between the offline online not only increases the potential impact of privacy threats (Albrechtslund, 2008) but elevates the social cost of opting out. Further, the increasing popularity of social media also means that more people are more at risk. Finally, allowing commercial uses of the internet also meant allowing data mining, targeted advertising and other commercial activities that threaten the privacy of users. In the following chapters, I examine what this all means for privacy in the age of Facebook.

Chapter Three: Privacy, Surveillance & Social Network Sites

While Facebook has garnered a great deal of attention for its questionable privacy activities (boyd & Hargittai, 2010), concerns about privacy long predate the invention of SNS and indeed the internet itself. In 1890, American lawyers Samuel Warren and Louis Brandeis, famously defined privacy as "the right to be left alone" (Warren & Brandeis, 1890). In this notion of privacy as withdrawal or protection from unwanted disclosure -- a conception which continues to inform definitions to this day -- privacy exists in opposition to one of its key threats: surveillance. As such, these two concepts are intertwined.

In more recent times, as the surveillance capabilities enabled by computing and other digital technologies have grown exponentially, so too have academic and public concerns about the resulting threats to privacy. As such, privacy researchers have tended to look at new technologies from the perspective of digitally mediated surveillance -- that is, how technologies (such as computer databases, CCTV, the internet and so forth) facilitate increasingly pervasive and intrusive surveillance practices on the part of institutions such as governments, banks and credit card companies (e.g. Elmer, 2004; Lyon, 1994; Lyon, 2001).

In the public discourse around privacy, particularly concerning the internet, the primary concern has not always been surveillance. For example, a common worry in the 1990s surrounded the security and privacy of online commerce, particularly with respect to perceived threats from hackers.¹³ A more recent concern, perhaps the one most worrying to internet users, is the more subtle invasion of privacy engendered by the regular monitoring and collation of online activities by the very companies who

13. For example, from 1994 to 2001, Alan Westin's privacy surveys of public opinion were all focused on consumer privacy online (Kamaraguru & Cranor, 2005). E-commerce related privacy concerns were also reflected in the literature (e.g. Furnell & Karweni, 1999).

provide those services. As I have touched on previously and explore more in this chapter, there has also been a significant amount of anxiety around perceived privacy threats to younger users, in the form of "oversharing" and online predation (Marwick, 2008; Raynes-Goldie, 2011).

Indeed, as the internet -- in particular SNS and social media -- have become part of everyday life in North America, so too have privacy concerns around their use (Utz & Krämer, 2009). In 2000, legal privacy scholar Anita Allen (2000, pp. 1180-1181) observed how privacy had become a more common point of discussion in academic, journalistic and policy circles. In contrast to the late 1980s when the internet was in its infancy, Allen recounts that by the early 2000s, privacy had more "buzz" (p. 1180-181). These concerns culminated in 2010, when the world's privacy commissioners and data regulators began to make SNS a serious priority.¹⁴ Indeed, privacy is now almost synonymous with digital or online privacy.

In order to provide a foundation and analytical framework for the rest of the thesis, this chapter examines digital privacy and surveillance from a number of different angles. In the first section, I provide an overview of conventional models of privacy and how they are being challenged by digital technologies, particularly in the context of surveillance. Through a review of the key literature in the field, the second section connects digital privacy issues with another key topic of this thesis: youth. I pay particular attention to the emerging yet still underrepresented body of critical work in the field. Based on the drawbacks of existing models as I show throughout this chapter, I conclude with framework for the rest of the thesis based on social privacy and Helen Nissenbaum's (2010) contextual integrity.¹⁵

14. The Office of the Privacy Commissioner was the first to challenge Facebook Inc.'s privacy policies and design, beginning with their investigation in 2008 which resulted in the company being forced to change their deletion procedure and policy (Office of the Privacy Commissioner of Canada, 2009). Since then, others have followed suit. In 2010, along with fellow privacy and SNS researcher Alice Marwick, I was invited to speak at the opening plenary at the annual International Conference of Data Protection and Privacy Commissioners, which is where the world's privacy regulators gather each year. We were told that this was the first year academics doing our kind of research were invited, reflecting a broader change in the mandate of the world's data and privacy commissioners.

15. Sections of this chapter appeared in an annotated bibliography for the Cyber-surveillance in Everyday Life Workshop (2011) at the University of Toronto.

Understanding Contemporary Privacy Issues

In this section, I explore and define the key concepts for use in this chapter and the thesis more broadly. I begin with an exploration of the changing and rather elusive concept of privacy, beginning with early conceptions and moving to contemporary times. I then examine one of the most discussed and perhaps the most pressing threat to privacy (both conceptually and practically) in a networked age: surveillance. To accomplish this, I begin by outlining the various threats to privacy as a result of surveillance. Then, bringing together the properties of information and communication technologies (ICT) -- a group of technologies of which SNS is a part -- I look at how SNS increases surveillance while decreasing privacy.

Defining Privacy in a Changing Landscape

Legal scholar Daniel J. Solove describes privacy as a "muddled" and "exasperatingly vague" concept whose definition is a source of debate amongst privacy scholars (Solove, 2007a, p. 8). Further complicating a clear definition of the term, concepts of privacy are contextual and can change over time. Yet, there is one commonality which runs through many discussions of privacy: the interrelated notions of disclosure, control and the public/private divide. As mentioned, Warren and Brandeis' 1980 definition of privacy as complete withdrawal has strongly informed contemporary conceptions of privacy, especially with respect to legal definitions. Within this definition is an equally longstanding and influential privacy concept: the public/private divide (Nissenbaum, 2010, p. 91). As one of the Western world's "grand dichotomies," notions of the public and private sphere have been deployed as key organising categories since classical antiquity (Weintraub, 1997a, p. xi).

In this dichotomy, the public sphere is generally linked with the world outside the home, such as one's professional or political life (Gavison, 1992, p. 6; Sheller & Urry, 2003, p. 112). Accordingly, it is a sphere where individuals, legally, should not expect privacy (Solove, 2007b, pp. 162-163). If something is ruled to be in the public domain, or to have occurred in public, it is not subject to legal privacy protection. The realm of the private is the only place privacy law has jurisdiction (Nissenbaum, 2010, p. 96).

The public sphere, however, implicates much more than a space of disclosure. For example, Robert Putnam (2000) emphasised the importance of the public sphere when lamenting what he perceived to be the decreasing involvement of citizens in public life. In this sense, the public is where political and community participation take place. In contrast, the private sphere is associated with the home, domestic activities and one's personal life. While the public is associated with interference, the private is associated with freedom (Gavison, 1992, p. 6). Thus, in private, privacy is expected. Overall, the boundary between the public and privacy spheres can be seen as a dividing line between visibility and invisibility; accessibility and reclusivity; and the individual versus the collective (Gal, 2002, p. 77; Gavison, 1992, p. 6; Weintraub, 1997b, pp. 15-16). It delineates both expectations of behaviour on the part of individuals as well as when privacy can be expected.

Consequently, much of the public discourse around privacy and digital technologies relies on a clear delineation between the public and private spheres. For example, cultural commentator Andrew Keen (2011) has argued that SNS are eroding the once stark distinction between the spheres of public and private. Keen's argument also reflects a common notion that historically, individuals had more privacy than today. Keen is half right. In the previous chapter, I discussed how the spaces of online and offline could be conceptualised as overlapping spheres. In the same way, the spheres of public and private should not be seen as clearly divided, rather they should be seen overlapping in a similar manner. Keen is correct in noting that SNS and other digital technologies have facilitated more overlap between the public and private spheres. However, as this metaphor suggests, there was never a clear demarcation between these spheres. As privacy philosopher Helen Nissenbaum argues, the reason digital technologies are "so disorienting" in the context of privacy is that "they reveal the inconstancy of boundaries and fuzziness of definitions" (Nissenbaum, 2010, p. 101). Overall, the spheres of public and private have always been, to some degree, overlapping. The "overlappingness" of the public and private is not new, nor is it entirely a result of digital technologies. Rather, digital technologies are making this overlap -- and the ensuing privacy threats -- somewhat more pronounced and more obvious, largely because these threats are now occurring in new venues and modes.

Further, as digital privacy lawyer and scholar, Lawrence Lessig (1999) shows, the narrative whereby individuals led much more private lives relative to today is a somewhat overstated. In the early days of the United States, it was not uncommon for individuals living in towns to subtly monitor each other through co-surveillance. Accordingly, people tended to know each other's comings and goings. A critical contrast with today's landscape, as Lessig notes, is that this form of monitoring did not leave a digital trail. Even though individuals may have been aware of each other's activities, these activities were not automatically recorded and stored for later retrieval. Put simply, human memory "cannot be searched, or collected, or produced as records" (Lessig, 2000, pp. 150-151). Thus, in early America, individuals were not any more or less private than today. Instead, they had a different kind of privacy while engaging in a different form of surveillance.

What Nissenbaum and Lessig show is that the contemporary change in privacy is not simply the reduction of one's ability to remain private as a result of an increased overlap between public and private. While it may appear that in a networked world, the capacity to avoid disclosure of many previously private activities has been reduced, this understanding does not quite capture the continuity between earlier times and the present day. Digital technologies have not, of themselves, swept away decades of well-understood and comfortable privacy possibilities. Rather, they have made more challenging, and more widespread, with more visible consequences, pre-existing overlap in the perceived public/private divide. The notion of well demarcated spaces for public activity, where one cannot or should not expect privacy, and private activity, in which one is free from interference and an expectation of disclosure, was already something of a legal fiction by the advent of SNS.

Another overlooked change with respect to privacy is a change in power. In Lessig's early America, co-monitoring reflected relatively level power relations. Individuals watched each other equally, knew they were being watched, and had a general idea of how information about them would be used. In using credit cards, SNS or even by walking down the street, individuals today are increasingly subject to invisible, top-down surveillance by parties who exert legal, social or economic power over them. This change in power is enabled by the communication features of digital networking

technologies which afford increased and widespread surveillance. It is these features that are new, rather than the privacy threats they create.

Surveillance and Privacy

As the conception of privacy as "right to be left alone" suggests, privacy is commonly defined as lack of exposure. In this context the threat of surveillance -- whereby someone else removes the ability for one to know manage what personal information is collected and disclosed -- is a clear privacy threat. In this section, I use a number of examples to show the ways in which surveillance can lead to a threat of privacy, particularly around the prevention of disclosure.

Solove's privacy taxonomy maps out four different modes of surveillance and their possible consequences: information collection; information processing; information dissemination and invasion (Solove, 2007a, p. 11). In addition to the obvious category of surveillance, the threats most relevant to the use of Facebook are information processing and collection, which can result in aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion.

David Lyon's notion of "leaky containers" provides an example of how electronic surveillance can cause some of the threats outlined by Solove. Leaky containers, a notion similar to what software developers call "function creep," refers to the collection and storage of data intended for one purpose, which is then used for another (Raynes-Goldie & Fono, 2009). In Lyon's example, Canadian police use a GPS system installed on a stolen car for the purposes of navigation to track the car and apprehend the suspect. In this case function creep is of benefit to citizens. However, much more questionable examples have emerged, especially in a post September 11 world. The USA PATRIOT act, which was enacted for the specific purpose of "fighting terrorism" through intelligence gathering has been repeatedly and unlawfully misused against American citizens (Staff, 2007). Specifically, the act, which was intended for gathering intelligence against foreign terrorist threats, rather than domestic criminal investigations, has been used to carry out unlawful investigations of sus-

pected criminals without probable cause (Lichtblau, 2003). A perhaps even more questionable and unintended use of the act was its deployment in 2005 to remove homeless people from a train station in New Jersey (Parry, 2005).

Whether or not information is gathered for explicitly for surveillance purposes, or it is collected from a leaky container, it can be used to for numerous reasons that can threaten the privacy of both those deemed dangerous by society as well as the innocent. The release of embarrassing or incriminating information can be used to silence or control dissenting or politically unfavourable individuals (Solove, 2007a, p. 17). There is also the threat of blackmail, and wrongful accusations. Indeed, misuse of personal information can lead to a "miscarriage of justice based on false information" (Albrechtslund, 2008).

In fact, the very collection and storage of data, no matter what the original purpose, can create privacy threats that would not have existed otherwise. For example, believing they were doing a favour to the research community, AOL Research *purposefully* distributed a file in 2006 which contained the search data and keywords of 650,000 million AOL users (Arrington, 2006). Even though the users contained in the file were given anonymous numbers, there was enough personally identifiable information to identify some of the users, as well as their social security numbers or addresses. After three days, AOL Research finally realised their mistake and removed the file from their site, but given the nature of the internet, their actions came too late. The file had been mirrored on multiple sites across the internet. Other individuals had created websites with easy-to-use front end interfaces which allowed anyone to search through the file as easily as a Google search. As this example demonstrates, the very existence of digital databases pose a potential privacy threat, even from well intentioned and reputable organisations.

Another example of well intentioned misuse of collected information occurred in in 2008, when the Canadian Radio-television and Telecommunications Commission (CRTC) created a "do-not-call" list that Canadians could use to avoid being called by telemarketers. In 2009, the Consumers Association of Canada reported that people who had registered their numbers on their list were getting *more* calls, because the

CRTC had been selling the list online to anyone who wanted it for a mere \$50 (Oosthoek, 2009). The reason this was happening was because telemarketers were required to buy the list to know who *not* to call. It did not occur to the CRTC that scammers and other disreputable businesses could also download and exploit the list.

Even though AOL Research and the CRTC had good intentions, the result of their actions was that innocent individuals had their privacy violated. All of these examples show that privacy is not simply about hiding "bad things," (Solove, 2007a) but ensuring that information is not misused, and, that when it is collected and used, it is carried out with the fully informed consent of those involved.

The potential for misuse, reuse and repurposing of information gathered through surveillance increases as digital technologies become widespread. They allow for increased data collection of information about a greater number of individuals, by a greater number of organisations with varied political or ideological orientations and levels of security. Given their built in surveillance features, the integration of SNS into everyday life further increases these risks.

ICT, Surveillance and Privacy

Building on the privacy threat posed by the proliferation of surveillance technologies, this section examines the inherent surveillance-enabling and enhancing properties of ICT and SNS and their subsequent threats to privacy.

The inherent nature of information and communication technologies (ICT) is that they can enable increased surveillance in a number of ways. First, ICT facilitates the recording of otherwise ephemeral actions, which has the added consequence of increasing the sheer amount of data invisibly recorded about individuals. As Nissenbaum describes:

Once in the electronic sphere, the tracks of people's activities may be recorded directly into electronic databases. Electronic transactions, even carefree meanderings (popularly referred to as "browsing" and

"surfing") may be captured and recorded. Information like email addresses, system characteristics, and a trail of network-based activities are not only effortlessly recorded, but easily combined with information from the physical world. In this activity information technology is doubly implicated as it acts as the medium for transactions as well as repository for the information (Nissenbaum, 1998, p. 4).

Consequently, the collection of this information in digital databases can make it more difficult for individuals to control what information is kept about them, as much as how it is used and how it might be disclosed. This means information collected or shared in one context might be revealed in another context where it has the potential to be damaging. For example, one's medical history could be life saving in a medical context, but could damage one's insurability or employability if made public. Another potential privacy threat enabled by ICT is when two or more pieces of otherwise innocuous data are recombined into something damning to an individual. As I showed in the previous section, there are numerous situations where this can occur.

Mediated and networked communication, particularly SNS, rely on the inherent surveillance properties of ICT. For example, the functionality of SNS is built on the ability for the system to record the activities of users, thereby turning otherwise ephemeral activities and communications into reproducible artifacts. In this mode of operation, there is no way for users to opt-out of having their data collected, stored, and shared if they want to use SNS like Facebook. As Palen and Dourish state: "Active participation in a networked world requires disclosure of information simply to be part of it" (Palen & Dourish, 2003).

On SNS, these mediated communications and activities usually contain a high degree of "communication attributes" meaning "all the information that can be learned about a communication, such as when and where it occurred, to whom and from who it was sent and how long it lasted." (Freiwald, 1996, p. 3) On Facebook, for example, public wall conversations show the time, date and author of a post, as well as the intended recipient. It can also be said then that mediated communications are "lossless" --

that is, there is no loss in the quality or detail of information when it is stored or transferred (Floridi, 2005, p. 194).

In her 2002 overview of internet computer-mediated communication (CMC) which focused on pre-Facebook technologies such as email and Usenet, Susan Herring observed similar challenges to privacy posed by ICT, particularly around the persistent nature of text-based online communication. Herring also noted that online communications could be easily observed by invisible parties outside the intended readership of a certain message (Herring, 2002, p. 145).

Building on these basic properties of ICT, it can be said that as mediated spaces, the activities and communications on SNS are thus persistent, transferable, aggregateable, scalable, searchable, and cross-indexable (boyd, 2008c, p. 2; Tufekci, 2008, p. 20). As Tufekci (2008) notes, these properties can lead to audiences who are obscured to users, or who exist in the future. In other words, users do not know necessarily who will be looking at their profile, or even when.

The privacy implication of these properties of ICT are demonstrated in the following scenario. If I post a scandalous story about someone on Sarah's wall, it will be there until she or I delete it (persistence). Before it was deleted, the story could have been copied and sent to many other people beyond my original intended audience (scaleability). My missive, if it spreads far enough, or even if Sarah's profile is open enough, could end up on a page indexed by Google (searchable). If anyone is in doubt as to the truth of the statement, they can Google or search for me on Facebook (or the person in question) to find out more (cross-indexability). Or, as Facebook Inc. states it does in its Terms of Service, they can cross-reference the information you provide on Facebook with other sites you use. The sum of all these conversations and activities can then be collected and analysed by Facebook (aggregateable). Facebook Inc. also has its own records that are not visible to users that keep track of who looks at who, and how frequently; what ads people click on and so forth (Douglas, 2007; Stanford University, 2005). So, even activities that appear to be invisible still leave artefacts of that activity.

Given these properties, SNS can pose a challenge to privacy by facilitating conventional, top-down surveillance, as well as what Mark Andrejevic (2005) calls lateral surveillance as part of its very design. In Andrejevic's model of lateral surveillance, individuals employ the same strategies used by police or marketers in order to gather information on the various people in their lives. Using Friendster as an example, Andrejevic shows how fear and suspicion are employed to normalize and encourage peer-based surveillance: "In an age in which everyone is to be considered potentially suspect, all are simultaneously urged to become spies -- for our own good" (p. 479).

Michael Zimmer (2008b) provides another example of how SNS combined with search engines problematise privacy by increasing surveillance. "Search 2.0," as Zimmer calls it, results in the loss of privacy through obscurity due to the concentration and aggregation of one's online activities. Search 2.0 enables an unprecedented level of top-down surveillance through tracking, aggregation and deep database creation. In the past, bits of personal information were spread across the web. Now, SNS facilitates (and encourages) mass self-reporting of everyday activities in exchange for convenience and social benefits. The massive databases these activities create can now easily be searched, cross referenced, and aggregated using Google. And thanks to the commercialisation of the internet as I discussed in the previous chapter, the information gathered can then be monetised or sold.

Aside from having one's personal information sold to other parties, or used to better target advertising, the potential real-life costs of Search 2.0 are increased disciplinary power through the repurposing of collected data by third parties such as law enforcement; and an increased ability to impose a "panoptic sort" on users (Gandy, 1993), where they are identified, assessed and classified based on their economic value and thus their level of access to goods and services. What makes Search 2.0 even more potent, Zimmer argues, is the allure of social rewards combined with invisible surveillance. Even though most social media requires the sharing of personal information in order to participate, the majority of users do not know they are being tracked or surveilled nor how that information is being used. The design of social media does not make the data collection obvious nor does it provide any

method to opt out. The improvement of one's life thanks to social media is hard to resist, and the invisibility of the potential privacy threats inherent in their use make it easy for users to overlook.

In this section, I have provided a survey and definitions of the related concepts of surveillance and privacy. I showed how ICTs increase surveillance capabilities while decreasing privacy. I have also outlined some of the potential privacy threats arising from surveillance in its various forms. In the next section, I draw on these concepts to conduct an in depth examination of the literature on privacy, SNS and youth.

Literature: Privacy, Youth and SNS

As I have shown thus far, the use of SNS can create increased threats to privacy both from institutional and peer-to-peer surveillance. However, despite the features of SNS which inherently expose users to increased digitally-mediated surveillance by institutions, including the companies behind SNS, much of the research thus far has been on user-created or facilitated privacy threats, particularly with respect to youth (Raynes-Goldie, 2011). The reason for this youth focus, as I have touched on previously, is largely a result of the fact that until recently, SNS were targeted at, and used by younger users. For example, MySpace was initially popular with teenagers while Facebook launched as a college-only site. Consequently, a literature review of SNS and privacy is also unavoidably focused on SNS users under 30. Accordingly, one of the key themes examined in the literature review is the privacy paradox. To provide a more balanced perspective as well as for comparative purposes, I have also taken care to include most of the relatively rare studies on adults, SNS and privacy.

Youth and the Privacy Paradox

Alessandro Acquisti and Ralph Gross were among the first researchers who looked at SNS and privacy, and indeed were the first to specifically look Facebook from a privacy perspective. At the time of their research, Facebook (which was still called "the-facebook"), was still a niche student-only site and had relatively few (9 million) users. In line with the research to follow, their studies (2006, 2005) specifically looked at young Facebook users, in this case, 294 college and high school students.

They were also the first to identify Facebook as a privacy threat due to its large database of user information combined with its culture of sharing and "being yourself." Acquisti and Gross found that although most users express general concerns about privacy, they are unconcerned about their privacy on Facebook. Instead, they worry about *other* people's privacy on the site. They also found that 30% of respondents were completely unaware of the visibility of the information which they had posted on Facebook.

Perhaps most importantly, Acquisti and Gross reported an apparent disconnection between privacy attitudes and behaviours, a concept later named by Barnes (2006) as the privacy paradox. As noted in the introduction to this thesis, the privacy paradox is a foundational concept in this thesis. The term describes a perceived difference in privacy attitudes and reported privacy behaviours of youth, whereby youth put themselves at risk from sexual predation by sharing too much information online. This sentiment was reflected in the MySpace moral panic which was occurring around the same time Barnes' article was published. Overall, Barnes provides a useful summary of the "youth do not care about privacy" thread which runs through most early SNS and privacy research and is still seen today.

Two years later, Zeynep Tufekci (2008) problematised the "students say they are worried but they don't care" and "students say they are worried but they don't know" conceptions of youth, privacy and SNS use. Most conceptions of privacy, she argued, are based on the notion of privacy as total withdrawal. This model does not take into account the benefits of publicity, which gives rise to the apparent privacy paradox. Thus, building a framework based on Goffman (1959) and Altman (1975), Tufekci argued that "a better understanding of this conundrum [the privacy paradox] can be achieved by recognizing that in the self-presentation context provided by these Web sites, privacy should be understood as a process of optimization between disclosure and withdrawal." Using this model to expand on Acquisti and Gross' 2006 study, Tufekci conducted a study with 70 American undergraduates who were users or nonusers of Facebook and MySpace. She found that instead of being completely unconcerned about their privacy, youth knew there were benefits to publicity. Rather than aiming to hide completely, youth attempted to balance privacy and disclosure.

Tufekci's model, then, suggests that the privacy paradox is not a paradox at all. Youth researcher Sonia Livingstone (2008) found similar results in her study, reporting that British teenagers balanced the opportunities and risks in their use of SNS.

Further problematising the privacy paradox, Albrechtslund (2008) argued that the commonly used panopticon-based surveillance framework (largely informed by the public/private dichotomy) has contributed to the misunderstanding of youth privacy behaviours. Such an approach, he argued, yielded moral panics or anger at youth for "oversharing," which get in the way of actually understanding what people are doing on SNS and why. In his theoretically grounded paper which drew on surveillance studies and computer ethics (specifically Andrejevic's (2005) notion of lateral surveillance, see above), Albrechtslund argued that given their characteristics (sharing of activities, preferences and beliefs to socialize), SNS are anchored in surveillance practices and as such, the activities on SNS should be understood as participatory surveillance. Participatory surveillance, he argued, comprises a mutual horizontal practices made up of "the personal information people share -- profiles, activities, beliefs, whereabouts, status, preferences, etc. [it represents] a level of communication that neither has to be told, nor has to be asked for. It is just 'out there'" (2008) Thus, participatory surveillance can be seen as sharing amongst peers rather than as a trade. Counter to the common framing of conventional and lateral surveillance as disempowering, disciplinary and controlling, Albrechtslund argued that participatory surveillance can actually be potentially empowering, subjectivity-building and even playful. Overall, Albrechtslund showed a different aspect of surveillance (the social side), thereby providing insight into what motivates SNS use, despite privacy concerns. In line with Livingstone and Tufekci, Albrechtslund's theory supports the notion that there are benefits to sharing and being public that must be balanced with the benefits of privacy.

In the three years after Barnes' paper on the privacy paradox and MySpace moral panic, Sonja Utz and Nicole Krämer (2009) noted that much had changed in the SNS landscape, in respect to both use and functionality. As I touched on in the previous chapter, they observed that by 2009, SNS had reached mass adoption; online relationships and identities were now usually anchored offline; and mainstream

awareness about SNS and privacy issues has increased as a result of mainstream coverage of the issue. In response, the companies behind SNS began providing users with more granular privacy controls. Based on these changes and the evolution of SNS design and use, Utz and Krämer suggested that previous work supporting the privacy paradox should be taken as "snapshots" rather than static and final conclusions. To update Barnes' work, Utz and Krämer combined short literature review with a three survey-based studies of European SNS users and their privacy attitudes (totalling ~450 participants). Utz and Krämer's studies suggested that a number of important shifts have occurred with respect to privacy behaviours along with the broader changes with respect to SNS that they identified. First, they found that users were actively changing their default privacy settings. Second, they noted that privacy behaviours tended to be influenced by social norms. For example, a given user tended to reflect the same privacy attitudes and behaviours as their network of friends. Thirdly, Utz and Krämer observed that in some cases, increased narcissism decreases privacy protection (but not always, such as with respect to making an email address or mobile number public.) Broadly, Utz and Krämer's research supports Tufekci's findings that users balance the costs and benefits of disclosure and privacy. For example, the more concerned users were about reaching a large audience and leaving a positive impression, the less restrictive their privacy controls were.

Building on the emerging body of scholarship that identified younger users as balancing the benefits and challenges of publicity with a desire to be private, Petter Bae Brandtzæg, Marika Lüders and Jan Håvard Skjetne (2010) presented an updated model of the privacy paradox: the privacy dilemma. This model is based on the idea that content sharing and sociability are the most important success factors of an SNS. The more privacy is protected the harder it is to be social or to share content. Likewise, less privacy makes it easier to share and be social. Complicating matters further, users tend to share more if they feel they can trust who they are sharing with, which involves some degree of privacy. This dilemma causes a problem for designers because sociality and content sharing are core to the current design of SNS, and yet users also want and need privacy. In this way, the aims of the companies behind SNS can differ from the needs and desires of users. As I show in this thesis, this

divergence between the goals of Facebook and its users is one of the reasons users are facing increased privacy risks.

More recent work on SNS, youth and privacy contrast with the early work of Barnes and Acquisti and Gross. There are a number of potentially overlapping reasons for these differing results, all of which challenge the black and white nature of the privacy paradox. The first is that privacy and attitudes are changing, as noted by Utz and Krämer (2009) and a number of other studies. Lampe et. al (2008) noted that use of privacy controls have increased significantly from 2006 to 2008, when their study was conducted. danah boyd and Eszter Hargittai (2010) reported a similar increase between 2009 and 2010.

Another potential cause of changing privacy findings may be a significant change in functionality. At the time of Acquisti and Gross' research, Facebook was a student-only, closed community with straightforward privacy settings, with defaults generally set to protect privacy. In this early Facebook users, understandably, would be less concerned about privacy since potential risks were much less than the version of Facebook examined in later studies which was open to everyone, had more confusing privacy settings and generally set information to be public by default. As Tufekci's study and my own fieldwork show, perceived changes in privacy behaviour may also be due to a change in the understanding of what privacy means, thereby calling for a change in the way researchers frame their questions. As the privacy dilemma suggests, there are benefits to being public, such as building social capital, so the reasons that youth may choose to be less private can not simply be reduced to a lack of concern or knowledge. Finally, boyd and Hargittai (2010) note that the varied reports of some users taking measures to protect their privacy while others do not might be due to gender differences or the confusing design of privacy settings which cause users to think they are using settings appropriately, when in reality they are not. The complicated nature of privacy as evidenced by a changing suite of features, understandings and behaviours further underscores the need for research that is recontextualised, that is, that takes into account designers and users as well as the offline, physical context in which they inhabit. In Chapter 8, I bring together these findings with the conclusions from my field work to revisit the privacy paradox.

Adults

Despite these numerous findings which challenge the privacy paradox, it is still a pervasive narrative (boyd & Hargittai, 2010) which perhaps obfuscates the risks for adults. Indeed, very little work has been done on adults, privacy and SNS. For example, Palen and Dourish (2003) provide one of the few early examples that looked at adults and privacy in a "networked world." Yet, more recent research challenges the very notion that youth are more risk than adults.

Brandtzæg et al.'s (2010) study on the privacy dilemma also contained some important findings with respect to adult users. Brandtzæg et al.'s employed a novel approach that combined in-depth interviews with Norwegian adults and youth with a usability study. Such an approach, especially with respect to the comparison of young and old users, is probably the first of its kind in SNS, privacy and surveillance studies. As the authors note, the rapidly increasing use of SNS by adults since 2005 make such an approach necessary. The authors found that even though adults believed youth to be more open and prone to privacy violations, young people were actually more aware of strategies to maintain their social privacy than their adult counterparts. One of these tactics, the authors note, is social conformity, which "occurs when an individual's actions are exposed to increased visibility or surveillance by other members of a group (e.g., "followers" on Twitter and "friends" on Facebook)" (p. 1011-1012).

Brandtzæg et al.'s findings are supported by a Pew Internet study (2009), based on 2 surveys of 2,253 adult Americans. The areas of the report where age groups were compared suggest that privacy attitudes among teens and adults are not drastically divergent. However, younger people are still far more likely to have an SNS profile than their older counterparts. Specifically, the survey found that "most, but not all adult SNS users are privacy conscious." And while adults are generally more aware than teens of potential privacy threats on SNS from other people (such as being found or identified), the difference between the two groups is rather small. Indeed, teens were actually *more* likely than adults to believe that with enough work, a stranger could identify them from their SNS profile. The report also provides a valuable look at the uptake of SNS among adults, the use of multiple profiles, the

purpose of use (social or professional) and the age-based SNS preferences. Combined, these two more recent studies suggest that the common conception that youth are privacy unconcerned is an oversimplified generalisation. Indeed, a report on youth privacy by the London School of Economics from that same year concluded that "youth experience the same opportunities & challenges as everyone else who uses digital technologies" (Beckett, 2009).

Critical Perspectives

Despite the more critical perspectives towards youth and privacy as examined thus far, there still exists a dearth of research which critically examines the companies behind SNS, especially ideologically or discursively. In a response to boyd and Ellison's (2008) influential survey of the history and scholarship of SNS thus far, David Beer (2008) argues that the focus on users (supported by the research agenda that boyd and Ellison call for) ignores the critical role of the structures that create and shape these sites, both literally and rhetorically. Beer states that researchers must also examine the companies that make SNS, advertising strategies, software designers, third party users, and, more broadly, the role of capitalism and capitalist interests in the design of SNS. Most critically in the context of surveillance and privacy, he argues, researchers must examine the "motives and agendas of those that construct these technologies in the common rhetoric of the day" (p. 526).

As I touched on in Chapter 1, this user-focused approach is not new. Writing before the launch of Facebook and MySpace, Fuller (Fuller, 2003) noted that the prevalent "myth of technology as neutral" has discouraged critical, social, and political theorists from seeing software as a valid conceptual domain of study, thus creating a general lack of critical research in this area (p. 16). However, in the years since 2006 there has been a slowly emerging body of critical SNS scholarship. The growth of this approach which has been further gaining momentum since I began my fieldwork in 2008.¹⁶ This increasing interest may be due to the widespread coverage that

16. For example, in 2008, *First Monday*, one of the key internet research journals, published a special issue on critical perspectives of Web 2.0. In 2010, Facebook and privacy researcher Michael Zimmer put together a panel Internet Research 11, the annual conference of the Association of Internet Researchers, entitled *On the Philosophy of Facebook*. Zimmer has also blogged extensively about

Facebook received in May 2010 as a result of significant privacy changes to the site. Perhaps fueling the fire, Zuckerberg defended the changes by arguing that social norms had moved towards being more open and less private (boyd & Hargittai, 2010).

Writing during the height of generally unreflective excitement about the revolutionary potential of the internet and "Web 2.0," Canadian researcher Ryan Bigge (2006) provided one of the first academic critiques of SNS. Bigge looked at the personal costs of the use (or non-use) of social networking services within the broader context of capitalism. For Bigge, SNS are problematic because they commodify social relations, encourage self-surveillance and engage users in free digital labour, such as creating and maintaining their profiles and networks. It is this digital labour that creates the sociotechnical capital which represents almost the entire value of MySpace. Despite the value they create, MySpace users do not own their profiles; MySpace does. Bigge also notes that non-participation in social media comes at a very high cost: self-negation ("you do not exist"). As I touched on in Chapter 1, Bigge thereby presents a nuanced argument for an alternative perspective on SNS that runs counter to boyd's (2006a, 2006) earlier work. While boyd argues that SNS are emancipatory for teens -- they offer youth who are coming of age a much-needed space to play and develop their identities, a place to express themselves and build cultural knowledge -- Bigge argues SNS sites are actually oppressive. These sites act as a form of digital enclosure where users engage in unpaid digital labour in the form of self-generated surveillance. The output of this labour is massive amounts of personal data that can be surveilled, repurposed, datamined and sold. Furthermore, Bigge argued, even if one is concerned about one's privacy or the commodification of one's identity, opting out is not an easy choice. For Bigge, "membership [has become] a necessity, rather than an option." The social costs of non-participation are essentially that one does not exist (a fact proudly reported by Facebook co-founder, Chris Hughes). This observation also provides a deeper conception of the reasons why, despite privacy or surveillance concerns (as described

Facebook's "philosophy of information."

by the privacy paradox), users still use SNS. Finally, Bigge proposes an examination of the companies behind SNS, rather than the overwhelming focus on users which is still prevalent today.

Fred Scharmen (2006) is concerned with identity, interaction and ownership in the context of commodification and control on SNS. Like Bigge, Scharmen points out that users of social media create free content that can be repurposed, resold or used to sell things back to its very creators. Concerns about digital labour were also raised by Tiziana Terranova (2003) who wrote about these issues in the context of AOL's "volunteer" chathosts who decided, back in 1999, that they wanted to be compensated for their years of unpaid labour. Even though she was not writing explicitly about what is now called social media, Terranova's critique anticipates many of the concerns raised by Scharmen and Bigge. Terranova also provides a more broad critique of the political economy and culture behind SNS companies, such as the problematic blending of capitalism and the gift economy as promoted by the open source movement which is now also evident in Facebook.

In his Master's thesis, Marc Stumpel (2010) also critically examines the business model of Facebook, particularly around the commodification of user information through datamining and targeted advertising. He analyses Facebook Inc.'s use of discursive strategies and frames to support its continual push towards increased sharing and decreased privacy, thereby facilitating the collection and monetisation of user data. In light of the vast majority of SNS research which focuses on users and user behaviour, Stumpel's focus on the company behind Facebook itself provides valuable insight. By shedding light on Facebook's ideology of "openness and transparency" (along with Michael Zimmer (2010a), who was among one of the first researchers to do so) Stumpel provides a useful context for understanding why Facebook makes the privacy decisions it has. Zimmer and Stumpel set the groundwork for my thesis project, which further unpacks the discourse of Facebook through an examination of its historical roots in the California Bay Area. To my knowledge, no one has yet explored this connection or taken this approach in understanding Facebook's privacy architecture and discourse.

Other critical work of note includes research from the Toronto-based Infoscapes Research Lab (IRL), which also looked at how the "informational politics" (Rogers, 2004) of Facebook shape and constrain the activism and political participation that are carried out through the site (Langlois, Elmer, McKelvey, & Devereaux, 2009). They also note that while users are given new avenues for engagement they are exposed to new surveillance and privacy threats.

Along with these critical analyses of SNS, other scholars have examined social media and Web 2.0 more broadly, such as Matthew Allen (2008, 2009, 2011) who has critically examined the rhetoric and construction of Web 2.0; Alice Marwick (2010) who unpacked the historical roots of Web 2.0 culture; Trebor Scholz (Scholz and Hartzog, 2008; Scholz, 2008) who has examined the political economy of social media and Michael Zimmer (Zimmer, 2008a; Zimmer, 2008b); who, in addition to Facebook, has critically analysed search engines as they connect with personal information streams from SNS.

Framework: Contextual Integrity and Social Privacy

In reviewing the American privacy surveys -- conducted by Alan Westin and Harris Interactive -- from the late 1970s until recently, one can see that privacy has been largely understood as *informational* and *institutional*.¹⁷ In other words, if one were to ask a person about privacy they would frame their response based on how institutions such as governments, banks and other businesses, use or misuse their personal information. Prior to the mainstreaming of SNS, a good deal of academic work on electronic surveillance and the internet reflects this stance, as evidenced by the conception in the literature of privacy threats as originating from institutions, such as from governments or large corporations.

However, the features of ICT have necessitated a rethinking of current privacy definitions and models. As my review of the literature shows, multiple findings (2009; Tufekci, 2008; Livingstone, 2008) support the privacy dilemma model (Brandtzæg et

17. See (Gandy, 1993; Kamaraguru & Cranor, 2005) for excellent in depth discussions and analyses of Westin's body of research.

al., 2010) whereby users attempt to optimise public sociality with privacy rather than seeking absolute solitude. Furthermore, common conceptions of privacy -- especially with respect to surveillance -- are based around concerns about institutional gathering and (mis)use of private information. And yet, the widespread use of SNS combined with its inherent surveillance enhancing features, privacy violations are increasingly coming from other individuals. Andrejevic (2005) and Albrechtslund (2008) point to this trend in their notions of lateral or peer-to-peer surveillance, where individuals, facilitated by SNS, watch each other's activities. These findings suggest that panopticon and strict public/private dividend models of privacy (2008) -- where threats primarily come from institutions -- are outdated.

Accordingly, this thesis employs a notion of privacy that emerged based on observations from my fieldwork. Earlier in this chapter I provided a scenario where I posted something scandalous to a friend's Facebook wall. Privacy was challenged in two ways. The first was an institutional threat from Facebook Inc. in its collection, storage and aggregation of all the communications and activities on the site, thereby creating large databases of personal information about users which can be monetised or used well beyond its intended purpose, such as for law enforcement. The second was a different sort of threat. My wall post could have tarnished the reputation of the person whose wall I posted it on. It could have been copied and sent around to other individuals, such as an employer or a significant other. If no one deletes the post, it could exist for a long time, potentially harming the individual's reputation in the future. This second kind of privacy is one that centres around what I call *social* privacy.

Social Privacy

Social privacy encompasses two things: the management of what is disclosed about oneself to others (also called identity or reputation management) and the ability to navigate and manage various social contexts. Social privacy is threatened when the regulation or management of either of these things are threatened. The identification of social privacy as distinct from institutional privacy is increasingly necessary given the inherent social privacy threats built into SNS. As I flesh out in Chapter 7, with evidence from my fieldwork, while institutional privacy is about data management

and protection with respect to institutional use, social privacy is the management of identity, reputation, and social contexts.

Even though not explicitly described as such, my social privacy distinction has prior precedence. Prior to the advent of SNS, Judith DeCew (1997, pp. 75-76, 77-78) wrote about what she termed expressive privacy, which concerns the protection of personal information, such as one's daily activities, finances, lifestyle and so forth. Expressive privacy, then, is the desire to protect oneself from the influence of peer pressure or ridicule and to be free to express and control one's own identity. It is the ability to control what is said about oneself. In the same way, a 2010 Pew Internet study framed privacy concerns as reputation management (Madden & Smith, 2010). In 2003, Palen and Dourish also identified the contextual management aspect of privacy. In their words, privacy is not "simply a way that information is managed, *but how social relations are managed*" (emphasis mine) (p. 327). As with most of the implications of SNS, social privacy is not novel in itself. What is novel is the increasing likelihood that individuals will face social privacy violations in their everyday lives.

Contextual Integrity

Conventionally, definitions of privacy have not taken into account social privacy violations. As I have shown, in the United States, privacy is only legally violated if the information exposed was deemed to have been private (Solove, 2007b). However, most information shared on Facebook could be deemed public information (especially if the profile was being used in its default, open state), even if it was shared beyond its intended audience.

Without yet making clear a distinction between social and institutional privacy, researchers have wrestled with this problem, as reflected in the privacy dilemma. Most notably, a number of researchers have drawn on Irwin Altman's model of privacy as the optimization of disclosure and withdrawal (Altman, 1975), so that privacy becomes about disclosure management, rather than simply privacy as wanting to be left alone (e.g. Tufekci, 2008; Palen & Dourish, 2003).

The model I have found most useful and nuanced in the context of the findings from my fieldwork has been Helen Nissenbaum's (2010) contextual integrity. Contextual integrity is based on a model of privacy as disclosure management and optimisation rather than total withdrawal. This model, which has also been used by fellow Facebook privacy researcher Michael Zimmer, provides a framework that avoids the problematic public/private dichotomy by creating a nuanced framework that takes into account social privacy violations.

As I have noted, the common legal conception of privacy is the protection of that which is not public. Yet, even before the advent of ICT, this seemingly clear distinction had been challenged by the problem of privacy in public, where individuals want or expect privacy in public but are not legally protected (such as celebrities attempting to avoid the paparazzi). It is a problem which, like my conception of social privacy, has been largely overlooked or ignored (Nissenbaum, 1998). For Nissenbaum, ICT exacerbates this problem further in its facilitation of the gathering of private information in public spheres: "information and communications technology, by facilitating surveillance, by vastly enhancing the collection, storage, and analysis of information, by enabling profiling, data mining and aggregation, has significantly altered the meaning of public information." (Nissenbaum, 1998) In other words, public records are made even more public as a result of IT (Nissenbaum, 1998, p. 16).

Nissenbaum argues for a different conclusion to be drawn about the academic portrayal of privacy as muddled and vague. The meaning of privacy *is* multiple, she argues, but that multiplicity is the point. Privacy expectations and norms are related to the social situation in which they arise. The meanings of privacy are varied, but with contextual privacy they can be made sense of. So instead of giving up and saying privacy cannot be defined, Nissenbaum is essentially arguing that the variedness of privacy definitions and understandings are part of the very nature of privacy (Nissenbaum, 2010, p. 1).

Contextual integrity can be used to explain violations of privacy that, by traditional conceptions of privacy based the public/private-based model, are not considered violations of privacy at all. For Nissenbaum, proper privacy design respects social

contexts and context-relative informational norms "which prescribe the flow of personal information in a given context, [and] are a function of the types of information in question" (pp. 127). When these norms are ignored, it is experienced as a violation of privacy (or in Nissenbaum's terms - a violation of contextual integrity). In applying Nissenbaum's contextual integrity to SNS, one can see that they threaten privacy because they violate contextual informational norms by mixing surveillance and social life. Users share their information on Facebook in the context of socializing. However, they are not expecting to have the company behind Facebook surveilling them or using that information for purposes unrelated to social activities.

In this chapter, I provided an overview of emerging privacy threats and the drawbacks of conventional definitions and models. Combined with social privacy, contextual integrity provides a more helpful, alternative model of understanding privacy in the age of Facebook. As I have shown in the introduction to this thesis, it is not uncommon for journalistic and public narratives to frame SNS users (especially youth) as entirely responsible when their privacy is violated. Often, the strictly delineated public/private dichotomy is invoked to support these narratives, with the refrain being along the lines of "you made that information public by putting it on Facebook -- what did you think would happen?" In so doing, such an approach denies social privacy challenges, such as needing to balance the benefits of publicity with privacy. Overall, contextual integrity provides a model whereby social privacy violations, which are not otherwise legally acknowledged, are actually considered to be valid privacy violations. Broadly, then, contextual integrity provides a framework where the privacy issues faced by Facebook users can not only be taken seriously, but they can be opened up for analysis.

Chapter Four: Opening Facebook

This chapter charts the historical evolution of Facebook both as a company and as an SNS. Unlike physical field sites, Facebook is constantly and rapidly evolving, with design, feature and policy changes occurring on a fairly regular basis. Accordingly, Facebook's dynamic posed logistical challenges for my research, particularly around documentation and boundary setting. For this reason, I focus primarily on the time period beginning with Facebook's launch in 2004, until 2009, when my fieldwork was complete. To match with my fieldwork findings, the features and policies described in this chapter are circa 2008, unless stated otherwise. Where it is relevant, I will also describe more recent changes up until the time that this thesis was near completion at the end of 2011.

Through a survey of the cultural and design changes on the site with a particular focus on privacy, this chapter provides the context for understanding how the belief systems which inform Facebook -- as examined in the next chapter -- has shaped the site's privacy architecture over time. This chapter also provides a snapshot of Facebook as it was in 2008, and thus a picture of Facebook as a field site during that time. This snapshot provides a helpful foundation for the presentation and analysis of my fieldwork findings in Chapter 7 and 8 where I examine the consequences for, and meaning of, privacy in the age of Facebook. Overall, even though Facebook will continue to change long after I have finished this project, my hope is that this chapter will become a useful historical account of Facebook's earlier years which will be of benefit to future researchers.

I will begin with a historical and financial overview of Facebook Inc., followed by a survey of the features and design of the site itself with particular focus on their evolution over time. I conclude with an in depth examination of Facebook's privacy settings and policies and evaluate them in the context of Canadian privacy law. Overall, I chart a shift on Facebook's features, design and policy from being a closed, student-only site, to a mainstream SNS, used by individuals from all walks of life. Through-

out this process, as I will show throughout this thesis, Facebook has moved towards less privacy for users.

Facebook: the Company

As Facebook has grown in popularity, so too has curiosity about the founding story of the company behind it. However, when I began this research project in 2008, nothing substantial had yet been written about Facebook Inc., save for a little known self-published account by early Facebook engineer Karel Baloun entitled *Inside Facebook: Life, Work and Visions of Greatness* (2007). While this account of the early days of Facebook was tremendously helpful in providing insight into the culture of Facebook Inc., it was largely critically unreflective. At some points Baloun almost fawns over Zuckerberg, for example he compares the Facebook founder to a "Greek god" (p. 23). As Facebook became popular, the number of books documenting or analysing Facebook Inc. as a business started to grow. Most notable were two books by technology reporters: Sarah Lacy's *Once You're Lucky, Twice You're Good* (2008), which examined a number of Silicon Valley companies including Facebook Inc., and David Kirkpatrick's *The Facebook Effect* (2010), which as the name suggests, was entirely focused on on the site and the company behind it. But Facebook Inc.'s legendary status was sealed by Aaron Sorkin's 2010 cinematic account of the early years of Facebook Inc. in *The Social Network*. The film, heavy with factual inaccuracies, was based on the more accurate *The Accidental Billionaires* (2009) by Ben Mezrich. Mezrich wrote his book almost from accounts of people never or no longer employed by Facebook Inc., acts as a counterbalance to Lacy and Kirkpatrick's work -- both of whom had access to Facebook Inc. employees as well as Zuckerberg himself. Augmented with technology blogs, newspaper articles and communications from Facebook Inc., I have used these works as sources for the factual information in this chapter. In this section, using these sources, I examine the founding and revenue model of Facebook Inc.

Early days: Facemash and ConnectU

Facebook was launched in February 2004 out of Mark Zuckerberg's Harvard dorm room while he was still an undergraduate. Even though Zuckerberg is usually credit-

ed as being the sole founder of Facebook, he actually co-created the site with the help a few of his friends: Chris Hughes, Dustin Moskovitz and Eduardo Saverin, who also provided some of the initial capital (Facebook, 2011; O'Brien, 2007; Philips, 2007).

Before Facebook, Zuckerberg was involved in the creation of two similar sites, both of which were not only surrounded by controversy and questionable ethics, but were also critically linked to the later founding of Facebook. The first was Facemash, which presented users with photo pairs of Harvard students for ranking based on attractiveness (Baloun, 2007, p. 16). Essentially, Facemash was a college version of Hot or Not, a site popular in the early 2000s which allowed users to upload their photos for rating by other members. The critical difference, however, was that while Hot or Not was opt-in, those being ranked on Facemash had no choice in the matter. Facemash was only live for four hours in late October 2003 before it was shut down by Harvard (Staff, 2003). Despite its short life span, the site garnered 22,000 hits from 450 people (Baloun, 2007, p. 16). Aside from deeming the site as mean-spirited, Harvard was displeased about the way Zuckerberg had obtained the photos which were rated on the site. He had gained unauthorized access to photos of almost every undergraduate students by hacking the school servers and then copying the photos from the house photo directories, also known as facebook (which was ultimately inspired the name of Facebook itself) (O'Brien, 2007). Not only were the individuals ranked on the site unwilling participants, their photos had been stolen. In response, Harvard put Zuckerberg on academic probation (Goldstein, 2007).

Further incriminating Zuckerberg was the digital trail he left behind as he made Facemash. During his development process for Facemash, Zuckerberg documented his activities on a public blog where he mused about comparing students with farm animals.¹⁸ His diary also suggests that Zuckerberg started the project to keep his mind off a young woman, who he claimed was being "a bitch" (Zuckerberg, 2003).

18. *The Social Network* portrays Zuckerberg keeping this blog under the username "zuckonit" on LiveJournal, an early SNS and blogging platform that is, in many ways, a cultural predecessor to Facebook. However, it is unclear if this was artistic license on the part of the filmmakers.

Even though Zuckerberg took this blog offline, its contents re-emerged as evidence in his legal battle with ConnectU, as I will discuss shortly.

The profile Zuckerberg gained with Facemash caught the attention of three other undergraduates who were working on a social network site for college students, originally titled Harvard Connect, which was later changed to ConnectU. The site was the brainchild of Divya Nerendra and his twin brother friends, Cameron and Tyler Winklevoss (O'Brien, 2007). Just weeks after launching Facemash, Zuckerberg was enlisted by the three undergrads to start coding the ConnectU site (O'Brien, 2007). What happened next was of much debate and was the cause for an ongoing series of court cases between Zuckerberg and the ConnectU team, the first of which was settled in early 2008 (Levenson, 2008). The conflict was also a key narrative point of *The Social Network*, which left the story ambiguous but painted a rather negative picture of the Winklevoss twins. Nerendra and the Winklevosses contend that Zuckerberg made himself nearly impossible to reach, but kept promising that the site would soon be ready to launch. In January 2004, Zuckerberg told the ConnectU team he was working on another project, and by February Zuckerberg and a team of friends had launched Facebook (O'Brien, 2007). The ConnectU team contends that Zuckerberg stole the source code from ConnectU to build Facebook (Maugeri, 2004). According to Luke O'Brien's article on the case, which was based heavily on court documents:

The similarities between Facebook and the concept for Harvard Connect are abundant and obvious, and the plaintiffs have accused Zuckerberg of stealing several ideas, including: the concept of an on-line social network for the college community; registration with .edu e-mail addresses to encourage users to enter accurate information into their profiles; grouping users by schools, starting with Harvard and then moving on to the rest of the Ivy League and beyond, and allowing them to connect to other groups; letting users adjust privacy settings within their groups; allowing users to request connections with other users; enabling people to upload, post, and share photos, videos, and information and exchange goods such as books or personal items (O'Brien, 2007).

Facing a legal threat from Facebook Inc., the court documents (including the Face-mash blog posts) which O'Brien included in his article have since been removed, along with the article itself (Swisher, 2007). While the ConnectU case will likely never be conclusively resolved, it can be justifiably argued that the creation of Face-mash is reflective of some questionable activities and attitudes, particularly concerning privacy and the respect of users. As I show in this thesis, Zuckerberg's activities before Facebook hint at the way in which Facebook Inc. would later conduct itself.

Revenue Model

In its early days of the site, Facebook Inc. made its money from "super fancy" targeted ads based on the information users gave about themselves; sponsored groups, events, notifications and flyers (Baloun, 2007, pp. 66-68). The company also received a great deal of venture capital, beginning with \$12.7 million in funding from Accel Partners in 2005 and \$27.5 million from Greylock Partners, Meritech Capital Partners in 2006 (Facebook, 2011). Facebook also made advertising deals with partners such as Microsoft, who bought a \$240 million equity stake in the company in 2007, giving them 1.3% ownership. Throughout this period until the time of writing, Facebook Inc. has experimented with different forms of advertising, such as social ads and the ill-fated Beacon in 2007 (Pearlman, 2007). Advertising is still a key revenue stream for Facebook Inc. Sales of banner advertising accounted for half of the company's revenue of \$500 million in 2009, which was also the first year in which Facebook Inc. was cashflow positive (Carlson, 2010) In 2010, Facebook Inc.'s advertising revenue reached \$1.86 billion (O'Dell, 2011).

At the time of writing, Facebook is still privately held, but there are strong indications that Facebook is planning an initial public offering (IPO) in May 2012 (Schaefer, 2012). At the time of writing, the significant owners of the company include Zuckerberg with 24%, Accel Partners with 10%, Digital Sky Technologies with 10%, Dustin Moskovitz with 6%, Eduardo Saverin with 5%, Sean Parker with 4%, and

early angel investor Peter Thiel with 3%. In 2011, Facebook Inc. has 750 million users is valued at as much as \$100 billion (Carney, 2011).

Facebook: the SNS

"Facebook is a natural extension of our daily human interaction, online."

- Facebook promotional video, SXSW 2008

When Facebook was first launched in 2004, the site was essentially an interactive, online version of the paper-based facebook¹⁹ around Harvard. Accordingly, the original name for Facebook was actually "thefacebook" which, appropriately, resided at thefacebook.com. This digital facebook allowed students to see who they shared classes with, find more information about people they were interested in as well as develop new friendships. As Baloun claims, the early Facebook largely designed to facilitate sexual encounters (Baloun, 2007, p. 91). According to Zuckerberg in 2007, he intended for Facebook to "make it really efficient for people to communicate, get information and share information" (Locke, 2007). Just as it has become for the general public, Facebook served as a kind of third space for the Harvard student body. Today, Facebook is a richly featured service aimed at facilitating social interactions for anyone and everyone. In this section, I examine what Facebook is, what it does and how it is used in everyday life.

Features and Design

The foundation for all the activities on Facebook are individual profiles for each user which are linked together by people who are listed as Friends.²⁰ Indeed, the profile and the Friends-list reflect the two core activities on any SNS: self-presentation and the maintenance of relationships (Utz & Krämer, 2009). The Friends-list is a publicly viewable list of a given user's Friends, and can be browsed or surfed by other

19. Paper facebook^s were literally just that: books of head shots which were put out by each dorm, so that students could get to know each other better

20. I use 'Friends' to distinguish Facebook Friendship from the conventional definition of friendship.

Friends. Users can send each other Friend requests, which come with only two options: Accept or Ignore. On other SNS such as Twitter, LiveJournal and the newer Google+, one user can follow or be Friends with someone who does not follow them back. On Facebook, Friendship must be reciprocated. The profile is made up a series of text boxes that a user fills out in order to articulate and share their identity with other Facebook users, and includes demographic and personal information as well as photos and a list of Friends. The linking of profiles is what forms a social network which generally reflects the physical yet ephemeral social network of the individuals in a user's life. As Albrechtslund (2008) describes, profiles allow Friends to passively or ambiently interact with one another, gathering information invisibly.

Compared to other services in the same genre, such as MySpace, Facebook has a clean, minimalist design based on a blue and white colour scheme. Starting out simply, Facebook's design has grown increasingly complex and feature-rich throughout my research. In an attempt to maintain its relative minimalism, Facebook gives users very little control over how their profiles look beyond the information they share or the third part applications they add, such as games or quizzes.

Defining Facebook

Facebook has the three defining features of an SNS: profiles; Friends lists and comments; and a move away from place (virtual cities, homepages) as a mode of organisation, which was a common navigation metaphor in online communities around the turn of the millenium (Zoolers, 2009, p. 603). In lieu of place, Facebook uses metaphors related to people and identity, as reflected by the focus on the profile as the key element of interaction. This has also been called egocentric networking (Wellman, 1993). Accordingly, Facebook users network with people they already know, sharing activities, preferences and beliefs as a means to socialize (Albrechtslund, 2008). Facebook also meets boyd and Ellison's definition of an SNS (2008), as a "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."

While the consensus among researchers and the mainstream press seems to be that Facebook can be classified as an SNS, Zuckerberg disagrees. In the early years of Facebook, Zuckerberg insisted on defining the site as a "social utility," as clearly distinct from an SNS. Reflecting Beer's sentiment that boyd and Ellison (2008)'s definition of SNS was too broad and slippery, Zuckerberg told *Time*:

I think there's confusion around what the point of social networks is. A lot of different companies characterized as social networks have different goals — some serve the function of business networking, some are media portals. What we're trying to do is just make it really efficient for people to communicate, get information and share information. We always try to emphasize the utility component (Locke, 2007).

Zuckerberg's definition was also reflected in the official term used on the front page of Facebook in earlier years and is can still be seen on their press release page: "Facebook is a social utility that helps people communicate more efficiently with their friends, family and coworkers" (Facebook Inc., 2011). To this utilitarian end, Facebook Inc. began branding itself as a "social operating system," like a version of Windows, but instead of running software it runs your social life (Gannes, 2007). As I will demonstrate in the following chapters, this approach to social interaction as improved by increase efficiency and information sharing can have a profound effect on the privacy of users.

Taking a different tack than earlier online communities, including early SNS such as LiveJournal or Friendster, Facebook is much more focused on nonymous, fixed identities -- in Facebook Inc.'s terms, "authentic" identities. As such, interactions on the site are usually between people who have already met in person, and who use Facebook to grow and maintain those relationships. Studies of American undergrads at number of American universities found most participants did not use Facebook to meet new people (Bumgarner, 2007). Consequently, instead of using an alias, people tend to be their physical, anchored identities on Facebook and will share lots of accu-

rate personal information. In this way, Facebook is "identity rich" (Baloun, 2007, p. 71).

These sort of authentic relationships are still often (somewhat erroneously) described as "offline relationships," but as I noted in Chapter 2, the online and offline has become increasingly overlapped as a result of a number of factors. The anchored relationships and identities on Facebook reflect this shifting landscape (Zhao et al., 2008).

Using Facebook

In my fieldwork I observed a variety of activities on Facebook. Participants chatted with their friends; looked at photos of someone they had a crush on; found things to do on the weekend or played a game of Scrabble. Kirkpatrick (2010a) reports similar activities from his interviews with early Facebook users. Based on these activities, Facebook's affordances can be generally placed into three categories. The first is the basic social networking features: a profile page and a list of Friends. Users fill out a profile with personal details and build their social networks by "Friending" or "adding" people. The participants in my study were continually adding new Friends as they make new acquaintances in their everyday lives. They would also continually update their profile pages with status updates, new profile photos or by becoming Fans of new things. The Friend network forms the foundation for the rest of the features of the site, such as communicating, which is the next category. Users can send private messages, write public messages on the walls of their Friends (which appear on the profile page) or comment on the things they upload. The third and final category is link and media sharing. Users can post photos, hyperlinks, videos or notes (which are similar to blog posts) to their profile which are then viewable to Friends. The most popular of the media sharing features on Facebook is photos (Schonfeld, 2009), which people use to share their lives, and observe the lives of their Friends. The communication and sharing aspect of Facebook are what make up the core activities on the site.

During my fieldwork, Facebook was mainly used in the English speaking world, especially Canada, the United States, the UK and increasingly Australia. However, in 2008, Facebook began releasing multilingual versions of the site to compete with sites like Friendster, Orkut and Hi5, which are the dominant equivalents in non-English speaking countries (Bonfils, 2011).

The Evolution of Facebook

Facebook is continually evolving and has changed dramatically since it was first launched in 2004. Like the other early SNS such as Friendster, Facebook started out with relatively simple features. Like its competitor MySpace, what set Facebook apart from other early sites, however, was that the company continually added new features and tweaked the site design (boyd & Ellison, 2008). In contrast, after a user added all his or her Friends on Friendster, there was really nothing to do with that meticulously created list. Facebook and MySpace went beyond this basic functionality, and leveraged the list to make it a user's audience, a contact list, a source of information and entertainment. This constant change not only drastically changed how the site worked, but also kept users entertained and engaged (and sometimes made Facebook users angry -- as I discuss in Chapter 6). Inevitably, MySpace and Facebook became the two most popular SNS, with Facebook recently taking the lead.

Even though Facebook has constantly evolved and changed since it was first launched in 2004, there is a clear trajectory that can be summarized in terms of access, audience and information. Facebook has moved from being a closed, student-only SNS, to a service that is open to anyone with an email address. In the process, the audience has changed from students to everyone. And finally, the information on Facebook has moved from being ephemeral to artifactual. In this section, I examine Facebook's evolution through a chronological survey of the site key features.

Early Facebook: Students only

While known as "The facebook," Facebook was launched as a Harvard-only service. By requiring a Harvard email address to register for the site -- something only those actually at Harvard would have -- Facebook essentially created a walled garden

which kept its community secluded from the rest of the internet. Awareness of site spread virally and new users joined at a rapid pace. Within 24 hours, the site had 1,200 registered users and within a month over half of the undergraduates at Harvard had joined (Philips, 2007). Within a month, Facebook was opened to Stanford, Yale and Columbia. Shortly after, Facebook expanded to all the universities in Canada and the United States.

Facebook's early success can be attributed to its leveraging of the strong and pre-existing (offline) social networks that exist within college and university communities. These social networks facilitated the rapid spread of knowledge about the site but also demonstrated the immediate usefulness of Facebook as a social tool. As Baloun (2007, p. 85) reported from his time working at Facebook in the early days:

Facebook won the college space because it enabled college students to interact with their natural college communities, and only with those communities. Each college was isolated and protected from the rest of the internet, sharing a safe private space. Building on natural existing communities leverages the inherent feeling of trust among their members (p. 85).

By requiring new user to provide an approved school email address, thereby proving their student status, Facebook provided a safe and seemingly private space to grow and maintain relationships. It was seen as a space away from the prying eyes of parents, school administrators and employers. This meant users were comfortable sharing a lot of information that they would not in other SNS:

On Friendster, and especially on MySpace, some users are playing roles: thirteen-year-olds pretending to be nineteen, virgins pretending to be vixens, forty-two-year-old F.B.I. agents pretending to be adolescent girls. Because Facebook users were required to have a valid Harvard e-mail address, most were students, and many were willing to post their e-mail and home addresses, their cell-phone numbers, and even their sexual orientation (Cassidy, 2006, p. 2).

As I outlined on in Chapter 2, in the past fifteen years, there has been a significant shift in the way the internet is used, whereby offline identities and relationships became increasingly overlapped with their online counterparts. By leveraging its unique position on college and university campuses, Facebook built on and then helped to further push these changes. In offering students ways to connect with individuals they already knew offline, Facebook gave students a reason to share their personal details on the site, thereby being their "real", "authentic" selves. In this way, Facebook enabled an increased overlap between the on and offline spheres. In a sense, Facebook invaded the offline world through the physical social networks of American college campuses. As Facebook became influential amongst a wider demographic, they were able to further push this shift to encourage more people to use the site as part of their social lives while using their "real" identities.

Friends, Profiles and Pokes

Compared with the Facebook of today, the early Facebook was very simple. Even today's most popular features -- the wall and photos -- did not yet exist. Facebook first launched with basic social networking features: the ability to add and display friends and profile pages where users could put their picture and basic details. However, one of the key features that set Facebook apart was the now famous "poke" feature, which sends a notification to the pkee that they had been poked. An early FAQ states that the poke was made with "no specific purpose", other than to see what people would do (Facebook, 2004a). The poke, however, became a way of nudging someone, or a lower risk way of seeing if someone is interested in talking without adding them as a Friend. At the time of my fieldwork, poking someone also granted them temporary access to the "basic," "work" and "educational info" on the poker's profile. The site also let users see who was in their courses and navigate through a visualization of their social network, features that were both later removed (Facebook, 2004b). While Facebook commented the removal of the courses feature was to encourage the developer community to create something better, the move was another clear mark of Facebook's move away from its student focus towards a general social tool (Morin, 2007). As Facebook evolved, new features which built on the core features of the Friends-list and the Profile were continually added.

The Wall

In September 2004, Facebook launched what is now one of the most integral parts of the site: the wall. Essentially, the wall is a way of having personal, yet public, conversations with one's friends. Until mid 2008 (and during the time I conducted the majority of my field research), the wall was a section on the profile page that anyone on a user's Friends list could write on (except individuals who had been blocked). In 2008, by default, the wall was located at the bottom of a user's profile, under demographic and contact information. The most ten most recent posts, complete with the details of the author time posted were displayed, the most recent at the top. The wall also included a link to see all wall posts, as well as a link for each individual post called "wall-to-wall." This would display just the wall conversation between the owner of the profile and a person leaving a message, in essence, allowing anyone to easily read a user's personal communications with other people.

After the major site redesign of mid-2008, which divided the profile elements into tabs, the wall became the primary focus of the profile page and was made the default tab displayed on profile pages to visitors. The wall was enlarged and integrated to include information from other activities (then called the "mini-feed"), such as status updates. The wall can be seen as a novel form of communication which merges public and private conversation. The functionality of Facebook's wall is not new to SNS, however. The way the wall is used is more of a shift in thinking about posting comments to profile pages. Friendster, for example, had a testimonial feature. The functionality is the same as the wall, except that is framed differently, which changes the norms and culture around its use. Instead of leaving one sided testimonials about Friends, the wall encourages public, two-way (or group) conversations.

Networks

Originally, Facebook's networks were entirely school-based. For example, if a user joined the site with a University of Toronto email address, that user would automatically become a member of the University of Toronto network. In a similar vein to

Friendster's degrees of separation model (designed to enforce Friendster's desire for its users to only connect with people they knew) networks were important ways of managing social interactions as well as privacy. Networks were also a critical piece of Facebook's privacy architecture. For example, the default during my fieldwork research, profiles were viewable to anyone in the same network. Such a design allowed users to balance findability with privacy -- being open to the people they were more likely to know in their networks, but closed to the general population. Broadly, networks fulfilled Facebook Inc.'s mandate "to help people find and connect with the people around them" (McDonald, 2009).

In 2005, Facebook Inc. added regional networks to accommodate the fact the company's shift towards was open access to anyone with an email address. In 2008, Toronto had the second largest regional network on Facebook, second to London, UK. All networks were later removed in 2009, as Facebook Inc. pushed its privacy settings towards being more open by default. This made it harder for users to manage the already shaky relationship between publicness and privateness. The numerous negative comments on the Facebook blog suggest that many users were not happy with this move (McDonald, 2009).

Groups and Events

In September 2004 Facebook Inc. launched groups. Events were formally launched just over a year later, when they were renamed from the original "My Parties" to "My Events," again reflecting the move away from a focus on students to towards a mass audience (Kagan, 2005). They were both given a large redesign in April 2006 which added most of their current features (Kagan, 2006). Groups and events are very similar in terms of functionality and can be created by any user on any issue or cause that is within the Facebook Inc. Terms of Use. Many groups are absurd, such as "Geordi La Forge: Sees all, Knows All" while others are serious and aimed at political or social change. During the time of my fieldwork, groups and events had much of the same functionality as profile pages, such as a wall, group/event info and group/event profile picture. Events also have an invite and RSVP function, that allow users to see an attendee list. Depending on the permissions set by the group or event creator, members can add photos, videos and posted items (which are just nicely formatted

hyperlinks) as well as participate in threaded discussions on the discussion board. Since the groups which a user was a member of appeared on his or her profile, joining a group was not always about active participation by members. They could also be about making statement about one's identity, such as proclaiming "I Don't Care How Comfortable Crocs Are, You look Like A Dumb Ass," or they could act as petitions where group membership indicates support for the cause (Davies, 2008). Since the 2008 redesign, however, group membership has been made less prominent and was moved to the secondary "info" tab.

Photos and Tagging

By December 2004, Facebook had reached 1 million active users. However, it was not until almost a year later, in October 2005, that Facebook added its other most popular feature: photos.²¹ Since the beginning of Facebook, users could always upload profile pictures, but the addition of the photo application allowed users to upload, edit, describe, comment on and sort photos into albums. But most importantly, the photos feature furnished users the ability to tag their Friends in photos. Tagging someone in a photo connects that photo to the person's profile page, so if a user clicks "View photos of Kate" the user can see all the photos that I have been tagged in by other people.

While the photo feature has improved since it was first launched, at the time of my fieldwork it still had a somewhat awkward interface, especially in comparison to competing photo sharing sites such as Flickr. Despite this, Facebook was still the number one photo sharing application on the web in mid 2008, even though it was not specifically aimed at that purpose (Facebook, ND). Within two months of the photos application launch, Facebook reached 5.5 million active users. As was the case with the wall, the photo feature of Facebook was so popular that they made it one of the core features in the 2008 redesign by giving photos its own tab, right next to the main wall tab.

21. As of May 2007, there were 1.7 billion user photos, 2.2 billion people tagged in user photos, 160 terabytes of photos stored, and over 3 billion photos served everyday. (Beaver, 2007)

Status

While it existed as early as 2006, the exact time at which Facebook Inc. added the status feature is unclear. This feature lets users write a short note telling their Friends what they are up to. Some use it more creatively, writing cryptic or humorous updates, or use it to send out links. Originally, Facebook forced all status updates to begin with "Kate is..." which wound up with people either making their status grammatically correct and writing about themselves in the third person, or just writing as if the "is" was not there. In November 2007, Facebook bowed to user pressure (there were even groups set up demanding the change) and made the "is" optional (Schiffman, 2007). Users stopped writing about themselves in the third person. Facebook Inc. took a step further in the 2008 redesign and reworked status to be more like the opened ended updates found on microblogging services such as Twitter.

Facebook for Everyone

Since day its launch, Facebook Inc. has continually extended its reach. Within a month of its launch, Facebook began expanding to other Ivy League schools. Just over a year later, in May 2005, Facebook supported over 800 university networks. By mid-2006 Facebook started moving beyond the college space. After adding high school networks the year before, they then added work networks for a select group of technology firms, such as Microsoft and Apple. When Facebook finally opened up to everyone in September 2006, it could be seen as a series of small changes, rather than one large change. In reality, these small changes added up to something quite significant. Up until mid-2006, Facebook was a student-only space where what happened on Facebook tended to stay on Facebook (there were increasingly exceptions²², of course). But in September 2006, to match with the new school year in North America, the gates of the walled garden had been thrown open. This shift from closed to openness and the ensuing privacy implications are examined in depth in Chapter 6.

22. As early as 2005 university administrators began using Facebook to monitor their students, and began handing out sanctions for behavior that violated the University's codes of conduct (Stutzman, 2005).

Introduction of Feeds

On September 4, 2006, the same day Facebook opened its doors to everyone, Facebook Inc. launched a new feature that drastically changed both site functionality. Up until this point, what a user put on the site was essentially ephemeral. If a user changed a profile picture or political stance or favourite movie, there would be no trace except for what was in the memories of that user's Friends (and perhaps data that was on the Facebook servers). In a sense, a user could rewrite his or her identity over and over again. The addition of feeds meant that everything a user changed or added to his or her profile was recorded and rebroadcast.

The feeds took on two forms. First, there was the mini-feed, which appeared as a box on the profile page. It summarised what a user had changed or added. This feature was so popular that it was later merged with the wall on the profile page and made the primary interaction on the profile page. Second, there is the news feed, which is an aggregation of all the mini-feeds of a user's Friends displayed together on the homepage, similar to a social RSS feed. To control the flow and display of this information, Facebook offered a set of sliders that allowed users to choose which "story types" they want to see more or less of (such as relationship stories -- for example, who broke up with who). Users could also add a list of 40 friends "that you find interesting [so that] you will get News Feed stories about these people more frequently" and up to "40 friends you prefer not to see in your News Feed" (Facebook, ND).

The combination of feeds that let users automatically watch each other, combined with the opening of Facebook to everyone caused quite an uproar among existing users (boyd, 2008b). Up until this point there was a degree of privacy through obscurity: users were able to change their profile without anyone being notified. They could also be relatively certain that anyone who could be looking at that profile, due to the school email address requirement, was very likely a fellow student, rather than an employer or parent. With these changes, users became concerned about how their privacy might be threatened. Despite these concerns, the changes seemed to attract even more users, and the userbase continued to increase at a rapid pace. Within two months, Facebook had 12 million active users, and less than a year later that number

reached 50 million. By August 2008, Facebook reported 100 million active users (Zuckerberg, 2007).

Facebook's introduction of feeds set a precedent for other social media sites, with Flickr and LinkedIn adding similar functionality. Since the core activities on Facebook are communication and sharing, the automated aggregation and publication of these activities through the feeds turned Facebook into a livestreaming service. A livestream is defined as "An online record of a person's daily activities, either via direct video feed or via aggregating the person's online content such as blog posts, social network updates, and online photos" (McFedries, 2011). The introduction of feeds on Facebook helped to embed livestreaming into an everyday activity that occurred automatically as individuals use the site. I explore the privacy implications of livestreaming in Chapter 6.

Facebook Platform

In May 2007, Facebook launched Platform to much excitement and acclaim in the technology community (Gannes, 2007). Platform allows third-party developers to build applications that work within Facebook to extend the site's functionality. Consequently, applications, and thus application developers, were given access to a user's data. While the expectation was that developers would produce some groundbreaking applications that would enhance social interaction, most of the applications ended up being of poor quality. Indeed, a few months after Platform's launch, a prominent tech blog observed that Facebook applications were a "cornucopia of uselessness" (Wag, 2007). Once added, these applications had a great deal of access to a user's personal information and activities. Exploiting this design, most applications were designed to send out spam-like invites to all of a user's Friends. As of writing, the most popular and commercially successful use of the Facebook Platform has been for "social games" such as Zynga's Farmville, where players are commonly incentivised to trade personal information for in-game currency or power-ups. Thus, from the beginning, Platform tended to put a user's privacy last.

Beacon

Beacon sits in contrast to the user-facing features which I have discussed thus far. Beacon, now officially defunct, was a subtly integrated advertising system that users were generally unaware of. Launched in November 2007, Facebook Inc. described Beacon as "a new way to socially distribute information on Facebook" that "connected businesses with users and targeting advertising to the audiences they want" (Facebook Inc., 2007). In practice, this meant Beacon collected data about users' activities on Facebook, and then quietly sent it to external partner websites, such as Coca-Cola and Blockbuster. Some of these activities were also automatically published on a user's news feed, causing users to unexpectedly share what they had purchased with their entire Friends-list. Since by default, the system was opt-out (rather than opt-in) most users were not aware they were participating. Despite this, Facebook Inc.'s press release insisted "In keeping with Facebook's philosophy of user control, Facebook Beacon provides advanced privacy controls so Facebook users can decide whether to distribute specific actions from participating sites with their friends" (Facebook Inc., 2007). Beacon was met with a backlash from users who felt their privacy was not being respected and was subsequently the target of a petition from the civic action group MoveOn.org (Stumpel, 2010, p. 25). Facing class action lawsuits and angry users, Facebook Inc. claimed Beacon was finally shut down in late 2009. As I explore in Chapter 6, this was not exactly the case.

Privacy Architecture, Policies and Concerns

In this chapter thus far, I have examined the chronological development of Facebook's features. Given the focus of this thesis, this section provides a more in depth look at Facebook's formal privacy settings and policies. In order to lay the groundwork for the rest of the thesis, I also provide an overview of how Facebook's policies and architecture serve to functionally or administratively violate the privacy of its users. I begin by providing a comprehensive list of the ways in which Facebook's designs and policies were alleged to legally violate the privacy of Canadian users in 2008. Using this list as a frame, I unpack how various elements of Facebook's policies, features and settings come together to create the privacy violations described.

Concerns

During the time of my fieldwork in 2008, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a complaint to the Office of the Privacy Commissioner of Canada (OPC) about Facebook Inc. on the grounds that Facebook's designs and policies violated Canadian privacy legislation. Specifically, according to the OPC's summary, CIPPIC argued:

Facebook does not inform users of the extent to which their personal information may be shared through the default settings and so does not have meaningful consent.

Facebook does not direct users to the privacy settings when they complete registration, when they upload photos, or when Facebook makes changes to the settings.

Facebook does not inform users that failure to alter the default settings constitutes consent to those settings.

Facebook fails to provide adequate notice to users posting photo albums that the default privacy settings for photo albums enable sharing with everyone, with the result that a user's non-friends can view his or her photographs and associated comments, even if the user's profile is searchable only by his or her friends.

When users sign up for a network, their default privacy settings enable the sharing of their personal information, including sensitive information, with everyone on the network (Denham, 2009).

As I show in this section, these concerns are a confluence of a number of administrative and functional choices made by Facebook Inc.

Confusing and Changing Settings

Over the years, Facebook's formal privacy settings have grown increasingly complicated and confusing while at the same time generally reducing the control a user has over their information or identity. Consequently, Facebook's privacy settings have been described as "the most confusing privacy settings in the industry" (boyd, 2008d). In their various incarnations since 2004, Facebook's privacy settings have given users some degree of control over how visible their profile is, primarily around what appears on their profile, when that profile is searched or how personal information is shared with Friends. Broadly, Facebook's privacy settings are entirely focused on the control of information with respect to other people (social privacy), while providing users no means to prevent information from being shared with Facebook Inc. (institutional privacy). As one of the participants told me in a privacy workshop I ran in 2010, "there is no setting on Facebook that prevents information from being shared with Facebook [the company]."

In 2008, Facebook's privacy settings were relatively simple and largely binary in the choices they provided. As the CIPPIC complaint notes, by default Facebook Inc. sets many of these settings to share or show personal information, without giving users adequate warning or obtaining informed consent. Despite CIPPIC's complaint, the trend towards more openness by default continued, with Facebook Inc. gradually changing its default settings to automatically more share information each year, such as educational background or a user's photos (McKeon, 2010). More recently, the ability to control the visibility of profile elements such as a user's name, profile photo, or location, has been removed entirely, meaning it is will be public regardless of user's wishes (Stumpel, 2010, p. 28).

Further adding to the already confusing nature of its privacy settings, Facebook Inc. is constantly changing the site's functionality, to the point where it was even a challenge for the Canadian Privacy Commissioner to evaluate CIPPIC's allegations against Facebook. As the Privacy Commissioner noted: "Facebook is a dynamic environment that has undergone many changes, primarily in terms of appearance and documentation since CIPPIC filed its complaint..." (Denham, 2009). Critically, without the knowledge or consent of its users, Facebook Inc. has on a number of occa-

sions changed its privacy settings in a way that publicly exposed information which was marked by users as private (McKeon, 2010; Opsahl, 2010).

Policies

Likewise, Facebook's privacy policy and Terms of Service (ToS), are equally as confusing as the site's privacy settings. Intellectual property lawyer Scott Buchanan has lamented the confusing and opaque nature of Facebook Inc.'s Term's of Service,²³ In a 2007 talk, Buchanan printed out Facebook's Terms of Service and found that the document was over 30 pages, despite being single spaced and in relatively tiny 10 point font. Accordingly, he argued, the company's expectation that a user would read such a document was entirely unreasonable. Further, in 2008, Facebook's policies also stated that they owned any intellectual property that a user uploaded to the site, and thus could use that property for any purpose. This meant that a user could potentially have their own image used by Facebook for advertising or other unexpected uses. Indeed, in 2009, this seemingly unrealistic scenario came true, when Facebook Inc. began allowing certain partners to use a user's profile picture in their banner advertising on the site (Smith, 2009).

Unclear Consequences

As the reuse of profile photos for advertising purposes suggests, Facebook Inc. does not make it too easy for users to understand the consequences of their participation on the site. In its complaint, CIPPIC also argued that "Facebook does not, in the context of its privacy settings, make a reasonable effort to advise users of the purposes for which and the extent to which their personal information is used and disclosed." (Denham, 2009) boyd takes a similar stance, stating that the problem with Facebook's privacy controls is that they are not placed in the context of how they are to be used, so it is confusing and unclear to users how a setting might actually work in practice (boyd, 2008d). Drawing on the field of Human and Computer Interaction

23. A contract each user agrees to when they join the site. If the user violates the terms, they can have their account deleted or suspended by Facebook Inc.

(HCI), Facebook's design can be described, then, as lacking an "integration of configuration and action" (Dourish & Anderson, 2006, p. 336).

As CIPPIC has argued, Facebook Inc. is also unclear with users as to how it aggregates and analyses their data and the subsequent consequences of that aggregation. In a 2005 interview at Stanford University, Zuckerberg casually reported that he had algorithms crawling the site, performing various tasks such as analysing how "real" users were, in order to sniff out fake accounts, and even predicting who would date who:

One of the things that one of my friends and I were messing around with the other night was seeing if we could use the information we had to compute who we thought were going to be in relationships. So, we tested this about a week later and we realised that we had over a third chance of predicting whether two people were going to be in a relationship a week from now (Stanford University, 2005, p. 43:09).

This is only one example of how Facebook Inc. uses its users data without informing them or obtaining consent. For example, in 2008, users started discovering a hidden feature in the search box that displayed five of their Friends that were the "most important" to them, according to Facebook Inc. The All Facebook blog reported that this list reflected the Friends a user "stalked" or "creeped" the most. After the feature started to become well known, Facebook removed it to "avoid any confusion" (O'Neill, 2008a). Despite this change, Facebook Inc.'s employees are still given access to this information. The ability that is considered a "job perk" and employees have used it in unprofessional ways, such as seeing who likes to look at their own profiles (Douglas, 2007).

Conclusion

In this chapter, I charted the historical development of Facebook, concluding with an in depth examination of Facebook's privacy settings, policies and potential privacy

threats, particularly in the context of Canadian privacy law. In the following chapters, I build on this chapter to unpack the historically informed rationale behind Facebook's evolution and current architecture and show the consequences it has for users. I begin this process in the next chapter, which provides a chronological overview of the history, culture and discourse which is manifest in Facebook's privacy design.

Chapter Five: The History and Origins of the Discourse of Facebook

*THE ROBOT OVERLORD CONTINUES TO ENTICE US WITH AIRS
OF HUMANITY*

- December 6, 2010 Tputh.com headline
(the day the new Facebook profile page was launched).

Since the launch of the site in 2004, Facebook Inc. has consistently pushed the privacy envelope. Indeed, Nick Bilton, a New York Times technology writer reported that when he asked a Facebook Inc. employee what Zuckerberg thought about privacy, the employee laughed and said "He doesn't believe in it" (Yarow, 2010). Yet, the common narrative that runs through most mainstream accounts is that Facebook Inc. is simply making poor, ill-informed privacy choices (for example, a Google search of "Facebook privacy blunder" returns over 1.5 million results). *The Social Network*, Aaron Sorkin's cinematic account of Facebook's founding and early days portray site creator and CEO Mark Zuckerberg as a somewhat socially and emotionally inept genius, who was motivated by a desire for women and entry into one of the prestigious Harvard final clubs. This account is perhaps unsurprising, given that the film was adapted from Ben Mezrich's book *The Accidental Billionaires* (2009) which was based on evidence from many parties, except anyone actually at Facebook, including Zuckerberg himself.

Commenting on the film for *Slate*, Nathan Heller, a former Harvard acquaintance of Zuckerberg's, notes the superficiality of the film's portrayal of Zuckerberg's motivations:

We seem to be meant to think that Zuckerberg grew and administered a global communications network in order to prove his power to a

couple of blazer-wearing kids who cold-shouldered him once during college (or else, maybe, to get with the hot babes who, in the movie, frequent Cambridge and the tech industry as if a Miller High Life ad might break out any moment) (Heller, 2010, p. 2).

However, as with the film itself (and indeed most other commentaries on Facebook), Heller's analysis remains at that surface level. Correspondingly, the film does not provide any insight into why Facebook Inc. has made such troubling choices with respect to privacy, other than perhaps Zuckerberg's supposed social ineptitude. Instead, Sorkin's film offers a simplistic explanation that negates any need for further investigation. The film is, essentially, a nice bit of PR that masks the real problem by providing an explanation that most people can relate to, thereby preempting a more nuanced discussion or analysis.

Zuckerberg's stance on privacy hints at something deeper and more longstanding. Almost ten years before Zuckerberg was outed as a privacy non-believer, Scott McNealy, the then CEO of Sun Microsystems, addressed privacy concerns related to his company's new chip by saying "You have zero privacy anyway. Get over it" (Sprenger, 1999). What Zuckerberg and McNealy are reflecting is a longstanding way of thinking about information sharing, technology and society that is dominant in California's Bay Area, particularly Silicon Valley. Given that the vast majority of top social media companies, such as Google and Facebook Inc., are headquartered in the Bay Area, it is a way of thinking that can have a profound impact on the privacy of social media users.

In this context, Facebook can only be made sensible through an examination of the history and discourses which have informed the site's creation and development. Accordingly, in this chapter, I will unpack the historically rooted ways of thinking about technology and society which created the necessary preconditions for the existence of Facebook. In so doing, I will provide a critical lens for understanding Facebook Inc.'s privacy choices. In later chapters, this lens will be used to unpack and analyse the architecture and consequences of Facebook, concluding with a revisitation of the privacy paradox.

To provide a map for this section, I will begin with a cursory overview of the historical development of the culture and discourse described in this chapter. From there, I continue with a historical examination through a number of key movements and moments, beginning with the Cold War and first order cybernetics, moving to the New Communalists and the 1960s American counterculture and then finally with the Californian Ideology and cybernetic totalism. Throughout this analysis, I pay particular focus to a number of strands which connect these movements over time: technological utopianism, cybernetics and libertarianism. As I will show, the development of these belief systems has been intertwined with the development and rhetorical framing of the personal computer and the modern internet, including, of course, Facebook itself.

Overview

As I will show in this section, the discourse of Facebook represents the culmination and evolution of a certain way of thinking about technology, economics, humanity and the world which is prevalent in the science and technology communities of the Californian Bay Area today. Described most simply, the discourse that is reflected in Facebook is a form of technological utopianism whose rhetorical roots lie in a fusion of cybernetics and Cold War research culture combined with 1960s American counterculture. Culminating into what Alice Marwick has called cyberdelic utopianism, this culture and discourse went on to shape the personal computing and digital networking technologies of the 1980s and 1990s (Marwick, 2010, p. 108). The 1990s saw an emphasis on the neoliberal and libertarian strands within the movement. The 1980s and 1990s were also when cybernetic totalism -- an extreme form of computationalism (or the belief that everything can be understood as code), became influential in technology circles and beyond (Lanier, 2000; Lanier, 2010). The most recent incarnations of cybernetically inspired thought gave us the dotcom bubble and the Californian Ideology in the 1990s and then Web 2.0 (as both a culture and a group of technologies) in the mid 2000s. It is a way of thinking about technology that codeveloped along with the technology it created (Hayles, 1999). As technology and culture evolved, so too did the cultures and discourses that informed it -- taking on various

and multiple forms along the way. Much like cybernetics itself, the discourse reflected in Facebook and the Bay Area more broadly, can be seen as "a historical entity, can be seen as part of a much larger cultural assemblage" (Pickering, 2010, p. 396).

The core tenets of this way of thinking include the cybernetic belief that flattened social hierarchies, open communication and efficiency will make the world better; that the world and everything in it can be understood as a system or code; and that technology is inherently positive and can overcome the limitations of the flesh. It is a mode of thought that draws on the neoliberal focus on the individual, efficiency and a drive towards profit. As I lay out fully in the next chapter, these prescriptive beliefs about the way the world *should* be are reflected in the way Facebook is designed, particularly with respect to privacy.

Technological Problems, Technological Solutions

As I discussed in Chapter 1, technology is often assumed to be, or implicitly treated as, the sole determining factor of social change. Technological utopianism is a form of technological determinism that takes that belief one step further. In technological utopianism, technology, by its very nature, has the ability to solve all the world's problems. As with technological determinism, technological utopianism downplays the role of social, economic or political factors in shaping world affairs, instead focusing on technology as the driver of global change. An example of this sort of thinking in the context of social media is the belief that "computers might empower individuals to transform their social worlds..." (Turner, 2006, p. 105). More broadly, technological utopianism gives rise to technological fixes for technologically created problems, such as urban isolation or climate change.

Indeed, the way first order cybernetics frames humanity's problems privileges technology as the solution. According to much of the rhetoric from early cybernetics, it is chaos, hierarchical bureaucracy, and obfuscation, which all lead to poor, inefficient communication and information sharing. The result is war, fascism, and alienation from work and life. Equality rather than top-down hierarchies, combined with efficiency, openness, and better control and understanding of systems and the world

more broadly would lead to peace, democracy and justice. As Norbert Wiener believed, efficient, ordered systems (such as those afforded by computers) were sources of "moral good" (Turner, 2006, p. 24).

An examination of the evolution of the mainframe to the personal computer reveals that there is a certain irony to the technological utopian belief system. In the 1940s and 1950s, stemming from their use by governments for military purposes, mainframe computers were seen as sources of automation, dehumanization and control (Turner, 2006, p. 2). Such early computers are a far cry from today's laptops, iPhones and gaming systems which are generally treated as useful objects which seamlessly intertwine with everyday life. These early computers are why personal computers (PC) have the *personal* qualifier. For society to embrace personal computers, the negative attitudes shaped by mainframes and their military use had to change, and ironically, it was the technological utopians who changed those perceptions. Computers are not inherently harbingers of positive social change, it is their *use* and how that use is embedded and influenced by society, culture and economics that determines the impact of technology on the world.

Likewise, as Turner argues, there is nothing inherent in the design of the internet that necessarily results in the flattening of social hierarchies, more authentic identities, a revival of democracy, or any of the other revolutionary claims made by technological utopians (Turner, 2006, p. 3). Similar arguments were made about offset printing, FM radio, the VCR, and even cable television (Barbrook, 2007, p. 270). As history has shown, arguments about the inherently revolutionary nature of the internet are equally fallacious. Even though the technological utopians argued that the internet itself would be the source of revolutionary change, what created this view of personal computers and the internet was something else entirely. The change in perception came not from the technology, rather it was the discourses that were crafted around computing and network technologies over many years. It is this way of thinking about technology that facilitated the acceptance of personal computers and the internet into everyday life, and more importantly, informed how technologists and designers think about the technologies they create.

Kevin Kelly, a contemporary cyberneticist and influential technologist, provides an an representative example of this utopian mode of thought: "No one has been more wrong about computerization than George Orwell in *1984*. So far, nearly everything about the actual possibility-space which computers have created indicates that they are the end of authority and not its beginning" (Kelly, 1994, p. 467). Of course, this statement now seems rather ironic in the context of digital privacy. Some of the more esoteric or obscure beliefs about social structures and communication, however, are widely influential in the Californian Bay Area, where they have shaped, and continue to shape, the design of social media technologies. These ways of thinking, which are manifest in the architecture of Facebook privacy, can be traced back to early cybernetics, particularly that espoused by Norbert Wiener and other first order cyberneticians.

1940s-1970s: Cybernetics

Cybernetics is not an easy concept to pin down. Most simply, it is a way of thinking about society, systems and technology; particularly about human and artificial brains and the relationship between humans and machines that has developed over many years, coalescing into a nameable discipline and field of study in the 1940s and 1950s. Even though it existed well before the advent of networking and personal computers, cybernetics was taken up by movements such as a branch of the 1960s American Counterculture called the New Communalists to understand early personal computers and the internet. Cybernetics is an inherently cross-disciplinary field that "cuts right across the disciplinary map... mathematics, engineering, chemistry, evolutionary biology, economics, planning and military science... as well as brain science and psychiatry" (Pickering, 2010, p. 147).

The term *cybernetics* is based on the Greek word *kybernetes* (sometimes spelled *ku-bernetes*), which means governor or steersman (of a ship). It can be said then, that at its most basic level, cybernetics is the study and implementation of control. But not control in the classical, top down sense. For the ancient Greeks, the word government usually meant self-government, in other words, control from within rather than from above (Kelly, 1994, p. 119). Louis Kauffman, the President of the

American Society for Cybernetics provides a definition: "the study of systems and processes that interact with themselves and produce themselves from themselves" (Andrew, 2008, p. 214). Indeed, *systems theory* and *cybernetics* are often used interchangeably.

Control within a cybernetic system comes from within and is produced through the harmony of all the different parts constantly adapting relative to each other, rather than from an imposition from above. Cybernetic systems, then, do not have a clear, linear cause and effect. Instead they embody circular or mutual causality. These internal adaptations through feedback loops create systems that are highly responsive and adaptable to external situations and changes (Dupuy, 2009; Kelly, 1994; Pickering, 2010; Turner, 2006; Wiener, 1950). Cybernetic historian and sociologist of science Andrew Pickering provides an insightful contrast here between cybernetic and non-cybernetic devices:

Bridges and buildings, lathes and power presses, cars, televisions, computers, are all designed to be *indifferent* to their environment, to withstand fluctuations, not adapt to them... Cybernetic devices, in contrast, explicitly aimed to be sensitive and responsive to changes in the world around them, and this endowed them with a disconcerting, quasi-magical, disturbingly lifelike quality (Pickering, 2010, p. 7).

In cybernetic systems, indirect control is produced through feedback and self-regulation. Complex systems that would otherwise be hard to control directly, can organise and adapt themselves. Adjustments in the system can be carried out by altering one variable rather than many, leading to increased efficiency, accuracy and order. The change in one variable produces changes across the whole system. As Kelly describes: "...if all the variables are tightly coupled, and if you can truly manipulate one of them in all its freedoms, then you can indirectly control all of them. This principle plays on the holistic nature of systems" (1994, p. 121).

Another property of self-regulating cybernetic systems is an inherent efficiency. A thermostat in a house is a very simple but apt example here. By regulating the heat of

the furnace based on the level of heat in the house (feedback), the amount of energy used is much less than it would be if the furnace was just left on at all times, or adjusted manually by a person (Kelly, 1994, p. 123). At the most basic level, then, cybernetics is interested in indirect control; efficiency; and order with respect to the management of machines, humans and society at large. By understanding and implementing cybernetic systems, cyberneticists believe the world can be made better.

Norbert Wiener and the Macy Conferences

While most accounts of cybernetics begin in the 1940s (American Society of Cybernetics, 2000a), many of the core themes in cybernetics -- such as the control of machines or regulation of society -- had been areas of interest and debate as far back as the ancient Greeks (recall that the origin of the word is derived from an ancient Greek word). What the 1940s represented was the culmination and coalescence of these strands into a formalised discipline and area of study. The Macy Conferences that ran from 1946 to 1953, sponsored by the Macy Foundation, are credited as being one of the key sites of this process (Kelly, 1994, pp. 451-452; Turner, 2006, pp. 26-27). The conferences served to refine core cybernetic concepts and give them a name. In a sense, it was the Macy conferences where cybernetics became cybernetics, a term provided by Norbert Wiener, the man often credited with being the father of cybernetics. Richard Barbrook suggests that the conference attendees were looking to develop a cross disciplinary "metatheory" that could be used in natural and social sciences so they could continue working in the collaborative nature they enjoyed during the Second World War (Barbrook, 2007, p. 44). This metatheory was cybernetics.

The inaugural conference was entitled "Feedback Mechanisms and Circular Causal Systems in Biological and Social Systems" However, by the 7th conference, thanks to Wiener, the term cybernetics was added to the title (American Society of Cybernetics, 2000b). The conference series was an invitation-only event that assembled thinkers from across a wide swath of disciplines, from psychology to anthropology to mathematics. It brought together key thinkers from the US and the UK, including Norbert Wiener, Gregory Bateson, John von Neumann, William Grey Walter and

Ross Ashby. This collection of thinkers later became known as the Cybernetic Group. The subjects most discussed during the conference include human and social communication; logic machine as way to understand brains and computers; analogies between organisms and machines; cybernetic machines (aka robots and artificial intelligence); and information theory (Dupuy, 2009, p. 79). This wide range of topics speaks to how broadly the concepts of cybernetics can be applied, and indeed how feedback and networked control can be employed as a way of understanding the workings of humans, society, and indeed, the universe.

By the end of the series, the work done in and around the Macy Conferences had facilitated the launch of cybernetics as an influential mode of thinking in the Cold War era (Turner, 2006, p. 27). As Pickering argues, the impact of cybernetics expanded well beyond the academic world, becoming not just a field of study, but an ontology unto itself: "Unlike more familiar sciences such as physics, which remain tied to specific academic departments and scholarly modes of transmission, cybernetics is better seen as a *form of life*, a way of going on in the world, even an attitude that can be, and was, instantiated both within and beyond academic departments, mental institutions, businesses, political organizations, churches, concert halls, theaters and museums" (Pickering, 2010, p. 9).

One of the most influential thinkers in early cybernetics was Norbert Wiener, who is commonly credited with turning cybernetics into a coherent discipline (Barbrook, 2007; Kelly, 1994; Turner, 2006).²⁴ Wiener's research greatly informed cybernetics as a field, particularly his work designing systems to shoot down enemy aircraft, where he realised the benefits of systems thinking. He saw the human operators of anti-aircraft guns and the guns themselves as self-regulating feedback systems. In this model, humans were described using the metaphors of machines. They become part of the human/machine system as "mechanical information processors" (Turner, 2006, p.

24. Despite his later influence in progressive and countercultural movements, his work has a somewhat dark history. Wiener was a mathematician at MIT's Rad Lab, where he involved in military research during the Second World War, which to his credit he later gave up during the Cold War for ethical reasons. While the military influence on his work is often mentioned, his horrific neurological experiments on cats aimed at testing his cybernetic hypothesis (Wiener, 1949).

21). Attending the Macy conferences from the beginning, Wiener "emerged as the theoretical guru" (Barbrook, 2007, p. 44). During the run of the conference series, Wiener published his *Cybernetics: Or Control and Communication in the Animal and the Machine* which became a best seller and helped to put cybernetics into the mainstream. While some would disagree about his level of influence, stating that his contribution is overstated by contemporary accounts (American Society of Cybernetics, 2000b), Wiener's brand of cybernetics is the one that emerges most clearly throughout the history of technoculture.

One of his key contributions to technoculture was the notion of hierarchical flattening between human and machine, treating both as equal parts of a system. This approach reflected the culture of the lab at MIT where Wiener worked. MIT's Radiation Laboratory (Rad Lab) was "a system where man and machines collaborated, amplifying their respective capabilities, sharing control and ultimately serving the human good of stopping the Nazi onslaught" (Turner, 2006, p. 21). The culture of the Rad Lab was reflected years later in the Macy Conferences: "Much of the brilliance of these conferences came by the then unconventional approach of rigorously considering living things as machines and machines as living things" (Kelly, 1994, p. 452). Here, one can see the beginnings of the computational metaphor, which holds that everything in the universe can be understood as an information system, including people, as demonstrated in the above examples. Put another way: "...the world can be understood as a computer process, with people as subprocesses" (Lanier, 2010, p. 153). Years later, this way of thinking was used as a creation myth, when Kelly proclaimed "God had created the world as a series of algorithms, which ran until life, the universe and everything emerged" (Kelly, 1999, p. 390). Influential technologist Jaron Lanier calls this mode of thought *computationalism*, a metaphysical metaphor which he strongly disagrees with. Despite Lanier's lack of enthusiasm, this metaphor remains highly influential today among technologists (Stein, 1999), and acts as a common glue or framework among the otherwise diverse groups in Silicon Valley (Lanier, 2010, p. 153).

Computationalism can be seen in approaches that understand or describe the brain as if it were a computer (or, conversely, the belief that artificial brains are possible if

given enough computing power). Indeed, one of the core beliefs of the Cybernetic Group was that "thinking is a form of computation" (Dupuy, 2009, p. 3). Even some of Freud's lesser known models of the brain reflect a computational approach (Curtis, 2011). Not surprisingly, it was also computationalism which helped to give birth to the field of artificial intelligence. Indeed, in the 1950s, Jon von Neumann used the feedback metaphor to suggest that computers operated like humans, an approach which guided his research on artificial intelligence and helped to shift the core project of cybernetics in that direction. (Barbrook, 2007, pp. 48-49).

The unspoken notion that runs through this paralleling of humans and machines is that humans could be improved if they acted more like infallible machines. In his *On the Origins of Cognitive Science*, Jean-Pierre Dupuy argues that cybernetics is not about the anthropomorphisation of machines but rather the mechanisation of humans (Dupuy, 2009). Indeed, Neumann's work on managerial cybernetics which intended to improve the management of employees was predicated on his belief that "the most rational form of human behaviour was doing what computers did" (Barbrook, 2007, p. 61).²⁵

Such a levelling of humans and machines was also manifest in a more "human" way. As the culture of the Rad Lab reflects, a flattened rather than top-down approach with respect to managerial hierarchies became part of the broader research climate, beginning during World War II and continuing into the Cold War. In order to create the most innovative and potent weapons against the USSR, Cold War science overturned traditional boundaries and hierarchies to become a interdisciplinary and inter-

25. This concept, like many other cybernetic strands, actually pre-dated the formal foundation of cybernetics as a discipline, and was central to the social transformation in Russia after the revolution of 1917. The utopian vision held by those in power was predicated on the belief that humans could be trained to act entirely logically and rationally, just like machines. This transformation would allow a true symbiosis between humans and machines, thereby enabling a level of planning, control and efficiency which would bring about a perfectly ordered and predictable utopian society (Stites, 1991). The similarities of the ideas in this massive social project and the project of cybernetics were formally confirmed when the USSR turned to American cybernetics in the 1950s to help them reform their government controlled social and economic planning scheme (Gosplan), leading to the foundation of the Institute of Cybernetics in the Ukraine in 1957 (Curtis, 1992). These "cybernetic Communists" believed computers would bring about their utopian dream by enabling them to calculate the optimal distribution of labour and resources (Pickering, 2010, p. 262).

institutional space that "blurred the traditional distinctions between theory and practice, science and engineering, civilian and military and classified and unclassified" (Leslie, 1993, p. 2). In this way, both the research methods and the research itself were interdisciplinary. As well as embodying the values of entrepreneurship and networking across disciplines, cybernetic rhetoric also acted as a facilitator by providing a "contact language" that allowed for communication about similar concepts across disciplines. All in all, the culture of these research labs combined with cybernetics created new modes of social interaction which we see the legacy of today in the working culture of the Californian Bay Area (Turner, 2006, pp. 24-25).

American cybernetics thus owes its rhetorical and cultural roots, such as the computational metaphor and notions of control, to American Cold War research (Turner, 2006, p. 20). As Turner argues, Wiener facilitated much of this by acting as a bridge connecting cross disciplinary concepts and facilitating interaction between the different research groups of which he was a member (Turner, 2006, p. 24). As he did in his work at the Rad Lab, Wiener's best selling *Cybernetics* connected a number of disparate disciplines under cybernetics: digital computing, information theory, neural networks, feedback systems and servomechanisms, psychology, psychiatry, decision theory and the social sciences (Pickering, 2010, p. 3).

The influence of Wiener's *Cybernetics* was widespread, with the key cybernetic metaphors -- feedback, information and systems -- becoming part of every aspect of technical culture, as well as part of everyday speech (Barbrook, 2007, p. 45; Kelly, 1994, p. 120). *Cybernetics* even became a best seller, rivalling even *The Kinsey Report* (Kelly, 1994, p. 119). A few years later, Wiener published the more accessible, *The Human Use of Human Beings: Cybernetics and Society*, in which he applied the computational metaphor to society. In his vision, Wiener saw society as a whole functioning like machines and organisms who sought self-regulation and balance through informational processing. Television, then, would be a feedback mechanism for society, with the media having the ability to "correct" society by providing accurate information to the public (Turner, 2006, p. 22). Wiener argued for the value of flattened hierarchies of communication, rather than the usual top-down approach. By asking everyone involved equally, leaders would get more accurate, reliable informa-

tion which would enable them to make better informed, more rational decisions. One of the key themes here is the value placed on more open communication to enable better information flow. In this vision, information is power: "Wiener's cybernetics holds that information itself is what gives people control over their environment. The concept of feedback, self-monitoring by an organism, demonstrates the inherent ability of information in a cybernetic framework to allow control" (Burge, 2007).

In this way, more accurate, relevant information leads to a better self-regulating society. As Turner argues:

Embedded in Wiener's theory of society as an information system was a deep longing for and even a model of an egalitarian democratic, social order... computers may have threatened automation from above, but they also offered metaphors for the democratic creation of order from below (Turner, 2006, p. 24).

It is the application of Wiener's notion of flattened hierarchies combined with the Cold War culture of blurred boundaries to the personal computer and networking technologies (such as the internet) which yielded the belief that such technologies (by virtue of their peer-to-peer rather than top down design) would bring about a more equal and democratic world. Accordingly, it would be a world where individuals could be themselves and would be free to determine their own destinies.

Along with the power of information and flattened hierarchies, Wiener believed in the inherent power of systems. Recall his assertion that the organising power of feedback and systems improved the world by overcoming disorder and chaos, thereby making them sources of "moral good" (Barbrook, 2007, p. 44; Turner, 2006, p. 24). In his own words in *The Human Use of Human Beings*, Wiener actually called disorder and chaos "evil" (Wiener, 1950, p. 11). Embedded in Wiener's model is the notion that most of the world's problems are problems caused by inefficient, closed communication, disorder or poor information sharing.

In the light of Wiener's notions about systems and information, computers too can be seen as sources of "moral good." If we extend the computational metaphor to the entire universe -- meaning the entire universe is made of code (a favourite notion of Kevin Kelly), then the conversion or merging of the analog with the digital would turn the physical world into a manageable system, one that can be indexed, managed, sorted and redistributed (and of course aggregated and datamined as well), thus making the world ordered, open, efficient and transparent.

Strands, Evolutions and Forks

In *The Cybernetic Brain: Sketches of Another Future*, Pickering charts how the style of American cybernetics usually associated with Wiener -- sometimes called first order cybernetics -- developed into a form of cybernetics that ran counter to many of the core tenants of modern science. The principal difference between these two strands was that while first order cybernetics was concerned with the use of cybernetic systems to control complex systems, second order cybernetics was instead interested in self-organising, autonomous systems which controlled themselves (Umpleby, 2001). Likewise, second order cybernetics, which seemed to gain more traction the UK, had more of a nonmodern ontological bent, to use Pickering's term (Pickering, 2010). In this nonmodern ontology, experience and outcomes are more important than modern science's knowledge for its own sake. Counter to modern science's notion (often reflected in first order cybernetics) that everything in the universe can be understood by humanity, second order cyberneticists tend to believe that there are instead limits to human knowledge, and that this limit should be accepted. In fact, there is no inherent problem in not understanding the root cause of a given phenomenon.

Drawing on early French cyberneticist Pierre de Latil, Kevin Kelly (who draws on both first and second order cybernetics in his work) even goes as far to suggest any given cause is not even worth knowing (Kelly, 1994, p. 121). Rather than aiming to systematically categorize and represent the world, second order cybernetics instead focuses on experiential knowledge as an end rather than a means. Rather than being a means of unpacking the world, performance and experience are an epistemology in themselves. In practice, this means that second order cyberneticists are more interest-

ed in outcomes than representations. As Pickering puts it, second order cybernetics sees "articulated knowledge as part of performance rather than its container" (Pickering, 2010, p. 386).

Another difference between the two schools of cybernetics is where second order cybernetics derives its name. While first order cybernetics places the observer as a outside of the system being observed, as a neutral third party, second order cybernetics acknowledges "observations of a second order" (Fuller, 2005, p. 104) that can exist outside of the system. Counter to the concept of the neutral observer, second order cybernetics acknowledges that these outside observations can have an impact on the system being observed. It is a subjective cybernetics of the observer, rather than the objective observed system (Hayles, 1999, p. 11). For these reasons, second order cybernetics had ontological similarities with holistic and Eastern spiritual practices, such as Buddhism, which made it more appealing to countercultural movements such as the New Communalists, who, as I will show, took up the rhetoric of cybernetics for their cause. According to Pickering (2010, p. 183) "northern California was a key site at which cybernetics crossed over to the broader field of the counterculture, as it hung on there into the 1970s and mutated into New Age" (p. 183). Indeed, Pickering credits cybernetics, especially second order cybernetics, as one of the origins of "psychedelic sixties" (p. 12).

Even though cybernetics has had a profound influence on many aspects of American culture, including contemporary computing and networking technology, it is no longer part of common language or understanding. Kevin Kelly, in his *Out of Control*, argues that cybernetics, as a movement, died. He offers a number of explanations, including the cybernetic project being refocused on artificial intelligence (Kelly, 1994, p. 453). Yet, on the very same page, Kelly states that his entire book is "an update in the current state of cybernetic research." *Out of Control* is essentially an application of core cybernetic concepts to help readers understand and shape what Kelly sees as the near future of biological machines; new social systems and a new economy. Indeed, Kelly's book shows how pervasive the rhetoric of cybernetics still is today. As Pickering puts it "[cybernetics] is alive and well and living under a lot of other names" (Pickering, 2010, p. 15).

One of these other strands is the contemporary technology culture of Silicon Valley. But unlike previous orders of cybernetics, the cybernetic thinking which informs Facebook is more of reflection of the legacy of cybernetic thought rather than an advancement of the field. It is a cybernetics that does not go its own name, or acknowledge its legacy. It is also a cybernetics that has merged with other movements, influencing them but remaining invisible, as it has in the case of the privacy architecture of Facebook.

As with the roots of cyberculture more broadly as noted by Turner, cybernetics has influenced and morphed into wide variety of different schools, focii, definitions and so forth, with bits and pieces that can be easily adopted to suit the various purposes of those who take it up:

The history of cybernetics shows us how easy it is to get from little robots to Eastern spirituality, brain-wave music, complexity theory and the Fun Place...I have stressed the protean quality of cybernetics, the endless multiplicity of cybernetic projects, and I want to note now that the reference to multiplicity implies a recognition that these projects are not inexorably chained together. It is entirely possible, for example, to take Beer's viable system model serious as a point of departure for thinking further about problems of social and political organization while admitting that hylozoism and tantrism are not one's cup of tea (Pickering, 2010, p. 399).

This selective use of cybernetics continued through the various movements and cultures that adopted it, resulting in its latest manifestation as reflected in Facebook's privacy architecture. In this next section, I will show that this picking and choosing in action -- particularly how flattened social and communication hierarchies; and computationalism, were taken up by the New Communalists for their countercultural project.

1960s and 1970s: The New Communalists and the Whole Earth Catalog

While the counterculture of 1960s is usually simplified into a homogenous movement, Turner argues that there the truth is more nuanced, especially when considering the history of the internet and cyberculture. Turner discusses two different branches which existed within the countercultural umbrella: the New Left, and a branch of the counterculture that Turner calls the New Communalists, whose influence is critical in understanding the discourse and culture embedded in contemporary technology. The New Left grew out of the work of the Students for Democratic Society, a group that emerged from the American Civil Rights and Free Speech movements. The movements were also influenced by deep anxieties regarding nuclear annihilation and anti-war sentiment -- first with the Cold War and then the war in Vietnam (Turner, 2006, p. 34). The New Left blamed a highly bureaucratic social structure for psychologically fracturing individuals and their identities, thereby them capable of the racism and other destructive behaviour. This unhealthy social structure could be changed through agnostic, direct political action in the form of protests, marches and manifestos. Turner argues that this group were very different from what he calls the New Communalists. While sharing the New Left's rejection of the state, they differed significantly on the correct approach to making change in the world. Inspired by the hippie counterculture, the back to the land communist movement and the rhetoric of cybernetics -- especially of the second order variety -- combined with a deep distrust of politics and other top down hierarchies, the New Communalists believed that a change in society would only come about through a change in mind (Pohflepp, 2008, pp. 11-12; Turner, 2006, p. 36; van Bree, 2010). And the way to change minds and consciousness more broadly was through technology.

Turner credits Stewart Brand as being one of the key connectors of the New Communist movement. Brand accomplished this through a series of what Turner terms "network forums," which took the form of gatherings, publications and online social networks (long pre-dating the common use of such a term) (Turner, 2006, p. 5). In the same way Wiener helped to solidify the cybernetic movement during the Macy Conferences (which network forums in their own right) as well as his book, Brand

did the same for the New Communalists. These network forums "generated new social networks, new cultural categories and new turns of phrase" (Turner, 2006, p. 5).

These network forums included the highly influential Whole Earth Catalog, which was published by Brand from 1968 to 1972. As David Silver noted, it was "Part manual to countercultural living, part shopping catalog, and part mindmap to Brand's disparate interests" (Silver, 2008). According to Brand, the *Catalog* was about computing technology from the beginning, and featured articles on how to program BASIC or steal unused computing cycles from mainframes at night (Kennedy, 2011). The Whole Earth brand was subsequently spun off into a number of related publications, including the *Whole Earth Review* and even one of the first "virtual communities," the Whole Earth 'Lectronic Link (The WELL). As John Markoff described the catalog in his chronicle of the 1960s counterculture's influence on personal computing revolution:

The first *Whole Earth Catalog* was a full-on tour of the counterculture, a hodgepodge of product descriptions, advice, commentary and quirky features, laid out in seemingly haphazard fashion, beginning with Buckminster Fuller and ending with the *I Ching*; it became an instant bible and serendipitous tool for finding interesting stuff. In doing so, it also helped scattered community that was in the process of defining itself find an identity (Markoff, 2006, p. 155).

In the same way the modern internet makes it easy for individuals to connect around niche interests and purchase obscure products, the catalog helped network the emerging New Communalist movement. The catalog also served to connect and apply Wiener's cybernetics to the New Communalist desire for social change through a change in mind, enabled by technology. Perhaps most crucially, the catalog legitimized and expanded the the New Communalist project into the mainstream by publishing letters written by rural hippies next to those written by high technologists:

[Brand offered] commune-based subscribers a chance to see their own ambitions as commensurate with the technological achievements of

mainstream America, and he gave technologists the opportunity to imagine their diodes and relays as tools, like those the commune dwellers favored, for transformation of individual and collective consciousness (Turner, 2006, pp. 5-6).

This utopian framing of technology as an inherent driver of social change speaks to another divergence between the New Left and the New Communalists. While the New Left entirely rejected any learnings or technologies coming out of the the Cold War military industrial complex, the New Communalists embraced both, repurposing them for social change (Turner, 2006, pp. 33-36). Here, too, one can see Brand and the New Communalist movement's expertise in connecting seemingly disparate communities and discourses -- an important feature in the history of cyberculture.

In addition to the humanising of Cold War technology, the New Communalists by way of the *Catalog* presented an alternative to capitalism, in the form of a gift economy. Turner describes how readers contributed product reviews and letters for publication because they believed in and wanted to support the community around the *Catalog*, rather than for the small sum of ten dollars they received in return (Turner, 2005, p. 509). This notion of sharing for the good of the community without an expectation of reciprocation or individual gain is core to the gift economy model. Individuals operating in a gift economy in its truest form are judged by their contributions rather than race, gender, class or other social status. In information based communities, such as the *Catalog*, a gift economy is seen as levelling the playing field, thereby helping to create the cherished non-hierarchical community where individuals are free to be their true selves. A gift economy was central to the hacker and open source cultures which emerged later, as well as the homebrew computer movement (Markoff, 2006, pp. 262, 275). In these cultures, those who contributed help on projects or relevant information were rewarded with status or fame among the community, also called social capital. Certainly, the *Catalog* informed these movements: a gift economy based on information underpins Stewart Brand's famous "information wants to be free," amplified by John Perry Barlow and others (Clarke, 2001) which has become the rallying cry of the open culture movement. In essence, the New

Communalists helped to bring the notion of a gift economy, based on information and networking, into technology culture.

The gift economy now is a large part of the working style of Silicon Valley -- building social capital helps get work down the road (Marwick, 2010; Rheingold, 2000).²⁶ As I will show in the next chapter, this notion of information as a gift is highly influential in assumptions behind Web 2.0 and Facebook, which are designed around the idea that *personal* and potentially *private* information wants to be free.

In sum, the legacy of the New Communalists, lead by Stewart Brand, was a rhetorical connection between technology, social change and consciousness, held together by cybernetics. Just ten years earlier, computers and other Cold War technologies were seen as sources of alienation and oppression by governments and other large bureaucracies. By merging counterculture with cybernetics and then popularising the result, the New Communalists began the humanisation of technology and the integration of cybernetic ideals into the mainstream. Most notable was the connection they created between technology and social change. The New Communalists promoted the technologically utopian notion that technology would enable non-hierarchical communities based on gifts, barter and volunteerism. Counter to the dehumanising nature of the highly structured bureaucracies which the New Communalists saw as the root of the world's problems, these technologically-enabled social arrangements would allow individuals to be their true, authentic selves. Thanks to the New Communalists, technological determinism; flattened social hierarchies; authentic identities; and sharing as an end in itself all became part of mainstream technoculture.

26. Science fiction author and open culture activist Cory Doctorow has called this "whuffie" in his *Down and Out in the Magic Kingdom*, a fictional account of a future with a social capital or status based economy.

1980s and 1990s: Neoliberalism, Personal Computers and Virtual Communities

In the 1980s and 1990s, Brand and his cohort of influential and likeminded thinkers - - Kevin Kelly, John Perry Barlow and Howard Rheingold, to name a few -- repeated the same network forum process, but this time their revolutionary technology of choice was the personal computer and then later electronic networks and the internet (Turner, 2006, p. 6). According to Markoff, Brand was been "immediately struck by the possibilities of computers that were moving beyond calculators" (Markoff, 2006, p. 156). As he did with the larger New Communalist movement, Brand helped to build connections between the various communities that gave birth to the personal computer, and even (somewhat inadvertently) funded the founding of the Homebrew Computer Club (Turner, 2006, pp. 101-102), which went on to "ignite" the personal computer industry (Markoff, 2006, p. 62).

Cybernetic rhetoric and the New Communalist movement it inspired were deployed to re-frame what was seen as a small calculation device or microcomputer as "personal" computer. As Turner shows: "The notion that computers might empower individuals and so transform their social worlds did not simply grow up alongside shifts in computing technology; rather, it had to be linked to the machines themselves" (Turner, 2006, p. 106). In this way the New Communalists, lead by Brand, continued their technological utopian project which first framed computers and then the internet as inherently social, beneficial and revolutionary technologies, all at once exposing the fallacy of technological determinism, as well as demonstrating the continued influential power of that discourse.

This time around, Turner's network forums took three main forms. The first of these forms was the Whole Earth 'Lectronic Link. Launched in 1985, the WELL was a bulletin board system which was essentially an early social network site. Second, the Global Business Network (GBN), a future focused strategic consulting firm founded in 1987. And, finally and perhaps most well known today, *Wired*, the highly influential technology and culture magazine, founded in 1993, which is still in publication today. Brand was strongly connected to all three. He was a co-founder of both the

WELL and GBN and was a writer for the early *Wired*, which also featured many of those involved with the Whole Earth publications such as Kevin Kelly.

Through these platforms, and gatherings that were organised through and between all three, the members of these network forums took their "techno-social visions" of the world into the mainstream and popularised "the potential social impact of computing, of information and information technologies as metaphors for social processes, and of the nature of work in a networked economic order" (Turner, 2006, pp. 6-7). As I will discuss shortly, such platforms also became the space where a new hybrid discourse and culture were forged, born from the the New Communalists and neoliberalism and held together by technological determinism.

The WELL, founded in 1985 by Larry Brilliant and Stewart Brand, was one of the first, and is now one of the oldest communities of its type still in operation. The name is a direct reference to earlier Whole Earth projects, including the catalog. Originally a dial up bulletin board system (BBS), the WELL also became one of the first commercial dialup internet service providers (ISPs) in the early 1990s. It served as a connection point for a number of key internet thinkers -- such as John Perry Barlow, cyberlibertarian and *Grateful Dead* lyricist, and Mitch Kapor, founder of software maker Lotus -- who through their discussions on the WELL, decided to found the Electronic Frontier Foundation (the EFF), an organisation aimed at defending civil liberties online.

What was special about the WELL was not simply the technology, but rather the convergence of a number of social, cultural and technical factors that would shape the discourse (especially the utopian variety) around the internet to this day. Through a combination of the influential thinkers who used it and the kind of interaction it facilitated between them, the WELL can be seen as the birthplace of "virtual community" model for thinking about networked communication. Inspired by his experiences on the WELL, Howard Rheingold, a teacher and writer connected with both *Wired* and the Whole Earth publications, wrote perhaps his influential work, *The Virtual Community* in 1994. Drawing on the same discursive ingredients as the New Communalists, Rheingold popularised the concept of virtual communities as a utopian space. As

Richards argues, Rheingold "provided a direct connection between a 1960s Californian countercultural ethos and the democratising possibilities of cyberspace" (Richards, 1999, p. 13). One of the key arguments for this utopian potential was the now familiar celebration of flattened hierarchies as a source of positive social change. By their very nature, virtual communities (and by extension the internet), could erase these hierarchies. As the argument went: "Within the virtual communities of cyberspace, the old hierarchies of race, class, age and gender mattered much less" (Barbrook, 2007, p. 264). Just as the New Communalists had hoped, virtual communities might be the place where individuals could be their authentic selves.

These utopian visions were embodied and supported by the informationally-based gift economy that was central to the functioning of the WELL, much like its predecessor the *Whole Earth Catalog*. On the WELL, experts would share their knowledge with others without an expectation of reciprocation, but rather in the spirit of sharing and community. Rheingold describes how this created an on demand pool of experts who he could count on for relevant information: "An editor or producer or client can call and ask me if I know much about the Constitution, or fiber optics, or intellectual property. "Let me get back to you in twenty minutes," I say, reaching for the modem" (Rheingold, 2000). In keeping with the notion of social capital in the gift economy, those who shared more were also rewarded more: "Sometimes you give one person more information than you would give another person in response to the same query, simply because you recognize one of them to be more generous or funny or to-the-point or agreeable" (Rheingold, 2000). In this way, the WELL, with the help of Rheingold, solidified many early conceptions about what the internet was and what it could do, especially around utopian visions of cyberspace.

Indeed, Barbrook suggests that the 1990s were a time when "many pundits believed that the Net had almost magical powers" (Barbrook, 2005). Within internet studies and related disciplines, this utopian way of thinking about the internet was highly influential and shaped the constraints around the way the internet was conceived. At the same time, it was also a source of much academic debate (see Wellman, 2004), with the equally technologically deterministic *dystopians* arguing that the internet would actually do the opposite of what the utopians believed. The internet would in-

crease alienation, fracture communities and destroy democracy. Robert Putnam's popular *Bowling Alone: The Collapse and Revival of American Community* captured this sort of dystopic thinking.

While Howard Rheingold and the spirit of the WELL generally stayed true to their hippie, anti-corporate roots (Barbrook & Cameron, 1995), Brand's other two core network forums -- *Wired* and the GBN -- came to embody a new form of technoutopian thought which merged its New Communalist roots with the American New Right and neoliberalism. It was an ontology which came to dominate thinking around technology and the internet during the dotcom era of the mid to late 1990s. Social scientist David Harvey defines neoliberalism in his book *A Brief History of Neoliberalism* as "a theory of political economic practices that proposes that human well-being can best be advanced by liberating individual entrepreneurial freedoms and skills within a institutional framework characterized by strong privacy property rights, free markets and free trade" (Harvey, 2007, p. 2). In neoliberal thought, "the social good will be maximised by maximising the reach and frequency of market transactions, and it seeks to bring all human action into the domain of the market" (Harvey, 2007, p. 3). Drawing on Aihwa Ong, Marwick underscores how neoliberalism celebrates the market principles of competitiveness, discipline, and most importantly for this discussion, efficiency. Further, neoliberalism encourages individuals to integrate these principles into their everyday lives (Marwick, 2010).

While the New Right of the 1990s was socially more conservative, it shared the neoliberal celebration of economic liberalism and libertarianism. The broader connection between the New Right, neoliberalism and the New Communalists is their mutual celebration of technological utopianism (Barbrook & Cameron, 1995). It is these principles of technological utopianism and personal efficiency that inform the privacy architecture of Facebook, as I will discuss later in this thesis.

Both the GBN and *Wired* acted as network forums for the development of this hybrid mode of thought. Through these forums, an alliance was forged between the "techno-libertarians of the computer industry, the former counterculturists of the San Francisco Bay Area and the social conservatives of the New Right" (Turner, 2006, p. 232).

Out of two seemingly contradictory belief systems, these two groups fashioned a new shared rhetoric around the power of the internet.

This vision of the internet reflected in *Wired* was simply the continuation and revision of a way of thinking about the internet that started in the 1970s. Augmenting Turner's account of the left-wing counter cultural movement, Barbrook and Cameron provide the following synopsis for the other side of the political spectrum:

Ever since the '60s, liberals -- in the social sense of the word -- have hoped that the new information technologies would realise their ideals. Responding to the challenge of the New Left, the New Right has resurrected an older form of liberalism: economic liberalism. In place of the collective freedom sought by the hippie radicals, they have championed the liberty of individuals within the marketplace. Yet even these conservatives couldn't resist the romance of the new information technologies. Back in the '60s, McLuhan's predictions were reinterpreted as an advertisement for new forms of media, computers and telecommunications being developed by the private sector. From the '70s onwards, Toffler, de Sola Pool and other gurus attempted to prove that the advent of hypermedia would paradoxically involve a return to the economic liberalism of the past (Barbrook & Cameron, 1995).

As Barbrook later argued, this mode of thinking was essentially a revision and repackaging of an "early-1980s neo-liberal model of the net" (Barbrook, 2007, p. 6).

In line with the WELL and Rheingold's *Virtual Community*, *Wired* continued the revolutionary portrayal of the internet, but this time in the service of free market capitalism, smaller government and deregulation. Libertarian telecommunications analyst George Gilder was a key advocate for this push. In an interview with Kevin Kelly, then editor of *Wired* magazine, Gilder argued that not only was the internet "a trigger for a libertarian reorientation of government" but that it might also be "both a metaphor for a libertarian, free-market system and a sign of that system's inevitability."

ty" (Turner, 2006, p. 224). The existence of both the internet and the success of Silicon Valley were used as evidence to justify the correctness of such a free market model, the latter being held up as a model for the model on which to base the "New Economy" (Barbrook, 2007, p. 262).

As Turner describes, those behind *Wired* magazine as well as New Right thinkers such as George Gilder and Republican politician Newt Gingrich evolved and popularized this new rhetoric through a "cycle of mutual legitimation" whereby the magazine would endorse the work of an individual and vice versa. This occurred through cover stories or conference engagements, building credibility for both (Turner, 2006, p. 222). As Barbrook describes, this was how "In the pages of *Wired*, the bitter political divisions of the late-1960s and early 1970s America had disappeared" (Barbrook, 2007, p. 264).

In this process, the rhetorical legacy of cybernetics was of course, again, invoked. But this time, this time its selective deployment was in a form that supported entrepreneurship and by extension, free market capitalism (Turner, 2006, p. 5). This appropriation of cybernetics was reflected in Kevin Kelly's *In New Rules for a New Economy*, where he merged "cybernetic communism with networked neoliberalism" (Barbrook, 2007, p. 264). Tapping into a slightly different cybernetic legacy for the same goal, Gilder drew on the communist cyberneticists of Soviet Russia to argue that the only way to bring about the efficient and ordered utopia through a cybernetic two-way feedback system was not communism, but rather de-regulated, free markets (Barbrook, 2007, p. 262).

But it was the familiar New Communalist cybernetic argument which celebrated the power of flattened hierarchies -- and their inherent ability to topple huge, impersonal bureaucracies -- that were invoked most frequently to support this new hybrid. In the words of Barbrook and Cameron, such a model holds that technologies such as the internet "empower the individual, enhance personal freedom, and radically reduce the power of the nation-state. Existing social, political and legal power structures will wither away to be replaced by unfettered interactions between autonomous individuals and their software" (Barbrook & Cameron, 1995).

To argue this point in 1997, Esther Dyson -- a libertarian technology journalist, author and commentator -- published her highly influential *Release 2.0: A Design for Living in the Digital Age*. In its pages, she proposed that the internet would provide liberation from tyrannical corporate hierarchies and bureaucracy by making everyone equal in cyberspace (Dyson, 1997). In her model, "everyone" included both humans and corporations. If all participants in the market were reduced to nonphysical packets of information which, by the nature of the design of the internet, are treated equally, then everyone can "negotiate from positions of equality" (Turner, 2006, p. 14). Likewise, a year earlier, John Perry Barlow, founder of the Electronic Frontier Foundation, penned a manifesto entitled *A Declaration of the Independence of Cyberspace*. The manifesto, which spread virally and was copied on numerous websites, proposed the liberation from government control via the internet. In an argument similar to Dyson's, Barlow suggested that those who "lived" online were in a way nonphysical, and thus free from physical coercion.

In 1995, this new hybrid of cybernetics and neoliberalism -- held together by technological utopianism -- was labelled as "the Californian Ideology" by Cameron and Barbrook. A manifesto of sorts, *The Californian Ideology's* title paid tribute to the area in which it had evolved. It was a reaction to the culture the dotcom era in the Bay Area, which also began in earnest around the same year Barbrook and Cameron coined the term, Californian Ideology. Also described as the dotcom bubble, the period from 1995 until 2000 was a time of (largely unfounded) optimism about internet startups -- the majority of which were California-based. Many of these startups had no business model. However, the mass excitement of the power of the internet -- fuelled by *Wired*, GBN and the rhetoric of Brand, Kelly, Dyson, Barlow and others -- resulted in record setting growth and investment by venture capitalists in internet-related business. The dotcom era can be seen as evidence of the success of the "mashup" of neoliberalism with New Communalists thinking in informing and furthering the popularisation and normalisation of the internet and computing technologies.

Barbrook and Cameron describe the discursive foundation of the dotcom era as "an anti-statist gospel of hi-tech libertarianism: a bizarre mish-mash of hippie anarchism

and economic liberalism beefed up with lots of technological determinism" (Barbrook & Cameron, 1995). Put more simply, "the Californian Ideology promiscuously combines the free-wheeling spirit of the hippies and the entrepreneurial zeal of the yuppies" (Barbrook & Cameron, 1995). As Barbrook and Cameron argue, the Californian Ideology was composed of conflicting belief systems, thereby "[deriving] its popularity from the very ambiguity of its precepts" (Barbrook & Cameron, 1995). What held everything together within that ambiguity was an foundation of technological determinism. As Barbrook later commented, the belief that technological innovation was the single, impersonal force pushing humanity to the future became, in the Californian Ideology, "a full-blown social philosophy" (Barbrook, 2007, p. 267). While Cameron and Barbrook differ slightly on the historical roots of the Californian Ideology than Turner (arguing that it was the New Left rather than Turner's New Communalists who brought the countercultural influence to the table), they are essentially describing the same thing.

The naming of "the Californian Ideology" is an indication of how influential and widespread it had become in the Western world, a trend that continued into the hype of Web 2.0 around 2006 and then the pervasiveness of social media a few years later. In his three part BBC series examining the influence of cybernetics and the Californian Ideology entitled *All Watched Over by Machines of Loving Grace*, Adam Curtis documents how cybernetic modes of thought have had a profound influence on models of the world in ecology, economics and computer science (2011). Barbrook agrees, and provides similar, equally broad examples: "Free markets were feedback mechanisms. Scientific innovation was a self-generating process. Intellectual debate was a cybernetic sign systems. Politics was an interactive network. True believers met in cyberspace... [technological determinism] was melded with New Age mysticism" (Barbrook, 2007, p. 272). As Curtis argues, the thinking in these fields has, in turn, permeated mainstream consciousness. Indeed, the Californian Ideology has been "enthusiastically embraced by computer nerds, slacker students, innovative capitalists, social activists, trendy academics, futurist bureaucrats and opportunistic politicians across the USA" (Barbrook & Cameron, 1995).

The type of capitalism that is taken up and supported in the Californian Ideology and then later in Web 2.0 is one where capitalism is a social and political movement. As Fred Turner describes “[In California] We believe in social change, but business and technology are the way to do it, and the market is the measure of the rightness of doing it” (Pohflepp, 2008, p. 24). Recall that the New Communalists believed that it was consciousness and technology, not politics, that would transform society. But now, according to the Californian Ideology, free market capitalism was the only effective means to change. As Barbrook describes, the Californian Ideology had an entirely new agenda: “Far from transcending the market, the Net was its apotheosis” (Barbrook, 2007, p. 266). Cybernetic systems such as the internet would enable a self-correcting, non-hierarchical and truly free economic system. The markets, then, would be truly free to govern themselves, safe from political influence or control (Curtis, 2011). Now it was not a change in mind, rather a change in the market enabled by technology that would save the world.

2000s: Cybernetic Totalism, Transhumanism and Web 2.0

The naming of the Californian Ideology opened up the culture and discourses described within it for discussion and critique beyond the technology circles in which it emerged. However, the Californian Ideology is not exhaustive in its description of the approaches that can be found in the Bay Area. Cybernetic totalism, transhumanism and Singulatarianism are other influential aspects of contemporary Bay Area technology culture which also need to be considered.

In late 2000, Jaron Lanier -- father of virtual reality and self-described friend of Kevin Kelly and John Perry Barlow -- shared his extreme concern about changes in technology culture in his *One Half a Manifesto*: “For the last twenty years, I have found myself on the inside of a revolution, but on the outside of its resplendent dogma” (2000). This revolution, he claims, is one in which cybernetic technology becomes a dominant culture. The design of technology now reflects a mode of thought that celebrates machines over humans and thus encourages impersonal, abstract communications where human identity and input are devalued. Ten years later, Lanier developed his manifesto in a book, which extends his argument to social media. Lanier

argues that cybernetic totalism has become dominant in both technological and mainstream culture.

At its most basic level, cybernetic totalism is an extreme evolution of the computationalist paradigm which could be seen in Wiener's cybernetics. It is a critical, influential and often overlooked part of Bay Area culture. In Lanier's view, the same "tribe" identified by Turner and Barbrook can also be considered cybernetic totalists: "the folks from the open culture/Creative Commons world, the Linux community, folks associated with the artificial intelligence approach to computer science, the web 2.0 people, the anticontext file sharers and remashers and a variety of others. Their capital is Silicon Valley, but they have power bases all over the world, wherever digital culture is being created... their embassy in the old country is *Wired*" (Lanier, 2010, p. 17). According to Lanier (2000), these groups deploy cybernetics as type of metaphysics. As such, they believe that the the best way of understanding reality is through "cybernetic patterns of information" (Lanier, 2000). People, just as everything else that exists in reality, can also be understood as cybernetic patterns. Extending this belief system into the near future, the cybernetic totalists believe that around the year 2020 "biology and physics will merge with computer science (becoming biotechnology and nanotechnology), resulting in life and the physical universe becoming mercurial; achieving the supposed nature of computer software" (Lanier, 2000). Through this process, computers will take over control from people and "will fundamentally change the nature of what's going on in the familiar neighborhood of Earth" (Lanier, 2000). In this future, being human "will be either impossible or something very different than we now can know" (Lanier, 2000).

Lanier's final point describes an event known as the Singularity, a belief held by some cybernetic totalists. According to Moore's law, computing power will continue to double every 18 months (Schaller, 1997), which will eventually lead to the processing power of computers exceeding that of the estimated processing power of the human brain, which in turn will result in the birth of artificial intelligence. So far, Moore's law has proven true, but the rest is yet to be seen.

Science Fiction Becomes Science

If cybernetics represents the mechanisation of humanity, as Dupuy (2009) argues, cybernetic totalism, then, can be seen as computationalism and mechanisation applied to every aspect of human life and reality. While Dupuy and Lanier are critical of this mode of thought, Ray Kurzweil -- a prolific inventor in the fields of speech recognition, text-to-speech synthesis and an assortment of other electronic instruments -- has wholeheartedly embraced it. Kurzweil is probably the best known proponent of the Singularity and the related concept of transhumanism,²⁷ another idea based on cybernetic totalism. Transhumanism holds that since humans are really nothing more than sophisticated computer code, it will only take a sophisticated enough computer to enable humanity to download their brains, thereby living forever in digital form (Ptolemy, 2009).

N. Katherine Hayles (1999) -- postmodern literary critic, feminist and former XEROX researcher -- has described this belief system as posthumanism, a mode of thought which is characterised by the celebration of digital information over physical matter, as exemplified by the notion that the body is simply a container or a "fashion accessory." According to Hayles, "the posthuman view configures human being so that it can be seamlessly articulated with intelligent machines" (Hayles, 1999, pp. 3,5) Like many of the ideas that I have outlined in this chapter, the ideas in post/transhumanism are not new -- first appearing in science fiction and then trickling into actual science (Hayles, 1999, p. 1).

Science fiction also helped the quiet trickling of these ideas into mainstream consciousness. For example, Kurzweil's book, *The Age of Spiritual Machines* (2000) influenced a concept album of the same name by then popular Canadian rock band, *Our Lady Peace*. The album features Kurzweil reading passages from the book. Indeed, Kurzweil and his work have gained a large following among influential technologists and celebrities. His life and work were the subject of 2009 documentary film, entitled *Transcendent Man*. In the film, Kurzweil is shown taking hundreds of

27. Other well known proponents of trans/post-humanism include Hans Moravec and Marvin Minsky

pills each day to prolong his life so that when the Singularity occurs, he will be able to digitise his brain, thereby granting him immortality .

Despite its scientific origins, the rhetoric of Kurzweil and his fellow transhumanists reaches the level of religiosity. At the end of *Transcendent Man*, Kurzweil asks "Does god exist? Well, I would say not yet." The implication, of course, is that humans are creating god, who will come into existence when the Singularity occurs. Kurzweil is not alone in this computational spirituality. While he disagrees with parts of the Singularity theory (Kelly, 2008), Kelly is clearly an advocate of cybernetic totalism (Kelly, 1999). Like Kurzweil, Kelly is an influential technologist -- he was the founding executive editor of *Wired* magazine and former editor and publisher of the Whole Earth Catalogue. In his appropriately titled paper, *Nerd Theology*, Kelly equates coders and AI researchers to mini-gods, who "seek God by creating gods" (1999, p. 388).

Peter Thiel, a self-made billionaire and founder of PayPal, is another influential cybernetic totalist of note. He describes himself as "way libertarian," sits on the board of the Singularity Institute for Artificial Intelligence and has invested millions in research into life extension research (Hodgkinson, 2008). Like Kelly, Thiel has proven himself as an influential tastemaker with significant economic resources at his disposal. Thiel is especially important in the context of this thesis due to his influence at Facebook Inc, where he was an early angel investor and longtime seat-holder on the company's board of directors. Thiel is also a friend and mentor to Zuckerberg (Lacy, 2008, pp. 153,208). As I will show in the next chapter, Zuckerberg's many statements regarding the use of technology and "radical transparency" (Kirkpatrick, 2010a, p. 200) to improve the world suggest that he and Thiel likely have many beliefs in common.

Hype, Popularity and the Data Body

A more influential but less extreme strand of cybernetically-inspired thinking was Tim O'Reilly's Web 2.0, which emerged about ten years after after Barbrook and Cameron defined the Californian Ideology. Through his O'Reilly Media, Tim O'Reil-

ly partnered with MediaLive to host the first Web 2.0 conference in 2003. Although the term had been used by others previously to describe different things (see DiNucci, 1999), O'Reilly's version of Web 2.0 became the most well known.

Beginning around 2005, Web 2.0 became a popular way of describing perceived revolutionary changes in the web, both behavioural and technological. Often described as a marketing buzzword, Web 2.0 was surrounded by a great deal of excitement and hype. Web 2.0 was also marked with a lot of confusion about what the term actually meant (Allen, 2008). Others questioned if it even described anything new (Baym, 2010a, p. 16). According to Tim O'Reilly, who popularised the term:

Web 2.0 is the business revolution in the computer industry caused by the move to the internet as platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effects to get better the more people use them. (This is what I've elsewhere called "harnessing collective intelligence.") (O'Reilly, 2006).

In O'Reilly's vision, Web 2.0 was not a specific technology or protocol, rather it was a rather nebulous term that described a collection of ideas, technologies, and aesthetics. Generally, the features that make up Web 2.0 are decentralized, reusable and remixable data; the web as an application (services rather than packaged software); collective intelligence, the power of many and the wisdom of the crowds; and perhaps most importantly, user generated content (O'Reilly, 2005).

While O'Reilly's definition implicates a large number of high level concepts which made it vague and confusing -- it even took O'Reilly himself a few attempts to properly define the term (see O'Reilly, 2006) -- the commonly accepted meaning of Web 2.0 has generally come to refer to the web services it describes. Accordingly, social media is now generally used instead of Web 2.0. As Marwick discusses in her PhD thesis on the culture of Web 2.0, Web 2.0 "is an umbrella term for websites that combine social interaction with functions like bookmarking, video-sharing, and content creation" (Marwick, 2010, p. 1). Examples of Web 2.0 usually include Facebook,

Twitter, Google, Wikipedia and YouTube. Drawing on recent critiques of Web 2.0 which analyse various aspects of the culture and discourse associated with it, I argue that Web 2.0 is best defined and understood as a cultural and discursive movement just as much as a technological one (Allen, 2008; Allen, 2009; Allen, 2011; Cammaerts, 2008; Fuchs, 2009; Jarrett, 2008; Keen, 2006; Marwick, 2010; Petersen, 2008; Scholz, 2008; Silver, 2008; van Bree, 2010; Van Dijck & Nieborg, 2009; Zimmer, 2008a; Zimmer, 2008b).

Indeed, within O'Reilly's definition is a set of political, social and economic assumptions about how the world should be (Allen, 2008). According to Andrew Keen, Web 2.0 critic and the self-described anti-Christ of Silicon Valley:

[Web 2.0] worships the creative amateur: the self-taught filmmaker, the dorm-room musician, the unpublished writer. It suggests that everyone -- even the most poorly educated and inarticulate amongst us -- can and should use digital media to express and realize themselves. Web 2.0 "empowers" our creativity, it "democratizes" media, it "levels the playing field" between experts and amateurs. The enemy of Web 2.0 is "elitist" traditional media (Keen, 2006, p. 2).

In this way, Web 2.0 can be positioned as the solution to many of the world's problems. In the same technologically utopian approach as the New Communalists and the Californian Ideologues, Web 2.0 heralds the deployment of technology's inherent ability to flatten hierarchies to fix democracy, journalism and economic disparity.

Within Keen's notion of the creative amateur who willingly contributes his or work to the commons is what is perhaps the most important contributions of Web 2.0: user generated content. One of the key elements of Web 2.0 -- as O'Reilly has consistently stated -- is the emphasis on the availability of data about people's and lives, activities and social interactions (O'Reilly & Battelle, 2009) which are freely shared both visibly through blogs, videos, tweets and other forms of livestreaming, and invisibly through cookies, usage statistics and other forms of web tracking. It is an unequal version of the gift economy where information is shared by users of Web 2.0 sites by

their very participation. In line with computational thinking in which the world and everything in it are reducible to computer code, Web 2.0 describes the automated conversion of previously ephemeral relationship and behavioral information into hard data that can be aggregated, cross-referenced and monetised. As I show in the next chapter, the information and content shared in the Web 2.0 paradigm can be both a gift and a commodity. In Web 2.0, then, user data becomes a resource in classic economic terms. Just like coal in the ground or wood from a tree, this data has value which can be extracted and monetised. Further, this value is surplus to the cost of extraction, because the computers algorithmically do the extraction as part of the very infrastructure of Web 2.0 technologies. What Web 2.0 really did was describe, for the first time, the link between online social interaction through computer mediated systems with the production and extraction of data about those interactions for commercial gain.²⁸

With respect to privacy, a potential contradiction emerges between a user's right to privacy and a Web 2.0 company's desire to extra value from user data. This is further complicated by the fact that the data Web 2.0 seeks to monetise is created by individuals. Most companies, including Facebook Inc., have user agreements whereby a person signs away the intellectual property which they share online. Accordingly, part of a user's identity -- their data body (Critical Art Ensemble, 1998, p. 145) or data shadow -- becomes property of someone else. In a sense, users lose control of their cybernetic selves, which are then used to sell things back to them. It is this emphasis on data is one of the reasons why Web 2.0 -- despite its diversity and complexity -- carries with it a movement towards a redefinition of privacy in society.

In sum, to use Marwick's description, Web 2.0 is a "literal instantiation" of the many of the ideals inherent in contemporary cybernetic thought (Marwick, 2010, p. 125). As such, Web 2.0 represents an updating, repackaging and marketing of the geek culture of the Bay Area. The revenue model of this repackaging of cybernetic thought is

28. I want to thank to Matthew Allen for helping me flesh out this understanding of Web 2.0

the monetisation of user data and other personal information, voluntarily and freely shared by users in exchange for free services or social clout (Marwick, 2010).

Conclusion

In this chapter, I have provided an overview of the history and origins of the discourse of Facebook. In this historically rooted mode ontology, transparency; efficiency; flattened hierarchies; and the free flow of information are seen not only as a social goods, but as the logical evolutions of human communication and society. I showed how this set of beliefs about the world evolved from a seemingly contradictory set of rhetorical roots, including Cold War research culture, cybernetics, New Communalist counterculture and neoliberalism, all bound together with technological utopianism.

Despite the small geographical area in which it emerged, I showed that the influence of this mode of thought is wide and deep, influencing the design of, and thinking around, technologies used around the world. As Markoff describes in his historic account of the personal computer, the PC's development came out of an "extraordinary convergence of politics, culture and technology that took place in a period of less than two decades and within the space of just a few square miles" (Markoff, 2006, p. x). Indeed, earlier iterations and strands of this way of thinking about technology and the world shaped not only the development, but the contemporary understanding of both the personal computer and the entire modern internet (Turner, 2006).

Contrary to most mainstream accounts, as I will demonstrate through the privacy architecture of Facebook in the next chapter, it is not that Facebook Inc. is unconcerned with privacy. That Zuckerberg does not "believe" in privacy is only half the story. The reality is that he believes in something else, and this something else is entirely at odds with protecting the privacy of Facebook users. Informed by the discourse and culture of the Bay Area as I have outlined in this chapter, Facebook Inc. has a mission to make the world more open, efficient, authentic and connected (Arrington, 2008; Facebook Inc., 2011). In other words, to change privacy norms and make the world less private. It is a future that could have never been anticipated by Wiener.

Chapter Six: Radically Transparent Sociality & the Architecture of Facebook

... let's be clear, Facebook is philosophically run by people who are extremists about information sharing (Dash, 2010).

In June 2010, Mark Zuckerberg was interviewed on-stage at the annual *D: All Things Digital* conference. He was sweating profusely, prompting Kara Swisher, who was conducting the interview, to suggest he remove the heavy hoodie that he was wearing. Zuckerberg was reluctant, telling Swisher "I never take it off" (Tsotsis, 2010a). When he finally give in, Swisher was surprised by what she saw. Inside the lining of the hoodie was a previously unpublished insignia which graphically illustrated the mission statement of Facebook. In large large letters, it read "MAKING THE WORLD MORE OPEN AND CONNECTED" (Tsotsis, 2010b). Upon seeing it, Swisher exclaimed "What are you in, some kind of cult?" (Tsotsis, 2010b)

Facebook Inc. has not hidden its seemingly innocuous goal of making the world more open and connected, nor have they made it overt. When I began my ethnographic study in 2008, Facebook's main page stated that the site's purpose was to "keep up with friends and family; share photos and videos; control privacy online; and reconnect with old classmates." But overall, it "connects you with the people around you." By late 2008, this description had been further simplified to "Facebook helps you connect and share with the people in your life." Taken together, Facebook Inc.'s corporate mission can be framed in the following terms: making the world more open, transparent and connected; improving information flow, relationships and sharing between people; encouraging trust and authenticity between users and making communication more efficient (Baloun, 2007, pp. 111-112; Smith, 2008; Zuckerberg, 2009b). These goals are likely why Zuckerberg and others at Facebook Inc. have insisted on making the distinction between Facebook and other SNS. Face-

book is not an SNS, but a social utility (Facebook Inc., 2011; Locke, 2007). On Facebook, socialising is not a frivolous activity, but a serious, instrumental endeavour. What has not been obvious is what such a utilitarian approach to communication and social interaction actually means in practice, particularly with respect to privacy. It is not that Facebook has actively hidden this agenda, it is more that no one has really questioned it.

As Zimmer argues, Facebook can be seen as an embodiment of a philosophy of information in which "information wants to be shared," a belief that "directly impacts the values built into the design of Facebook, ranging from its user interface, privacy policies, terms of service, and method of governance" (Zimmer, 2010b). This philosophy of information reflects a reworking of Brand's famous mantra: "information wants to be free." In the previous chapter, I charted the development of this varied yet related set of cultural and discursive strands in the Californian Bay, of which this philosophy is a part. I traced the path from Wiener's first order cybernetics in the 1940s and 1950s which provided the notions of flattened and efficient communication and social hierarchies, and the computational metaphor (Barbrook, 2007; Kelly, 1994; Pickering, 2010; Wiener, 1949). These notions were taken up and repurposed Turner's New Communalists in the 1960s, who imbued them with a drive towards changing the world for the better through authentic identities and flattened social and economic structures based on gifts and sharing (Turner, 2006). In the 1980s and 1990s this networked mode of thought, as Turner (2005) calls it, took on neoliberal and libertarian principles which celebrated individualism, libertarianism and efficiency, becoming The Californian Ideology, as described by Barbrook and Cameron (1995). The discourse of Web 2.0, as the next phase updated and repackaged Californian Ideology, is one where individuals are rewarded with free services or social capital in exchange for openly sharing personal information which can then be monetised (Marwick, 2010). At the same time, more extreme elements of Bay Area culture emerged, such as transhumanism and what Lanier (2000) terms "cybernetic totalitarianism." At their core, these beliefs hold that humanity can be improved by becoming more like machines. Overall, in the previous chapter, I provided a lens by which to understand Facebook's architecture and corporate culture. I showed how the values

of flattened hierarchies, efficiency; computationalism and technological determinism shaped and continue to shape thinking around technology.

In this chapter, I use this lens to illuminate and frame the findings from my media/archival research and textual analysis of Facebook Inc. to show how these values are also reflected in the discourse of the company. When Zuckerberg and his employees speak of openness, sharing, efficiency, transparency, authenticity and connectedness, what they are really invoking are various reworked elements of the culture and discourse of Silicon Valley. I demonstrate how this culture and discourse are reflected in the business model, discourse and privacy architecture on Facebook. I show how, arguing that it is improving the world, Facebook Inc. has encouraged its users to be more open, efficient, transparent, and authentic -- in other words, less private. Overall, I will show that it is not simply that Zuckerberg and those at Facebook Inc. are unconcerned with privacy. Rather, reflective of a number of strands of Silicon Valley discourse and culture, Facebook Inc. is actively pushing for a less private, more radically transparent world. The implications of this agenda will then be explored in the next chapter.

I begin with an examination of the beliefs held by key employees and board members at Facebook, particularly the company's CEO Mark Zuckerberg. I show how these beliefs are reflective of the discourse of Silicon Valley, culminating in what I call *radically transparent sociality*. I show how influential his thinking has been on the design and revenue model of Facebook. I then present two case studies to show how radically transparent sociality has manifested in the features, policies and deployment strategies of Facebook Inc. The first case study examines Facebook Inc.'s fostering of an open and transparent culture on its site. Here, I show the various strategies with which the company has used to further its radically transparent agenda. I pay particular focus on Facebook's rhetorical framing of its activities and strategic deployment of new features. In the second case study, I examine two key features of Facebook and show how they are both reflective of the discourse of Silicon Valley as well as supportive of Facebook Inc.'s longstanding goals. Overall, I will show how radically transparent sociality is embedded and promoted through Facebook's architecture.

Mark Zuckerberg and Radically Transparent Sociality

They "trust me." Dumb fucks.

- Mark Zuckerberg speaking about his users in 2004 (Orlowski, 2010)

I'm CEO ... Bitch

- Mark Zuckerberg's business card (Kirkpatrick, 2010a)

Just as Steve Jobs and Bill Gates both established and reflected the values of the technology companies which they founded, Mark Zuckerberg has set the tone for Facebook Inc. As I noted in Chapter 1, Zuckerberg created Facebook in his Harvard dorm room. With the help of a few friends, and later with the financial assistance of venture capitalists, he grew his small website into the influential, global company that it is today. Jose Vargas, a journalist who profiled Zuckerberg for *The New Yorker*, reports that the CEO been involved with almost every aspect of the site's design since day one (Vargas, 2010, pp. 6-7). Sarah Lacy, a technology reporter who spent a significant amount of time with Zuckerberg, provides a similar account, adding that Zuckerberg owns a third of Facebook Inc. and three seats on the board -- meaning he is the only one who can vote himself off (Lacy, 2008, p. 157) Former Facebook engineer Karel Baloun also confirms this: "Zuck carefully cultivates and maintains his effective control" (Baloun, 2007, p. 72). The first few years of the site's operation even saw "a Mark Zuckerberg production" written across the bottom of every page. In many ways, Facebook can be seen as a literal manifestation of Zuckerberg's beliefs about the world.

While he has never discussed the origin of his ideals, Zuckerberg is surrounded by the culture and discourse of Silicon Valley. And, before moving himself and his fledgling company to the Bay Area, Zuckerberg was immersed in the college culture of Harvard. According to Pierre Bourdieu's notion of habitus, individuals unconsciously take on beliefs and ideas about the world through the social milieu in which they inhabit (Bourdieu, 1977). Similarly, the social construction of technology (SCOT) model argues that "inventors are embedded in social contexts... [and] the

choices they make are seen as dependent on their social contexts" (Baym, 2010a, p. 39). As I demonstrated in Chapter 4, college culture, played a significant role in shaping the architecture and goals of Facebook. Indeed, the very name of the site was derived from a tradition at many American universities of aimed at facilitating social interaction between new students. In this case, the social milieu in which Zuckerberg has been embedded was first Harvard and now the Bay Area -- home to Facebook Inc., but Google and a host of top social media companies as well. Zuckerberg's mode of thought reflects the cultural context and background in which the Facebook Inc.'s founders and employees are steeped. Consciously or not, Zuckerberg's beliefs echo those of the culture in which he lives. Given Zuckerberg's significant influence within Facebook Inc., understanding his personal goals and beliefs is key to understanding Facebook and Facebook's privacy design.

Indeed, it is worth noting here the mutually reinforcing nature of the cultures or social milieu in which Zuckerberg created, developed and grew Facebook. The cultures of Silicon Valley and American colleges share many of the same historical roots -- particularly around the 1960s counterculture and the New Communalists. While there existed a large cultural gulf between the 1960s American corporate world and a college dorm room, today -- especially in high technology firms -- there is often not much difference between the two. As Baloun (2006) reported, Zuckerberg transitioned from the life of a student to the life of a CEO without significant changes to the way he dressed or behaved. As is the lore, Zuckerberg shows up to meetings in flip flops, jeans and a t-shirt. Thus, the move of both Zuckerberg and Facebook from Harvard to Silicon Valley can be seen as a natural step in the evolution of the site and the discourse embedded within it.

In 2010, technology journalist David Kirkpatrick published *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. In the process of writing his book, Kirkpatrick obtained an unusual level of journalistic access to Facebook Inc. and its employees. While it is clear Kirkpatrick is a fan of Facebook, his interviews with Zuckerberg and other key Facebook employees are not only revelatory, but they also confirm a number of earlier reports about the culture of Facebook Inc. and the influence of Zuckerberg on the direction of the company.

Kirkpatrick's research reveal that Facebook Inc.'s positive emphasis on openness instead of privacy was fundamental to the company since its inception. Zuckerberg, indeed, proudly proclaims his goal on his own profile page: "I'm trying to make the world a more open place by helping people connect and share" (Zuckerberg, 2009a). Dave Morin, who belongs to Zuckerberg's "inner circle" at the company told Kirkpatrick: "Our mission since day one has been to make society more open" (Kirkpatrick, 2010a, p. 207). This focus is confirmed by Baloun, who reported: "Facebook intends to improve the flow and quality of information shared between people, to actually improve communication and relationships. Facebook wants to broadly improve a fundamental human activity -- and why not?" (Baloun, 2007, pp. 111-112) Tellingly, Baloun's account was from Facebook's first two years. Zuckerberg's beliefs about privacy have been entrenched in Facebook from the start.

Underlying Zuckerberg's drive to make the world more open, authentic, efficient, and connected is his historically informed belief that this sort of change will make the world a better place. As Zuckerberg told Kirkpatrick, his thinking about helping the world has been shaped by liberal values, which he picked up from his college days:

I mean, picture yourself -- you're in college, you spend a lot of your time studying theories, right? And you think about these things in this abstract way. Very idealistic. Very liberal at this institution. So a lot of these people are just around you: the world should be governed by people. A lot of that stuff has really shaped me. And this is a lot of what Facebook is pushing for (Kirkpatrick, 2010a, p. 14).

Zuckerberg's vision of a world "governed by people" is enabled by connectedness and radical transparency. At the Facebook Developer Conference in 2008, he suggested that transparency can solve the world's problems by increasing empathy and understanding: "In the world we're building where the world is more transparent, it becomes good for people to be good to each other. That's really important as we try to solve some of the world's problems" (Smith, 2007). Through a series of somewhat

rhetorical questions in the introduction to his *The Facebook Effect*, Kirkpatrick clarifies just how Zuckerberg sees Facebook's role in solving the world's problems:

Could [Facebook] become a factor in helping bring together a world filled with political and religious strife and in the midst of environmental and economic breakdown? A communications system that includes people of all countries, all races, all religions, could not be a bad thing, could it? (Kirkpatrick, 2010a, p. 9)

While it may seem as though Zuckerberg is merely deploying altruism as a justification for his commercial, anti-privacy activities, it appears as if he truly believes in what he is doing. Baloun's (2006) account suggests that Zuckerberg really believes humanity can be helped if the way we communicate is changed to match his model of openness, authenticity, efficiency and connectedness. Likewise, according to Lacy: "[Zuckerberg] believes that [Facebook] is truly making the world better" (Lacy, 2008, p. 161). Zuckerberg's own comments echo Lacy's observation. boyd agrees: "My encounters with Zuckerberg lead me to believe that he genuinely believes ... that society will be better off if people make themselves transparent" (boyd, 2010). boyd goes on to comment that Zuckerberg also believes everyone else desires a world with less privacy and more transparency. Zuckerberg's goals are not only longstanding, but also pervasive among Facebook employees even what Kirkpatrick calls his "more extreme convictions" (Kirkpatrick, 2010a, pp. 200-209).

According to Kirkpatrick (Kirkpatrick, 2010a, p. 200), Zuckerberg and his fellow employees describe their beliefs as "radical transparency." In Chapter 1, drawing on Foucault (1972), I defined discourse as "systems of thoughts composed of ideas, attitudes, courses of action, beliefs and practices that systematically construct the subjects and the worlds of which they speak" (Lessa, 2006, p. 285). Accordingly, as a project that valorises and attempts to implement radical transparency in social life, one can say that the discourse of Facebook is radically transparent sociality.

Monetising Moral Goods

While it appears that those at Facebook Inc. are truly aimed at bettering the world through radically transparent sociality, this is not their only goal. As a commercial, for-profit business, Facebook Inc. also needs revenue. Just as the discourse of Facebook reflects the culture and beliefs of Silicon Valley, so too does the company's business model. In the Californian Ideology, capitalism could, and should, go hand-in-hand with activities that better humanity. In the same way, Facebook Inc. is pushing less privacy and more transparency not only to encourage empathy and empowerment, but also as a way to increase their profit.

In Chapter 3, I outlined the properties of ICT which threaten privacy by making online information and communication persistent, transferable, aggregateable, scalable, searchable, and cross-indexible. As an ICT, these same properties are baked into Facebook. It is these properties which make Facebook, in Wiener's first order cybernetics, a source of moral good, but also a source of profit. In the same way, the suggestion that increased empathy, as a social good, is a justification for decreased privacy and the monetisation of personal information is reflected in the public comments made by influential individuals at Facebook Inc. For example, Barry Schnitt, Director of Corporate Communications and Public Policy at Facebook Inc. stated:

By making the world more open and connected, we're expanding understanding between people and making the world a more empathetic place. And we know that when users find their friends, are found by their friends and learn more about the world around them -- they find more value on the site. From a business perspective, if users are finding more value from the site they will come back more and engage in more activity. *And you can imagine the business consequences of that* (Kirkpatrick, 2009) [emphasis mine].

Peter Thiel -- the Singulartarian angel investor and Facebook Inc. and board member since the company's early days -- has imagined the business consequences of encour-

aging the world to be more open, transparent and connected in terms of economic and cultural globalisation:

If globalization doesn't happen, there is no future for the world. The way it doesn't happen is that you have escalating conflicts and wars, and given where technology is today, it blows up the world. There's no way to invest in a world where globalization fails.... The question then becomes what are the best investments that are geared towards good globalization. Facebook is perhaps the purest expression of that that I can think of (Kirkpatrick, 2010a, pp. 9-10).

Implicit in these arguments about increased human connectedness and globalisation-enabled empathy are a number of assumptions about how the world should be. These assumptions reflect the technology culture of the Bay Area, which is strongly rooted in cybernetics. As I outlined in Chapter 5, Wiener's first order cybernetics frames most world problems as arising from inefficient, closed communication, disorder or poor information sharing. Computers, as systems, can be seen as sources of "moral good" because they can solve these problems (Barbrook, 2007, p. 44; Turner, 2006, p. 24). If, according to cybernetic totalism, the entire universe is code, then the conversion or merging of the analog with the digital would turn the physical world into a manageable system, one that can be indexed, managed, sorted and redistributed (and of course, aggregated and datamined as well), thus making the world ordered, open, efficient and transparent. By definition, privacy is the opposite of free, unfettered and efficient flows of information. In such a cybernetic utopia, privacy would be replaced by radical transparency.

This sort of computationally inspired thinking was evident even in the early days of Facebook, when Zuckerberg attempted to use collected data points to increase the efficiency, usefulness and by extrapolation, "moral goodness" of the site. As Baloun describes:

[Zuckerberg] has intentionally decided to collect Facts [sic] about how users know each other in the Facebook social map feature instead

of letting users make classifications. Facebook intends to algorithmically compute relationship closeness based on Facts and site behavior, more accurately and with less trouble than if users had to maintain them themselves (Baloun, 2007, p. 107).

Zuckerberg also reported that they had created an algorithm that accurately predicted who would be in a relationship with whom, based on site activity (Stanford University, 2005). While Zuckerberg may see this activity as bringing order and efficiency to the lives those on Facebook, those users will probably feel that their privacy is being violated. Indeed, the collection and cross-referencing of activities and information shared on the site can result in Facebook Inc. knowing far more about its users than they realise. Moreover, the collection and aggregation of personal information in this way is fundamental to Facebook's revenue model.

Through Facebook's features, in-line with the O'Reilly's Web 2.0 revenue model as well as Wiener's notion of order as moral good, users convert their activities into structured, formal databases and code so that they can be surveilled, managed, searched, aggregated, mined, monetised and sold. Indeed, simply using Facebook leaves a digital trail of one's personal information and activities. Zuckerberg describes this digital conversion is akin to indexing one's brain. As he told a technology journalist in 2010: "Most of the information that we care about is things that are in our heads, right? And that's not out there to be indexed, right?" (Vargas, 2010) By "indexing" all this previously unrecorded relationship and behavioural information into hard data that can be aggregated and cross referenced is commercially exploitable, particularly for marketing and advertising applications. In encouraging users to be more open, authentic and transparent, Facebook Inc. also increases the volume, accuracy and thus commercial value of the personal data it collects.

A critical piece of this personal-data-based revenue model is lifestreaming. As I noted in Chapter 4, lifestreaming capabilities have become core to Facebook's architecture, where feeds automatically push status updates, new photo tags and so on to Friends. Through lifestreaming, information sharing becomes automated and efficient, and social interaction takes on elements of invisibly watching and being

watched, both by other users as well as Facebook Inc. Josh Harris -- who created a physical prediction of Facebook's peer-to-peer and lifestream-based surveillance model in 2000 -- argues that "Google, Facebook and MySpace are training people to automate themselves" (Timoner, 2009). Through lifestreaming, relationships on Facebook become an automated, efficient and less private means of social interaction and communication. Moreover, technologically-mediated surveillance as a standard part of social interaction becomes normalised.

The productive output of lifestreaming, whereby a user's previously ephemeral activities are converted into informational flows, is often referred to as user generated content. User generated content is essentially a reworking of the New Communalist paradigm of the informational gift economy. As David Silver argues, the *Whole Earth Catalog's* editorial model which was based on a gift economy was a pre-digital example of user generated content (Silver, 2008). Connecting back to Facebook's discursive and cultural roots which I identified in the previous chapter, Zuckerberg sees information sharing on the site through the lens of the New Communalist concept of the gift economy, stating: "any individual's public expression on Facebook is a sort of "gift" to others" (Kirkpatrick, 2010a, p. 288).

Unlike the early online communities such as the WELL, as discussed in the previous chapter, Facebook and other social media sites monetise the gift economies that they cultivate by serving banner advertisements; selling aggregated user information to third parties; or by charging access fees. Facebook is not the most popular social network site because it has the best features or overall design. Rather it is because of network effects -- Facebook has the most people and the most content.²⁹ In a sense, most of the value of Facebook has actually been created by its users as "gifts." Ironically, the gifts are for other users, rather than for Facebook Inc. This form of immaterial free labour, according to Trebor Scholz, is a reflective of Web 2.0 discourse (Scholz, 2008). But again, the monetisation of gifts is not new, rather a continuation of an earlier, historically rooted idea. Tiziana Terranova identified the same phenom-

29. In 2009 Facebook was the top photo sharing website, beating out sites entirely dedicated to photos (Schonfeld, 2009).

enon on AOL in the late 90s, where unpaid moderators brought value and sanity to AOL's chatrooms for the sake of the community but AOL kept all the profits (Terranova, 2003). Fuchs has called this monetisation of gifts the "gift commodity internet economy":

Commercial Web 2.0 applications are typically of no charge for users; they generate profit by achieving as many users as possible by offering free services and selling advertisement space to third parties and additional services to users. The more users, the more profit, that is, the more services are offered for free, the more profit can be generated. Although the principle of the gift points towards a post-capitalist society, gifts are today subsumed under capitalism and used for generating profit in the Internet economy (Fuchs, 2008, pp. 6-7).

Even though the gift commodity internet economy may seem like an oxymoron, in Web 2.0 any contradictions are resolved. In Barbrook and Cameron's Californian Ideology, these two contradictory economic models existed simultaneously. The, first, that Barbrook and Cameron describe as commonly associated with the Left, was an electronic agora in the same vein as the WELL based on a gift economy. The Right-wing version was a laissez-faire electronic marketplace. In the same way *Wired* brought together the left-leaning New Communalists with the New Right, the Californian Ideology represents a marriage of these two disparate economic models - "by believing in both visions at the same time -- and by not criticising either of them." (Barbrook & Cameron, 1995) More recently, these contradictions have been erased through Web 2.0's literal embodiment of both sides, in what has been called a mixed economy. Social media has shown that information does not have to be a commodity or a gift. It can exist as both. (Barbrook, 2005) As Marwick describes: "Just as Burning Man [a festival in California that celebrates self-reliance and experimental community] is a blueprint for creating a community that runs on gifts, bartering, and volunteerism, the ideals of Web 2.0 suggest that technology as a business can embody the same values" (Marwick, 2010, p. 112).

In line with the Web 2.0 mixed economy model of the internet, where gifts can be both free and commodities, Facebook Inc. monetizes these lifestreamed gifts through datamining and targeted advertising. By encouraging users to be more open and transparent -- to lifestream their daily activities by using the site as a social platform - - Facebook Inc. can increase its revenues. Zuckerberg acknowledged that this has been their approach: "...as long as the stream of information is constantly increasing, and as long as we're doing our job...our role of pushing that forward, I think that's....the best strategy for us" (Zimmer, 2008c). Indeed, Facebook's architecture and culture based on openness and authenticity, the quantity of accurate personal information collected by Facebook Inc. has the company valued at as much as \$85 billion US as of 2011 (Raice, 2011). In 2010, Facebook Inc. reported revenues of \$1.86 billion for advertising alone (O'Dell, 2011).

In the discourse of Facebook, social change is brought about by a change in transparency. By encouraging its users to be more connected, authentic and transparent, those at Facebook Inc. believe can help the world become more caring and empathic. As Barry Schnitt, Peter Thiel and others at Facebook Inc. have argued, enacting these beliefs through Facebook also happens to be quite profitable.

Case Study: Towards a Culture of "Openness and Authenticity"

... doing a privacy change for 350 million users is not the kind of thing that a lot of companies would do.

- Mark Zuckerberg, 2010 (Kirkpatrick, 2010b)

In order to enact an apparent drive towards profit and social change by reducing privacy, those at Facebook Inc. have executed a consistent strategy to push radically transparent sociality on a number of different fronts. Combining rhetoric, strategic deployment of new features and a constant iteration of its overall architecture, Facebook Inc. has attempted to change user behaviour to be more in line with its vision of how the world should be. The most notable example of this process was a profound

yet gradual shift which I outlined in Chapter 4. This shift saw Facebook shifting on three core axes: access, audience and information. In terms of audience and access, Facebook evolved from a student-focused closed community which required a university email to a general purpose SNS. Around the same time Facebook became open to all, the site also began publishing and rebroadcasting previously ephemeral user activity and information. In Chapter 2, I noted how the increased online and offline overlap combined with the domestication of the internet were necessary conditions for the existence of Facebook. In Chapter 4, I provided a cursory overview of Facebook leveraged its position in the college community to first take advantage of these shifts, and then when they had enough influence, to push them as well.

In this section, I show in greater detail how Facebook Inc. further pushed these shifts -- particularly around online/offline and "authentic identities." I also analyse the company's deeper motivations for doing so. To accomplish this, I examine in detail how Facebook Inc. is constituted through the discourse outlined in Chapter 5, as reflected in its business model, corporate mission, and most importantly, its privacy architecture. As I will show, the initial design of Facebook reflected its historically rooted origins, thereby setting the pathway for the site's further development. Through a case study of Facebook's evolution from a walled garden to a site open to all, I show how the company's discourse has manifest in its privacy architecture. I present how Facebook Inc. has attempted to create a culture of usage that encouraged openness, transparency and authenticity which normalises, rewards and monetises digitally mediated surveillance. In other words, a culture where users are more likely to accept and expose themselves to surveillance, both from their peers as well as Facebook Inc. itself. In so doing, Facebook Inc. encouraged a change of user culture on its site.

Zuckerberg's initial design of Facebook in 2004 included an email based verification system that required new Facebook users to input their Harvard email address. Since only those associated with the university could obtain a such an address, the design created an exclusive student-only community.³⁰ According to boyd and Ellison

30. While school administrators and teachers could also gain access to Facebook through their

(2008) the email address requirement "contributed to users' perceptions of the site as an intimate, private community." The sense of exclusivity encouraged students to be their "authentic," "real" selves, sharing phone numbers, legal names and even their class schedule. In exchange for their disclosure, students gained social capital, new friends and even sex (Baloun, 2007, p. 91).

Initially, the email address verification meant that Facebook embodied only one, clear social context: of student life at Harvard University. As such, the norms of behaviour reflected that of a college dorm, bar or sorority. Since they were crafted to appeal to other university students, student profiles on the site reflected this context and identity. Such a clarity in context made contextual privacy easy to manage. As such, students felt safe posting photos of themselves drinking, partying or engaging in mischievous behaviour. Moreover, there were significant social benefits to participating, such as being able to nurture a new romantic relationship or easily find and share notes with class partners. This feeling of safety combined with a high social return meant, as Zuckerberg observed, that they would be more likely to share sensitive information, such as phone numbers, on their profiles so that other people could reach them more easily (Stanford University, 2005). Indeed, Zuckerberg later noted that this open sharing of personal information online was relatively uncommon at the time (McCarthy, 2010). Facebook Inc. was fostering a culture of openness and authenticity inside the then walled garden of Facebook.

As early as 2004, Facebook Inc.'s design was already encouraging a different type of user behaviour around privacy. Evidence suggests that Facebook Inc. was aware of what it was doing. Based on extensive interviews with Facebook employees, including Zuckerberg, David Kirkpatrick reported in his *The Facebook Effect*: "In the beginning it became apparent [to Facebook Inc.] that users at Harvard shared so much about themselves because they knew only other Harvard students -- members of Facebook's Harvard network -- could see it" (Kirkpatrick, 2010a, p. 209).

school-provided email addresses, the then relative obscurity of Facebook kept them unaware and thus off the site. Facebook also launched well before the moral panic around SNS, so there was little concern or interest among university staff.

In 2005, Facebook Inc. began accepting students from other universities, first with American colleges, then international schools (Facebook, 2011). Even though the email address requirement remained for new schools, it became harder to maintain the same sense of security and clear context which students felt when the site was Harvard-only. Zuckerberg's solution was to add school networks. By default, a user's information would only be shared with that user's network, thereby loosely mimicking the barriers that segregate social contexts in the physical world. In her model of contextual integrity which I outlined in Chapter 2, Nissenbaum (2010, p. 130) defines social contexts "structured social settings with characteristics that have evolved over time... and are subject to a host of causes and contingencies of purpose, place, culture, historical accident and more." These contexts can include home, work, religion and health care. Each context has its own norms of behaviour. In a similar, albeit a much more limited way, networks gave users boundaries and norms of behaviour with which to navigate their social interactions.

At first glance, networks may have seemed like a feature designed to protect the privacy of users. In 2006, Zuckerberg told users that Facebook Inc. had created networks "to make sure you could share information with the people you care about. This is the same reason we have built extensive privacy settings -- to give you even more control over who you share your information with" (Zuckerberg, 2006). In reality, the opposite was true. In an interview at Harvard University a year earlier, Zuckerberg described his rationale with respect to way he designed school networks. His goal was not to increase privacy. Rather, Zuckerberg stated that he gave users just enough privacy so that they would still share lots of information (Stanford University, 2005, pp. 6:40-8:30). In other words, he wanted to find a sweet spot where disclosure was maximised and privacy was minimised. What Zuckerberg recognised was a notion of privacy as the optimisation of disclosure, whereby there are social advantages to being seen -- advantages that must be balanced with the benefits of privacy (Tufekci, 2008). As I show in Chapter 8, Either as a reaction to Facebook, or

perhaps as a result of Facebook's encouragement,³¹ privacy as the optimisation of disclosure has become an important paradigm in understanding SNS and privacy.

Zuckerberg's strategy was effective. By building in a feeling of safety and closedness into the site through email verification combined with school networks, Facebook Inc. had created and continued a culture of authenticity and openness in the early Facebook whereby users disclosed their "real" identities and contact information. In the words of law professor James Grimmelman: "Facebook systematically delivers signals suggesting an intimate, confidential, and safe setting. Perhaps unsurprisingly, these signals are the same ones that make it such a natural place for socializing" (2009, p. 1160). On the surface, Facebook's design suggested to users that the company behind it cared about privacy. In a 2006 open letter to Facebook users, Zuckerberg encouraged this perception:

When I made Facebook two years ago my goal was to help people understand what was going on in their world a little better. I wanted to create an environment where people could share whatever information they wanted, but also have control over whom they shared that information with. I think a lot of the success we've seen is because of these basic principles (Zuckerberg, 2006).

Yet, there are a number of important details that Zuckerberg left out of this open letter. As his design goals with school networks suggest, Zuckerberg was using privacy in an almost paradoxical way -- to encourage disclosure. As Charlie Cheever, a former developer at Facebook Inc., stated "[Zuckerberg] does not believe in privacy that much" and sees Facebook's privacy settings as a "stepping stone" which Facebook provides to help people get over their need for privacy (Kirkpatrick, 2010a, p. 203). Sheryl Sandberg, COO of Facebook echos this account: "Mark really does believe very much in the transparency and the vision of an open society and open world, and so he wants to push people that way... I think he also understands that the way to get

31. As with most things, the truth is probably somewhere in between.

there is to give people granular control and comfort. He hopes you'll get more open, and he's kind of happy to help you get there. So for him, it's more of a means to an end" (Kirkpatrick, 2010a).

Leveraging the sense of security and culture of openness and authenticity created by school networks and an email-based verification system, Facebook Inc. began strategically expanding its userbase. After adding more American colleges in 2005, Facebook opened to international universities, and then high schools. In 2006, Facebook Inc. then began to push beyond universities and colleges, first by adding work networks for companies like Apple. Then, in September 2006 (the start of the new school year in North America), Facebook became open to anyone with an email address (Facebook, 2011). By implementing changes little by little, rather than all at once, Facebook Inc. made it more difficult for users to identify the exact point where things had changed too much. As Facebook slowly allowed more people to join, the open and authentic culture that had been created set the tone for future users. The old users set an example for the new users.

Facebook Inc. actively enforced these established norms of authenticity. The company required that users not only use their legal names, birthdays, and so forth, but also that users only connected with people they "really" knew. In 2008, for example, Facebook Inc. deleted accounts of users who were not using the site according to these rules, telling users:

Please note that Facebook accounts are meant for authentic usage only. This means that we expect accounts to reflect mainly "real-world" contacts (i.e. your family, schoolmates, co-workers, etc.), rather than mainly "internet-only" contacts (Arrington, 2008).

That same year, Zuckerberg reflected on the progress of his efforts to make the world more open and authentic at the Web 2.0 Summit:

Four years ago, when Facebook was just getting started, most people didn't want to put information about themselves on the Internet. So,

we got people through this really big hurdle of getting people to want to put up their full name, a real picture, mobile phone number...and connections to real people...as long as the stream of information is constantly increasing, and as long as we're doing our job...our role of pushing that forward, I think that's...the best strategy for us (Zimmer, 2008c).

Two years later, Zuckerberg proclaimed that society was gradually becoming more open and transparent: "Since [the 1990s], people have just been sharing more and more information and a lot of that was still being shared by a small number of companies or content producers" (Business Insider, 2010). Facebook's role in this process is to "shape" how things unfold. These comments not only show the longevity and depth of Zuckerberg's thinking around his goals, but are two of many examples of the contradictory narratives that Facebook Inc. has systematically deployed to support its creation of a culture of openness and authenticity. In the first narrative, changes with respect to privacy are inevitable and are occurring on their own. Facebook's "role" is simply to help people get through "hurdles" that are holding them back from falling in line with broader social change. In this version, Facebook Inc. cannot be blamed for giving users what they apparently want. In the second narrative, Facebook is responsible for "pushing" things forward and changing privacy norms for the betterment of society. Depending on one's perspective, either story can frame Facebook in a positive light.

The combination of rhetoric; strategic design; iterative changes and social rewards for disclosure had helped to create and maintain a culture of openness and authenticity on Facebook. Even though the terms of engagement had changed, this open culture remained, and began to spread beyond Facebook. Observing these changes, Zuckerberg noted in 2010: "Up until recently, the default on the Web has been that most things aren't social and most things don't use your real identity" (McCarthy, 2010). In line with Baym's domestication of technology (2010a, p. 24), Facebook helped to normalise the web as a social space that should be connected to one's "real" and everyday relationships and identity.

In so doing, Facebook Inc. created a culture where users share accurate personal information. In other words, a culture where users are authentic, transparent and connected with each other, which, in the discourse of Facebook, builds trust, empathy and understanding. Observing these changes, Zuckerberg noted in 2010, "Up until recently, the default on the Web has been that most things aren't social and most things don't use your real identity" (McCarthy, 2010). Not only did Facebook encourage people to be their "real" selves online, Facebook has served as an entry point for people to see the internet as a social space which augments everyday relationships and identities. This was the case for one of my study participants named Penny. Even though she had not previously used the internet to socialise (seeing it as a place for geeks and technologists), Facebook became an integral part of her social life after she joined in 2006. Like other Web 2.0 technologies of the time, Facebook helped to domesticate the internet, by making it more friendly and relevant to the average person, thereby becoming invisible.

Case Study: Friendship and Profiles

Being Friends on Facebook is not only a public acknowledgement and digitised formalisation of a relationship between two people, but it is also a functional information access control. As I noted in Chapter 2, Facebook Friends are lists of people who have access to each other's profiles. A list of one's Friends are also displayed on each user's profile. This list is viewable and explorable to all other Friends, and depending on one's privacy settings, this list might also be viewable to a broader audience, such as Friends of Friends or potentially everyone on Facebook and al. Since one's activities are pushed automatically to the news feeds of everyone who is a Friend, Friend-ing also acts like a subscription feature. The result of this feature is that users automatically become privy to the activities of their Friends, such as a status update or being tagged in a photo. Being Friends also grants others access to some control over what information appears on one's profile page. Friends can post to the wall, which appears to all other Friends, as well as tag users in photographs, activities that both get pushed out to the newsfeeds of all a user's Friends. At the time of writing, there is no way to pre-emptively prevent unwanted wall posts or photo tags, other than through meticulous observation and deletion by a user.

Unlike other sites such as Twitter or LiveJournal where users can follow or have one way Friendship, Facebook Friendship also requires reciprocity -- that is, both Friends must agree on the relationship. The result is that by default, both Friends equally and openly share information with each other. However, the reciprocity requirement can put pressure on the person receiving the Friend request to accept, even if they do not feel comfortable doing so.

Friendship, then, is a binary control that modulates information sharing between two individuals. It determines the visibility of one's relationships, activities, photos and other profile information, as well as who can edit and amend some of that information. Thus, even though it is not described as such by Facebook Inc. or by its users, Friendship is a powerful, yet simplistic privacy setting. Indeed, since the vast majority of users do not change their actual privacy settings from the default (Polakis et al., 2010), it can also be said that Friendship is the most frequently used privacy control on the site.³²

Using the lens of Friendship as a profile privacy control helps to reveal how the discourse of Facebook, particularly with respect to flattened hierarchies, openness, efficiency and authenticity are manifest in the privacy architecture of Facebook. Specifically, Friendship can be seen as a contemporary take on the ideals that informed the WELL, which themselves were based on "the New Communalists dream of nonhierarchical, interpersonally intimate society... a unified social sphere, a world in which we were 'all one'" (Turner, 2006, p. 248). The Facebook version of a nonhierarchical, unified social sphere is the merging of life's social contexts and related hierarchies into one flattened context. Through the Friendship feature, individuals from various social contexts are merged together as Friends, who, by default, all have equal access to the same profile information and status updates. For example, individuals on one's Friends list are not just populated friends, but also include co-workers; acquaint-

32. The usefulness of Friendship as an access control, however, has steadily decreased since the time of my ethnographic study in 2008 when by default, the majority of one's profile components were only viewable to Friends. This has since drastically changed, with most components now being open by default not only to all of Facebook, but to Google searches as well (McKeon, 2010). The relative power of Friendship as a binary privacy control now requires a user to change his or her privacy settings.

tances; long lost childhood friends; family members; complete strangers; and even enemies. Despite this varied mix of relationships, Friendship treats all Friends as non-hierarchical equals, giving everyone, by default, the same informational access. In so doing, Friendship creates a "context collapse" (Vitak, Ellison, & Steinfield, 2011) and reflects a situation where a user has to navigate multiple social contexts, audiences and sets of social norms with a single profile and identity. As I will show in the next chapter, this causes significant social privacy issues for users.

In addition to flattening social hierarchies and contexts, Facebook Friendship also enforces one, singular identity within those merged contexts. This singular identity arises through the profile feature, which only allows one profile for all Friends and all contexts. This choice, again, reflects a normative assumption about information sharing and the way the world *should* be. Zuckerberg and his colleagues at Facebook Inc. believe that by having a singular and thus "authentic" identity, society can be improved (Kirkpatrick, 2010a, p. 200). In this more "open and transparent" world, people will be held to the consequences of their actions and will be more likely to behave responsibly (Kirkpatrick, 2010a, p. 200).

Early in my research for this thesis, I had wondered whether Friendship had been intentionally designed to flattened contexts and impose this singular "authentic" identity on users or if it was simply a design oversight. At SXSWi in 2008, I attended the Facebook Developers' Garage. Since it was an official company event, Mark Zuckerberg also made an appearance. I asked him why Facebook did not have multiple profiles which would enable users show different sides of themselves to different people.³³ Zuckerberg replied that he thought it was "lying" to show people different aspects of oneself, depending on the context or relationship. He went on to say that the most "happy" people, according to an academic study he had read, were the same in all contexts of their lives. I argued that what he was describing was not lying, rather it was simply revealing different parts to different people. Zuckerberg de-

33. This interaction was one of my first clues that the architecture of Facebook had something much deeper behind it. In my field notes, I had written "This is a fascinating revelation of how Facebook is largely shaped by how Zuckerberg thinks people should interact, it's almost normative."

murred, and went on to say in the future Facebook would have more "organic" controls that allowed for more granular control of who sees what (which is what the Friends list is today). However, he told me, Facebook would never have multiple profiles because he thought it was an incorrect way of engaging in social interaction.

Baloun's account of his time at Facebook suggest that Zuckerberg's belief about singular identities have informed the design of Facebook since at least 2006. According to Baloun, even in those early days, Zuckerberg was clear on having one identity on the site to solve the "problem" of multiple identities (Baloun, 2007, p. 113). In fact, Baloun had a conversation with Zuckerberg that was similar to mine: "I told Zuck that older people display different personas to different groups of friends. And while he didn't tell me that was fake, not genuine and uncool, he said it might not have happened to me if I'd had Facebook. I could've stayed genuine to myself, and communicated that coherently to all my friends instead of just losing touch with them" (Baloun, 2007, p. 114).

A few years later, in 2009, Zuckerberg reiterated these ideas in a conversation with technology journalist David Kirkpatrick: "You have one identity... the days of you having a different image for your work friends or your co-workers and for the other people you know are probably coming to an end pretty quickly. Having two identities for yourself is an example of a lack of integrity... the level of transparency the world has now won't support having two identities for a person" (Kirkpatrick, 2010a, p. 199). Perhaps most tellingly, as Baloun (2007) describes, Zuckerberg himself lives this way -- reflecting the same identity no matter what social context he is in.³⁴ Through Facebook, Zuckerberg is attempting to impose his beliefs about identity and privacy onto the world.

34. Zuckerberg is known for wearing the same casual outfit -- Adidas flip flops, a hoodie and jeans -- in a wide variety of social contexts, including keynotes and business meetings with venture capitalists.

While one can easily assume that the choice of the word "Friend" to describe a core privacy control was a fairly innocent or accidental one, Zuckerberg's comments reveal the opposite. Again, speaking to Kirkpatrick, Zuckerberg remarked that even though the term is becoming overloaded, the term Friend has been useful in "[getting] people over a bunch of hurdles" (Kirkpatrick, 2010a, p. 312). Drawing on Zuckerberg's statements, Kirkpatrick concludes the friendly associations of the term helped people to feel comfortable sharing large amounts of personal information -- "after all, only friends would see it" (Kirkpatrick, 2010a, p. 312). As David Fono and I found in an study of LiveJournal, naming conventions play an important role in user behaviour and community culture. As one user told us, the use of the word "Friend" to describe relationships on LiveJournal was likely a critical component of the strong strong sense of community that existed on the site (Fono & Raynes-Goldie, 2006).

In the same way he used the official privacy controls to share more, Zuckerberg's comments suggest a conscious leveraging of the term "Friends" to help push openness and radical transparency. By merging multiple issues and choices around privacy and relationships into one binary decision -- "Are you my friend, yes or no?" -- the design of Facebook leverages social pressure to encourage people to connect and share as Friends, even if they are not actually friends. As I will demonstrate in the following chapter, this leads to situations where people accept Friend requests from people they do not like or even trust, simply to avoid embarrassment or negative social costs. Privacy is traded to save face. In the words of Kirkpatrick, "For better or worse, Facebook is causing a mass resetting of the boundaries of personal intimacy" (Kirkpatrick, 2010a, p. 200).

As I discussed previously, the concepts of social privacy combined with Nissenbaum's contextual integrity show that identity and context control are fundamental privacy management and protection mechanism. By removing the ability for users to properly manage their identities and social contexts, those at Facebook Inc. are making normative and discursively driven choices that challenge an average user's privacy. Indeed, they reflect a discourse opposed that is actively against privacy and in favour of radically transparent sociality.

Rhetoric and Deployment

Through these two case studies, I have shown how Facebook Inc. has attempted to encourage users to adopt its agenda of radically transparent sociality. Using the same strategies I outlined in the first case study -- particularly discursive framing and the strategic iteration and deployment of new features -- Facebook Inc. has continued to push its agenda on a number of fronts. In this section, I provide an in depth examination of how Facebook has strategically deployed a variety of key features and changes, including those examined in the case studies.

Facebook Inc. has employed a consistent deployment strategy for its new privacy features. The strategy is this: Facebook Inc. releases a new feature that radically pushes the boundaries of what users will accept by changing defaults or reworking the privacy settings. The inevitable backlash from users and the media occurs, Facebook Inc. apologizes and then scales back the changes ever so slightly. This process is repeated. Through generally small, persistent steps, Facebook's privacy norms are radically changed over a long period of time. In this way, users are slowly eased over privacy "hurdles," as Zuckerberg describes them.

The most notable example of this strategy was the release of a new advertising system called Beacon, which I described in Chapter 4. Without much warning, and unless a user opted-out, Beacon would share and broadcast a users' activities, such as purchases, to Friends on Facebook. Responding to huge a backlash, Zuckerberg issued a public apology, and made the system opt-in (Nissenbaum, 2010, p. 222).

Two years later, after continued backlash and legal action from users, Facebook Inc. claimed it had shut down Beacon. In reality, Facebook Inc. had taken a longer term strategy of waiting it out, while still pushing privacy norms. In 2008, the company simply relaunched a redesigned Beacon under another name: Facebook Connect (O'Neill, 2008b). Like Beacon, Connect literally connects a user's Facebook account with external websites, allowing them to use their credentials and personal information. But more importantly for advertisers, Connect enables a universal "Like" button on these external sites which users can click to have the item or website displayed as

liked on their profile. Despite Zuckerberg's apology for making Beacon opt-out, nothing had changed -- Connect was launched and remained opt-out.

A similar strategy was used when Facebook Inc. launched news feeds in 2006, a change whereby previously ephemeral information would now be streamed to one's friends. The change caused a significant backlash from users who felt their privacy was being violated (Kornblum, 2006). Instead of removing the feature, Facebook used the familiar tactic of apologising, leaving feeds in place while offering users limited privacy controls which, arguably, should have been there to begin with. Facebook Inc. had also planned to open the site to everyone around the same time, a change which they delayed (but did not cancel) (Kornblum, 2006). In this way, users could feel that Facebook Inc. was addressing concerns, while Facebook Inc. was still able to make its anti-privacy changes. In both the short and long term, Facebook pushed openness and sharing through its strategic deployment of feeds, Beacon and Connect.

Mark Stumpel, in his Masters thesis on the politics of Facebook, also observed Facebook Inc.'s strategy, noting "Facebook uses discursive reasoning not only to announce new features and subsequently apologize, but also to push its ideology of 'openness and connectedness'" (Stumpel, 2010, p. 38). Marc Rotenberg, Executive Director of the Electronic Information Privacy Centre (EPIC) puts it more simply. Facebook is wearing users down: "It's very unfair to users, who are trying to protect their privacy, to constantly be asked to revisit privacy choices they've already made" (Rotenberg, 2011).

Supporting this strategic deployment are number of rhetorical devices, which I have outlined previously. The first device is the framing of the new feature or privacy change as being beneficial to users. Through press releases, blog posts, interviews with the press or on the site itself, Facebook Inc. describes new features as "easier," "simpler" or giving users "greater control" of their personal information (Stumpel, 2010, p. 37). At the same time, Facebook Inc. also argues that users do not need to be protected. Mozelle Thompson, an advisor to Facebook Inc. and former Commissioner of the US Federal Trade Commission stated that it would be insulting to the intelli-

gence of users to force privacy controls on them (Thompson, 2011). Zuckerberg has put forth similar arguments that his company has done its part and should not force users into protecting their privacy. During an interview in 2008, Zuckerberg was questioned about the fact that most users are unaware or confused by privacy controls. Zuckerberg laughed it off by saying “Well, the privacy controls are there. The point is, as time goes on people are sharing more and more information” (Zimmer, 2008c).

The second device posits that privacy norms are changing regardless of what Facebook Inc. does. As I showed in the case study, on multiple occasions, Zuckerberg has stated that he helped or pushed users over a privacy “hurdle,” and that thanks to Facebook, “people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people” (Bigge, 2010). And yet, paradoxically, Zuckerberg in a typically technologically deterministic stance, has also stated that such a change was inevitable was already happening without Facebook's help (Business Insider, 2010). As Mark Zuckerberg stated in public interview in 2010:

People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time... We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are (Kirkpatrick, 2010b).

Facebook's privacy design, then, is simply a reflection of the larger societal move towards radical transparency. Barry Schnitt, Director of Corporate Communications and Public Policy at Facebook Inc. echos this argument: “Any suggestion that we're trying to trick [users] into something would work against any goal that we have. Facebook would encourage people to be more open with their updates because, he said, it was in line with the way the world is moving” (2009).

Taken together, Facebook Inc. has justified its activities by arguing that Facebook is merely reflecting a broader social push towards radical transparency. Through these two rhetorical devices, Facebook Inc. has been able to deflect criticism about its privacy design and choices, while avoiding the actual privacy issues at hand.

Conclusion

As with every technology, Facebook did not have to be designed in the way that it was. For example, LiveJournal -- an early SNS and blogging community -- was originally built to serve its community of users, rather than turn a profit. The site's design and operation was guided by a social contract. The result was a design that empowered with clear and powerful privacy controls and a revenue model that did not own or sell a user's information. In turn, a culture of privacy prevailed (Ford, 2010). Like LiveJournal, the way Facebook *is* reflects a discursive agenda.

As I have shown in this chapter, Facebook Inc.'s privacy architecture, policies and business model are all reflective of the legacy of cybernetics, computationalism, technological determinism and libertarianism. The result is a site architecture that values efficiency over privacy and where the monetisation of personal information can go hand-in-hand with saving the world.

Echoing New Communalists, Zuckerberg argues that the flattened social interaction and singular identity that he has enforced through Facebook is beneficial for individuals and society. In encouraging more connections between more individuals, where more information is shared by default, Friendship is bringing efficiency and transparency to relationships, thereby increasing empathy and understanding. However, as I show in the next chapter, when this radically transparent sociality is applied in everyday social life through Facebook, study participants did not experience increased empathy or other social goods. Instead, they experienced previously uncommon and often uncomfortable privacy challenges.

Chapter Seven: Radically Transparent Sociality in Everyday Life

In 1999 dotcom millionaire and Singularitarian Josh Harris unveiled *QUIET: We Live in Public*, a performance art piece that housed 150 residents in a communal bunker in downtown New York City. For a month, the residents -- self-described "pod people" - lived in a panopticon made real. As one of the residents describes:

[I lived] in a sub-basement warren of tiered sleeping capsules [pods], like a Japanese tourist hotel or something out of William Gibson, sleeping pallets with room for just a mattress and alarm clock. Each was also equipped with its own camera and pivoting TV monitor. We could not only tune into various live feeds being recorded and broadcast within the compound. We were also constantly on camera, producing our own flow of images. Anyone at the central control booth could watch as we ate, shat, argued, made art, fucked, etc. Theoretically, anyone in the bunker, at any time, could tune into anyone else in the bunker (Kaplan, 2009).

Everything was recorded and saved. Privacy was replaced with peer-to-peer and top-down surveillance. Ephemeral activities were captured and turned into information flows. All this was facilitated by a larger third party (Harris) who stated: "Everything [the food, accommodation] is free, except the video that we capture of you. That we own" (Timoner, 2009). Even though *Quiet* was created many years before Facebook, MySpace or any of the early SNS existed, it was, according to filmmaker Ondi Timoner who documented the project in her film *We Live in Public*, a "physical prediction of what life online would be" (Timoner, 2009). According to an article in *Wired* magazine published around the same time, Harris's beliefs about the world moving towards radical transparency echo Zuckerberg's: "[*Quiet*] previewed a future that Harris thinks is inevitable, in which high-speed Internet access and ubiquitous webcams

will shatter social and physical barriers, tempting us to watch one another and to enjoy this strange new form of intimacy" (Platt, 2000). It was a physical version of Facebook's radical transparent sociality, with cameras instead of keyboards and status updates, and televisions instead of computer monitors and newsfeeds. The pod people, as the term suggests, really lived in public. They stopped noticing the cameras and became accustomed to a radical transparency life (Timoner, 2009). And, just like on Facebook, the informational flows produced in that radical transparency belonged to someone else.

Introduction

As I showed in the previous chapter, Facebook Inc.'s motivations are not entirely driven by profit. Facebook's architecture and corporate mission reflect a strong belief about how the world *should* be. In making the world more open, efficient, authentic and connected, Zuckerberg and his employees apparently truly believe they are making the world a better place (boyd, 2010; Kirkpatrick, 2009; Kirkpatrick, 2010a, pp. 200-209; Lacy, 2008, p. 161; Smith, 2007). I examined the individuals and discourses behind Facebook Inc. and showed that the company's drive towards openness, authenticity, efficiency and connectedness is embedded in the site's architecture. I also showed how Facebook Inc. has attempted to encourage its users to behave in radically transparent ways through strategically planned new feature or setting deployments which are supported through a number of discursive strategies. Overall, I showed how, through the radically transparent sociality of Facebook, Facebook Inc. is trying to make the world a less private place.

This chapter is based primarily on my ethnographic fieldwork in 2008 in Toronto, Canada as examined through the lens of the discourse and history of Facebook. Specifically, building on the groundwork provided by the previous chapters to make sensible the findings from my fieldwork, this chapter examines what happens when Facebook's radically transparent sociality is taken up in the everyday life of young adults. As this chapter is based on ethnographic findings, the presentation of my results differs somewhat in style and content from the thesis thus far. For example, since context is a key component of ethnography, I include parts of transcripts from

face-to-face and electronic communications. I also provide a brief introduction to each of my study participants so as to provide deeper insight and background to what I observed and how I came to my conclusions.

In addition to the previous chapters, my approach is further informed by Fiske's (1989) model of popular culture. Just as Harris' pod people had some degree of choice and autonomy within his miniature surveillance society -- for example, they could leave the bunker or veil their faces -- Facebook users also have some degree of power and ability to resist. Rather than arguing that Facebook Inc. is simply forcing unthinking users into complicity, I instead draw on Fiske's to show how users are consciously and unconsciously resisting, reworking and managing their privacy within the system of Facebook. In addition to Fiske's work as a theoretical frame, I also draw on my notion of social privacy combined with Nissenbaum's contextual integrity as a way of understanding and unpacking privacy threats that arise from Facebook which could otherwise -- especially in legal models of privacy -- not be taken seriously as valid privacy concerns or violations.

After laying out my approach, I then provide a discussion of my fieldwork findings. I first examine Friendship and lifestreaming as the two key architectural features of Facebook which complicated and challenged privacy management for study participants. I then examine the broader social privacy consequences of these two elements of Facebook's architecture with respect to loss of identity control, creeping, and context collapse.

Overall, I analyse the intersection of Facebook and its users as a space where users take up and negotiate openness, transparency, efficiency and authenticity within the context of everyday social life. I show how the functional and utopian ideals within radically transparent sociality contrast with the nuanced and complicated lived social reality of study participants, thereby making it difficult for users to manage their privacy. The result is that users experience Facebook as a social and emotional space where social benefits and concerns (an element of social privacy) take precedence over institutional privacy concerns. In the next chapter, I show how the findings in

this chapter call for a rethinking of privacy in the age of Facebook, particularly with respect to youth and the privacy paradox.

Theoretical Frames

In his master's thesis on the politics of, and resistance to, Facebook, Marc Stumpel observes that Facebook Inc.'s continual and strategic pushing of privacy boundaries has resulted "in a situation whereby users, possibly unaware, must abide by the ideology of 'openness and connectedness'" (Stumpel, 2010, p. 38) Similarly, prominent blogger and social media commentator Anil Dash has stated "[Facebook is] advocating for a pretty radical social change to be inflicted on half a billion people without those people's engagement, and often, effectively, without their consent" (Dash, 2010). Yet, at the same time, users resist and rebel, experimenting and pushing the constraints of the system as far as they can. In Fiske's (1989, p. 4) theory of popular cultural production, Facebook users can be seen as reworking and "making do" with the resources which Facebook provides.

Fiske's model of popular culture, even though it long pre-dates Facebook and indeed even the web itself, is useful in unpacking the way in which Facebook Inc. on the one hand exerts a large degree of power and influence over users -- and increasingly social and cultural norms more broadly -- while at the same time, users have some degree of autonomy and power within those constraints. Drawing on French theorist Michel de Certeau's (1984) work on everyday life, Fiske argues that popular culture is not actually created by corporations who produce media and consumer goods. Rather, popular culture is made by individuals in society from the raw cultural goods and materials provided to them by those corporations, such as television programs or a mall. Similarly, in Certeau's (1984) model, consumption is one of the "tactics" used by "consumers" to subvert the "strategies" used by the "producers" of culture. While producers control the production of culture (or texts) as well as the spaces in which that culture is received, consumers can avoid the domination inherent in this relationship through resistive readings of texts. One of the examples Certeau provides is the writing of a love letter at work, whereby a worker essentially steals time from her employer, thereby subverting the power dynamic. Fiske (1989) applies this model to

the production of popular culture which he calls "the art of making do." Again, drawing on Certeau, Fiske continues: "The people's subordination means that they cannot produce the resources of popular culture, but they do make their culture from those resources" (pp. 4). For example, the mall is a privately-owned space designed with the aim of selling goods to consumers. As Fiske details, individuals can (to some degree) rework and remake the mall to suit their own purposes. Teenagers use the mall as a third space away from home to socialise with friends. Mall walkers use the mall as a warm, safe space to get their daily exercise. In both cases, the groups described use the mall for purposes other than consumption. In this way, individuals exert some degree of power within the systems they encounter in daily life. In Fiske's words: "[popular culture] always involves the struggle to make social meanings that are in the interests of the subordinate and that are not those preferred by the dominant ideology" (p. 2).

Using Fiske's model in this chapter, I show how users use and experience Facebook in ways that are not intended by its creators. Sometimes this is an intentional resistance, as I outline later in this chapter. Other times, this experience is unintended result which arises from the clash of Facebook's cybernetic utopian ideals with the everyday lived reality of participants, as evidenced by the case of social privacy -- a concept I introduced in Chapter 3 -- which differs from mainstream or legal conceptions of privacy which tend to render this form of privacy invisible or unimportant. On Facebook, social privacy issues arise as a consequence of the clash between the technological utopian values embedded in Facebook's project of radically transparent sociality, whereby society -- enabled by technologies such as Facebook -- can become more open, efficient, authentic and connected. As an essentially technological deterministic approach, the cultural, economic and social factors that may complicate the use of such a technology are ignored. The result of this disconnect between utopian ideals and the situated, everyday use of Facebook is social privacy threats, whereby users must navigate unfamiliar and uncomfortable social and privacy situations.

As I have argued in Chapter 3, the activities and communications on SNS are persistent, transferable, aggregateable, scalable, searchable, and cross-indexible. These

properties, especially the persistence of data, create reworked boundaries of time and space (Palen & Dourish, 2003) This means that information can be seen by unintended or unwanted audiences, even audiences that exist in the future (Tufekci, 2008).

Such a situation can create a threat to social privacy called context collapse or context collision, whereby users cannot manage the various aspects of their identities because their life contexts (such as work, home, religion) are merged into one. Thus, while institutional privacy is about data management and protection with respect to institutional use, social privacy is the management of identity, reputation, and social contexts.

In addition to Fiske's model of popular culture, then, another critical frame for this chapter is what I call *social privacy*. In Chapter 3, I identified social privacy as the management of identity, reputation, and social contexts. Social privacy concerns the management of what is disclosed about oneself by others, or identity management, and the ability to navigate and manage various social contexts. I also showed in Chapter 3 that institutional privacy threats -- such as top-down surveillance -- have been covered extensively in the literature. In this chapter, then, I focus on a the traditionally overlooked concept of social privacy. This chapter shows not only the existence of social privacy issues as a valid privacy concern, but also how immediate and pressing social privacy concerns become for individuals who use Facebook as part of their everyday social life. Building on this finding in the next chapter, I show that far from not caring about privacy, as the privacy paradox suggests -- the 20-somethings in my study were actually quite privacy concerned.

Friendship

I'm starting my exciting facebook (where people really live... what?!) and thought I would put up some pictures. These are from the summer of 2006 - so they include a lot of conference snaps and then some shots from the party that the wonderful Kate planned for my 25th birthday in september. Enjoy! - Penny's first Facebook post, late 2006

In the previous chapter, I showed how the design of Friendship is a physical instantiation of the discourse of Facebook where radical transparency and flattened hierarchies are a social good. Through a series of examples drawn from my fieldwork, this section examines the meaning and privacy implications of Facebook Friendship, where, as a result of this architectural imposition of flattened social hierarchies on users, choices about privacy and sociality become simplified and merged. I begin by introducing Penny, a study participant whose social life is heavily intertwined in Facebook.

Penny is a straight woman of Indian descent, but went to school in a number of different countries, finally settling with her family in Toronto. At the time of my research, she was in her mid 20s and was working as an educator. She was a heavy user of Facebook, with nearly 500 friends and 400 photos. Unlike many of the other early adopters of Facebook, she was neither in university or connected with the technology industry, nor would she describe herself handy with computers and the internet. However, she would credit Facebook with being her entry into the world of social media. She is close friends with Ben, another participant, and is also acquainted with his ex-boyfriend Dan, another study participant.

Penny frequently updated her status and was meticulous about her photos -- she regularly uploaded new ones, ensured they were properly labeled, and frequently changed her profile picture. Despite her heavy use, she joined later than most of her peers (but still relatively early relative to most users). She told me it took one of her friends walking her through the sign up process for her to join Facebook. Penny had not tried Friendster or MySpace because she thought they were "too teenybopery," which coloured her view of Facebook before she joined (and perhaps one of the reasons she resisted signing up). When she "finally" joined in 2006, all her friends welcomed her. She told me that she that "it was this whole world I discovered that everyone was on but me!" But she also notes that after she joined, "All these other people joined because of me. It became the way we communicated. We made a group for my workplace. And I remember everyone joking that I started this Facebook revolution."

During the course of my fieldwork, one of discussions surrounded a tumultuous friendship she had had during her university years with a young woman named Jess. The story is a snapshot of how Facebook's radically transparent sociality is taken up in the complicated social realities of everyday life. Penny had been living in a shared house with a very close friend of hers named Joe. Then Joe and Jess, who they were both friends with, started dating. Throughout the relationship, Joe was still very close with Penny, which became an issue for the couple. So when they broke up, there was an unspoken rift between Penny and Jess. Despite this, Penny added her on Facebook after the breakup and she accepted the request:

Penny: We're Friends on Facebook, but not friends in real life... I like the fact that I can see what she's up to, like going overseas for a year. She accepted me as a friend on Facebook, but would still never talk to me. I don't want to be friends with her again. I just wanted her to know that I wished her well.

Me: Was it a big deal when you added her?

Penny: No, I was just trying to show her that I wasn't mad at her. Because I thought that inside, she thought I was mad at her for taking him away in the first place. And I think I was just adding her as a "Obviously we used to be good friends, I'm wishing you well and I don't mind being friends again. I'm not gonna be the same kind of best friend because I'm not going to talk to you all the time but..." I would've talked to her more if she wanted to, but I wasn't going to, like, go out of my way to do that. So I just added her, and she added me back. And I wrote her a [Facebook] message, and then I wrote her an email cuz she didnt reply to the message. And then I wrote her a wall post. And she didn't answer either. When I found out through Facebook that she was doing her Masters, I wanted to write her and be like "Hey, I noticed on your Facebook page that you're doing this. I think that's great and I remember all the times you told me you wanted to do that. I'm just proud of you and I wish you well." She never

wrote back. And Joe got really mad that she never wrote back, cuz he was like "That was big of you, she's the one who hurt you. So with the Jess situation, I'm just happy that Facebook tells me that shes doing okay and doing her Masters for a year. And for me, since I had some level of guilt with Joe confiding in me during their breakup and then her feeling like I took him away -- which I didn't... Facebook helped me with that guilt in a way because I could see that she's doing fine and she's happy and I can wish her well because of it.

Me: What would you do if there wasn't Facebook though?

Penny: I don't know.

Me: Think about it...

Penny: Well, some of our mutual friends told me that she's fine. Actually, it's because of her mutual friends conversations on her wall that I know... I see them having these wall conversations and I click on their wall to wall I can read their conversation.

Penny's story points to a number of social privacy problems that arise as a result of Facebook Friendship's function as both a description of a relationship as well as a fundamental, yet covert privacy control. As a privacy control, Friendship regulates a two-way flow of personal information and activities between two individuals. For this reason, Ben, another study participant, saw Friendship in terms of trust. In his words:

The thing about Facebook is that the privacy only works if all your friends are well-intentioned. So really, who you add to your network is still really important. I was giving a talk on cyber bullying the other day, and I was trying to explain that the thing people are missing is that these sites use the word "Friend" for a reason... it implies a trust relationship.

In this context, choices about trust or privacy become conflated with social choices. Further complicating such choices is the binary and formalised nature of Friendship - users are only given a choice to accept or deny a Friendship request. There are no ambiguous, unarticulated in-betweens as is the case with conventional friendship. The result is that making good privacy choices becomes more challenging and convoluted for users. Indeed, even though Ben identified the trust aspect of Friendship, he was still faced with the challenge of balancing social courtesy with protecting his privacy.

An example of this entanglement between privacy and sociality was the unspoken rule I observed amongst study participants. If one receives a friend request from an individual you have met in person, it is considered rude to reject the Friend request even if the person making the request is disliked. In an IM conversation, I asked Penny why she herself was Friends with people she did not like, she stated "BECAUSE YOU ACCEPT PEOPLE WHEN YOU KNOW THEM."³⁵ Moreover, Facebook's design provides little in terms of plausible deniability whereby users can construct a socially acceptable fiction to explain why a Friend request was denied. Throughout the various iterations of Facebook's design, outstanding Friendship requests have been, to varying degrees, displayed prominently and persistently. In the early Facebook design, as study participant Lola recounted, outstanding Friend requests would appear at the top of every page until she made a design to accept or ignore. Thus, it is much easier to claim, for example, that a letter was lost in the mail than a Friendship request was not seen or received. As such, there is no often way to avoid social turbulence other than accepting a request. As Lola told me, the persistent requests for her to decide to accept or deny caused her to Friend people she did not really want to. As she describes: "I didn't want to be rude and decline, so eventually I think I added most of them [people she did not like]."

35. Penny's use of capitals denote how emphatic her statement was.

Jess likely accepted Penny's Friend request for social reasons, even though her lack of communication with Penny suggests she had no desire to actually be friends or share her personal life with her. And yet, as Penny told me, Penny was able to monitor Jess to the point where she knew Jess' activities and actually felt less guilty about how their friendship had turned out. Jess had made a social or emotional decision that ultimately compromised her social privacy. As the situation between Penny and Jess indicates, decisions about accepting a Friend request can become "Do I want to offend?" rather than "Do I want all of my life automatically shared with this person?" Likewise, I observed during my fieldwork that social concerns took precedence over privacy concerns. In Penny's words:

The thing is, a Facebook Friend, is not a real friend. And if you don't add them as a Friend, they know. And I don't want the embarrassment of having someone know that I didn't add them as a Friend. What if I bump into them later and they say "Hi, I tried to add you on Facebook, why didn't you add me?"

Elizabeth, who was on the receiving end of unwanted Friend requests, took a different approach. Elizabeth is much more of a private, reclusive Facebook user than Penny. She had just over 100 friends and about 25 photos. Elizabeth is a straight, white, and was also in her mid-20s. She was born in Vancouver, Canada and worked as a teaching assistant and an artist. Like Penny, she would not describe herself as tech savvy and was one of the later adopters of Facebook. She and Penny also went to high school together.

Even though she did not use the term "privacy" in her description, Elizabeth was concerned about the privacy functionality of Friendship. When Elizabeth and a mutual friend named Julie were talking about Facebook over dinner one night, the topic came up of Facebook rejection, which is the consequence of not accepting a Friend request. Elizabeth said: "I had to block both [two acquaintances from high school] because they both kept trying to add me... They just kept trying to add me [and didn't say anything]... It made me wonder, 'Why do you want to be privy to my life?'" Here, Elizabeth was on the receiving end of what she perceived to be a Friend request

made to solely to access to her life. Based on their ambivalent relationships in high school, Elizabeth came to the conclusion that the two acquaintances just wanted to spy on her. For Elizabeth, violation of privacy became the entire meaning for the Friend request -- her acquaintances just wanted functional access to her life.

Togther, Elizabeth, Ben and Penny demonstrate some of the complicated social situations that can occur when privacy choice become entangled with social choices. Moreover, it appears that this entanglement tends to emphasise one type of privacy over another. Unlike institutional privacy threats which are largely invisible and intangible, social privacy challenges can have immediate social consequences, including embarrassment or anger from peers resulting from a rejected Friend request. In this way, the immediacy of social privacy concerns created by Friendship's merging of privacy functionality with sociality -- such as worrying about one's reputation or the real motivation between a Friend request -- tends to distract from the potential, intangible institutional privacy threats, such as data collection, aggregation and mining.

The focus on social rather than institutional privacy concerns was reflected in my fieldwork. Many of the issues and concerns that study participants talked about can be described as social privacy issues. Institutional privacy issues were not discussed unless I specifically asked. For example, Penny told me that she had not realised until I mentioned it to her that personal information was being collected by Facebook Inc. or that the company was claiming ownership over everything she uploaded to the site, including her photos.³⁶ Further, study participants never described these social privacy situations using the word "privacy." By default, when we had conversations where the term was used, we were speaking about institutional privacy, which was something they tended to not be concerned about or even aware of in the context of Facebook.

36. Facebook has since changed their Terms of Service and no longer claims to own the intellectual property that users upload to the site.

The lack of connection between privacy and the issues being faced by study participants suggested that the use of a "Friend" -- a relatively vague relationship descriptor -- to describe a core privacy control on Facebook encourages certain conceptions of privacy over others. Intentional or otherwise, the avoidance of the term "privacy" may reduce user concerns about sharing, thereby helping users to get over what Zuckerberg see as privacy "hurdles" which keep users from sharing and being more open. As I outlined in Chapter 3, privacy, as a concept, is associated with various negative situations, such as being monitored, being exposed or losing control over one's information. In my previous work on LiveJournal Friendship, I found that the use of the word Friend as a functional system descriptor caused conflict for users faced with unwanted Friend requests. As with Facebook, users would sometimes compromise their privacy and accept unwanted Friend requests because of the connotations carried with the term (Fono & Raynes-Goldie, 2006). In using "Friendship" and its positive associations rather than "privacy," and its negative associations, Facebook Inc. can encourage users be more "open and transparent."

Overall, users in my study had a relatively large number of Friends and were, for various social reasons, often open to accepting Friend requests from individuals they did not wish to share with. The group average was around 300 Friends, with one participant having over 500. In the context of Dunbar's number -- which holds that the maximum number of people an individual can maintain a stable and cohesive relationship is around 150 (Dunbar, 1998) -- it seems unlikely that study participants had strong, trusting relationships with all of their Friends. This behaviour around Friendship fits with other research findings that suggest the norms on Facebook, especially among younger users, is to have number of Friends, even if most of those Friends can better be described as acquaintances (Brandtzæg et al., 2010, p. 1022). The result is that users are likely sharing more information with more individuals than they would otherwise.

Lifestreaming

As I have shown, Friendship is a binary privacy control which regulates informational flows between two individuals. By merging privacy functionality with a relation-

ship descriptor, Facebook's architecture makes privacy management more challenging, especially in the context of social privacy. As with Friendship, automated informational flow, or lifestreaming, is a central to radically transparent social architecture of Facebook. It too, creates novel privacy challenges for users. In this section, I examine the privacy consequences of lifestreaming on Facebook in the context of Nissenbaum's contextual integrity.

As I examined in chapters 5 and 6, beginning with the addition feeds in 2006, Facebook's architecture has shifted from static profiles pages to dynamic, continually updated streams of information. Features on Facebook, such as the wall, the newsfeed, status updates and so forth push automated streams of information out to one's network of Friends. Further exacerbated by the confusing and constantly changing privacy settings, even a seemingly small changes to one's profile -- such as removing a relationship status as a result of a breakup -- can become unexpectedly pushed out to all of a user's Friends. Since these feeds are automatically generated by Facebook, there is no feedback to the user to know which information has been seen by whom or when. Further, with Friends averaging in the hundreds, it can become difficult for a user to remember just who could be seeing a new status update or photo.

In this account of his activities on Facebook, James provides a telling example of how lifestreaming complicates and challenges the management of privacy. James, who joined the study through Lola, was in his early 20s and began using Facebook when he was a university student. James was a white, straight male and like Lola, was also an engineer. James had about 250 Friends. His favourite part of Facebook was photos, reflected in the very high number he shared with Friends (about 1,700). James was quite self-reflective about his Facebook use. For Lent³⁷ in 2008, James decided to delete his Facebook account. Before Lent was over, he posted a note on Facebook beginning with the following:

37. A Christian observance whereby individuals fast or give up a luxury as penance.

I'm back on Facebook. I know that Lent isn't up yet, but you'll have to take my word that I just needed an arbitrary checkpoint to pull myself from it. The purpose of leaving Facebook was mainly to take some time to think about what it meant to me and how I wanted to use it. I also wanted to see what would happen, since we all take it for granted, and I figured it would help me cut down on procrastination as well.

James' ambivalence about Facebook centred around the social privacy challenges with which the site presented him. On the one hand, James liked the social benefits he derived from being on Facebook, such as being invited to parties or being able to see what his friends were doing. Yet, at the same time, he was also keenly aware of challenges posed to managing access to his personal information and activities. As these situations were relatively uncommon before Facebook, James and other study participants are still working out how to negotiate and understand their implications, particularly around the negotiation of publicness and privateness. As I discussed in Chapter 3, the spheres of public and private are becoming more overlapped, particularly on sites such as Facebook. For example, James felt uncomfortable about the public nature of wall conversations, where for whatever reason, users tended to engage in conversations that would have otherwise remained private. Each user's profile has a wall which is not only public, but whatever is written on it is also automatically pushed to all of one's friends. As James told me:

[The wall] strikes me as something we've never done ever. There's no such thing as public conversation. It's like having a conversation on the subway with your friend, but shouting all the way across the car then sending transcripts of your conversation so that they can go home and read it anytime. It's nuts! Sure you can use it to send links, but people use it for the most dramatic conversations, with the most personal stuff. I don't trust my friends... I worry about something leaking.

As a reflexive Facebook user, what particularly alarmed James was his own behaviour with respect to wall posts and other lifestreamed information:

You know how you can vote for what you want to see on your homepage? I currently have mine set almost exclusively to photo events, wall posts, and relationship status updates. Ever posted a photo but taken it down the next day? I've already seen it. Broke up with your girlfriend but then resolved it on the phone an hour later? I saw what you did there. Friends feel the need to plan your next movie outing on your wall? Maybe I'll come too! I am the very person that I fear, and I find that fascinating.

As James recounts, he worries that other people will behave in the same way he does. Legally, James is not violating anyone's privacy, since all the information he is looking at has (at least arguably) been willingly shared by his Friends. Functionally, James can see the activity of his Friends, yet on some level it makes him feel he is seeing something he was not meant to. What James implicitly references in his concern is a violation of contextual integrity, whereby information shared for in one context or group of individuals ends up in another. Information shared by his Friends, although viewable to him, was likely not intended for him. This is either because a Friend changed their mind about sharing; made a mistake; or were not thinking about who might be looking beyond a certain group of Friends. The complex nature of Facebook's confusing, unclear and ever changing privacy settings could also be another reason: James' Friends were perhaps unaware of their privacy settings or how an element of Facebook functioned. As I observed with other participants, it can be easy to assume only the intended audience will look, while uninterested parties will simply not be paying attention. However, as I show later in this chapter, in the section on "stalking" or "creeping," the opposite is commonly the case.

In sum, James provides an example of why users must be ever vigilant in managing what and how they share on Facebook. Further, in order to ensure information is being shared appropriately, they must be constantly aware of, and reactive to, Facebook's changing settings or overall design. As I show in the next section, when lifestreaming is combined with other features such as photo tagging, the management of privacy can become an even greater challenge.

Loss of Identity Control

In addition to violating contextual integrity, the increasing integration of personal informational flows into the core functionality of Facebook poses challenges for privacy in terms of identity and reputation management. As I showed in Chapter 3, identity control is a critical, yet sometimes overlooked aspect of privacy. Indeed, identity is one of the principle boundaries that Palen and Dourish (2003) identify as key in understanding privacy management. Likewise, identity management is one of the fundamental elements of social privacy. As I will show in the next chapter, the management of social privacy is largely about achieving a the optimal balance between the social benefits and drawbacks of disclosure. In addition to identity, Palen and Dourish (2003) identify disclosure as another key privacy boundary. At the disclosure boundary, "determinations are made about what information might be disclosed under which circumstances..." (pp. 3). Thus, livestreaming creates turbulence at both the disclosure and identity boundaries by making it difficult for users to know who is seeing their information and in what context. As Palen and Dourish describe: "To withhold information [in order to manage one's identity], one needs to know from whom it is to be withheld and how that can be done, which requires an understanding of how our actions will be available or interpretable to others" (Palen & Dourish, 2003, p. 4). By removing the ability for users to know exactly what information about them is being shared, who is seeing that information and in what context, it becomes more difficult for users to know what information may or may not be appropriate to share. Without this knowledge and control, users face challenges managing their digital identities on Facebook.

Identity control was also one of the primary concerns of my participants. However, as I observed with the other aspects of social privacy, study participants did not use the term "privacy" to describe their concerns. The most common concern that I observed with respect to this form of privacy was regarding photos, particularly photo tagging or the linking of uploaded photos to one's profile page. Facebook's design permits all of a given user's Friends to tag them in photos. As such, Friends can tag any photo they wish, without prior consent, including photos that contain embarrassing or contextually inappropriate content. Once tagged, a photo not only appears on

one's profile page, an announcement of the new photo is automatically streamed out to all Friends through the news feed. The implication of tagging, then, is that requires a user to give up a degree of identity control to one's Friends, who must be trusted to not upload a photo that could cause social or professional strife. One of the most pressing issues reported by participants was that Facebook did not provide users with a privacy setting that would put new tags through a moderation process. Both Lee and James told me they did not like how they could not preemptively stop Friends from tagging. James told me he experienced a loss of control with respect to his identity because "you're competing against how many friends you have." James' experience is in line with Brandtzæg et al.'s finding that having high number of Friends -- as most of my participants did -- can compromise one's privacy. In their words: "the network asserts control over individual users by co-creating their self-presentation" (Brandtzæg et al., 2010, p. 1023). The bigger the Friend network, the less power the individual has over his or her identity. James also observed that "Even if you've killed your account people can still tag you in photos." Ironically, having a Facebook account in this case does provide more identity control, since without an account, individuals cannot untag themselves in photos.

In 2006, a former Harvard student wrote an email to Chris Hughes, the then head of privacy at Facebook Inc., explaining the impact the design of tagging had on his life: "By launching the photo feature and creating the system of easy linkages and tagging, you guys have dramatically changed social interactions. Some people envision an upcoming era of 'no camera' policies at parties and a growing sense of paranoia among college students worried that all their actions on Friday night appear online just hours later, accessible to hundreds or thousands of users (e.g., I can see Betty getting wasted at the Pudding even if I can't access Betty's profile). A single user with low privacy restrictions 'overcomes/ruins' all the protective and restrictive steps taken by peers." (Cassidy, 2006, p. 7)

Four years later, this prediction came true. In response to the lack of identity control they experienced on Facebook, students actually began having parties where cameras were banned, with others resorted to implementing dark rooms at parties to protect their reputations (Kirkpatrick, 2009). Combined with livestreaming and ever-

changing default privacy settings, features like tagging further challenge the ability of users to manage their social privacy. As I show in the following sections, these privacy complications manifest into two previously uncommon social dynamics, taking the form of "creeping" and "context collapse."

Creeping

As Penny and Elizabeth's stories exemplified, social privacy issues -- such as being surveilled by one's Friends -- come to the fore when choices about privacy and sociality are intertwined. Since Friendship is a privacy control, the act of a user accepting an unwanted Friend requests to avoid unpleasant social situations also opens them up to unwanted surveillance. Combined with increasingly open and permissive privacy settings (for example, the default setting for new photo albums in 2008 was open to everyone), a key outcome of Friendship as privacy is the prevalence of peer-to-peer surveillance (Andrejevic, 2005).³⁸ This activity is common enough among Facebook users that they have given it a name: "creeping." In this section, I show the increasing prevalence of this activity as reflected in popular culture and by the activities of my participants. I then examine creeping as a privacy violation in the context of social privacy and contextual integrity. I conclude with a discussion of creeping in contrast with the discourse of Facebook.

Creeping, which was used interchangeably with "stalking" and "spying" by study participants, describes "the subtle form of stalking" which people routinely engage in on Facebook (Kirkpatrick, 2010a, p. 92). It can describe routine observation of one's Friends, or surfing on Facebook for Friends of Friends or people who have open accounts or public photo albums. Since Facebook's design does not tell users who has viewed their profile or information streams, creeping is an invisible activity. The popularity of this activity is suggested by its increasing appearance in the mainstream media and popular culture. For example, a 2011 episode of *Nurse Jackie* used the term in an episode that centred on Facebook (2011). A 2011 article in *Maclean's* (a national Canadian news magazine) defined creeping "anonymously [invading] the

38. Tufekci (2008, p. 35) has also described it as "grassroots surveillance" or "peer monitoring"

privacy of people you don't really know" and also suggested that the activity was Facebook's "most attractive purpose" (Teitel, 2011). Creeping has an entry on *Urban Dictionary*, a popular user generated dictionary of slang, again suggesting how common the activity has become:

Following what is going on in someone's life by watching their status messages on Instant Messengers such as MSN, and their updates to their social networking profiles on websites like Facebook or My-Space. Akin to stalking in the real world, but usually done to people who are your friends that would normally share this information with you, however you're just too busy to keep up conversation with them (Urban Dictionary, 2011).

Even in the early days of Facebook, creeping was common enough phenomenon to be observed by Zuckerberg and other early employees, who called it "the trance" (Kirkpatrick, 2010a, p. 93). Sean Parker, an early investor in Facebook and co-founder of Napster described it as hypnotic: "You'd just keep clicking and clicking from profile to profile, viewing the data" (Kirkpatrick, 2010a, p. 93).

In my fieldwork, the most common surveillance-related activity which I observed participants going through another person's photos, sometimes making negative or judgemental comments. A 2010 study also noted that creeping or "social curiosity" was a common activity on Facebook (Brandtzæg et al., 2010, p. 1021). This study also reported that individuals who like to creep other people's photographs on Facebook prefer to creep individuals they do not know at all, or only very little. As I show in the following examples from my fieldwork, I also found the trend of observing strangers, near-strangers or enemies to be common.

Ben and Dan had extended discussions with me about creeping. Ben admitted to being Friends with people just so he could creep their profiles, while Dan described to me the extreme lengths he went to to creep people he did not like. At the time of my research, Ben was also in his mid-20s, was working in the education and technology industry and was living with his ex-boyfriend and roommate Dan. Ben is from a

Scottish family and was born and raised on PEI, a small island province on the east coast of Canada. He was an early adopter of Facebook and had over 350 Friends and more than 250 photos at the time of my fieldwork. Dan is a gay white man who was in his early 20s. He had moved from the United States and was attending university in Toronto. Like Ben, Dan was an early adopter, joining as soon as his university network was granted access to Facebook. Like most other participants, Dan was an avid user of Facebook with over 300 photos and over 200 friends. He told me he had had multiple fake accounts in different regional networks to circumvent Facebook's geographically-based privacy restrictions (which were, as of June 2009, slowly being overhauled). Dan would use these accounts to creep people he knew who had blocked his real account, but had left their privacy controls on the default privacy settings -- meaning only users in their regional network could see most of their profile information:

Dan: [Creeping] has even gotten boring, because I think I've done it to everyone that I've ever seen. I mean, I do have like three Facebook accounts. One for Toronto and one for Buffalo, because I've been blocked by two people on Facebook that I know of. And one's in Buffalo and she's stupid because her Facebook profile is open for Buffalo [the default setting at the time, which allowed anyone in that geographical network to view it], so my second Facebook profile is in Buffalo so I look at her profile and see what she's done.

Me: Why do you look at her on Facebook?

Dan: Because she blocked us so we like to know what she's doing because, like to spite her. Like we can still see it, ha ha. It's never interesting.

Me: Who are the other people?

Dan: Who I stalk? Oh, the other person who blocked me is this guy I dated for a little while and he blocked me on Facebook because I misdirected a text message. I thought I was replying to Ben and I was saying something like, "I don't like him, he's not fun to hang out with,

I don't even like his company" and then I realised who I sent it to, and I was like, "Ha ha just kidding" and he was like, "you didn't mean to send that to me," and I was like, "Nope you're right." So then, by the time I was home -- this was on the streetcar -- I was blocked on MSN, Facebook and his MySpace was private. Because of me. It was awesome. I didn't have to talk to him again, but I did have class with him.

Lee also admitted to using the same strategy to creep people. Lee is a white man originally from Sudbury, Ontario who was in his mid-twenties during my fieldwork. His sexual orientation is undeclared. Like Dan and Ben, Lee was a prolific user of Facebook and had the largest collection of photos that he was tagged in of all study participants (335). However, he had a relatively smaller group of Friends (165). During my fieldwork I spent time Lee's house with a group of his friends. We started talking about an ex-girlfriend of Lee's who Lee had had a dramatic falling out with years ago. The group wanted to know what was going on in her life. Lee did not have her as a Friend on Facebook, but his friend Calvin (who was also at the party) did. Calvin logged into his account on Lee's computer and showed us her account, so we could "see what she was up to."

Like Lee and Dan, Lola, a straight female engineer born in Toronto to parents who came to Canada from Hong Kong, also shared with me that she creeped people she "hated" or who "annoyed" her for the purpose of keeping tabs on them. Equating it to being like a "car crash," Lola would even avoid defriending someone she did not like simply so she could keep "spying" on them. Towards the end of my fieldwork, Lola was triggered by a bad breakup to delete her Facebook account. Her decision was largely related to the ability to creep enabled by Facebook, as she relayed to me over IM:

I didn't want to see any of [my ex's] updates or his anything. I know I could've just unfriended him, but just the fact that I could look him up (face it, we're all stalkers! Even for those people we don't want anything to do with) killed me. I think it was necessary so I could distance myself from him as much as possible.

In many of these examples of creeping, particularly involving the surveillance of enemies, Friendship becomes primarily functional as in informational access control, while not expressing elements of a friendship at all. Instead, it is a form of unwanted peer-to-peer surveillance enabled and facilitated by the architecture of Facebook. In this context, Friendship is not about friendship and trust, but about surveillance and privacy violation. As law professor James Grimmelman argues, Facebook's design encourages users to share more by making them feel their information is being shared with the right people, while still leaving them vulnerable to invisible and unwanted creeping: "Facebook's design sends mutually reinforcing signals that it's a private space, closed to unwanted outsiders... [yet] unlike in a restaurant, potential eavesdroppers are literally invisible" (Grimmelmman, 2009, p. 1162). Indeed, even if users have only Friendened people they actually wish to share with, Facebook's confusing and ever-changing privacy settings -- as demonstrated by Dan -- can still leave users unwittingly exposed to creeping.

As such, in the framework of Helen Nissenbaum's contextual privacy, creeping is a privacy violation. To varying degrees, participants were aware of being watched by their Friends. Penny carefully managed her photos and profile for this reason. Elizabeth was more overtly concerned about being creeped, and for this reason was careful who she accepted as a Friend. Generally, however, most participants did not seem concerned about being creeped by enemies or other individuals with whom they had troublesome relationships with. This disconnect suggests that participants shared information on the site expecting to share with Friends rather than enemies. Moreover, participants were generally not expecting to face judgement or ridicule from their Friends. This expectation is furthered by the invisibility of creeping -- users can only guess who is viewing their profile and why. Further, there is no feedback mechanism to indicate who, beyond one's Friends, might be viewing one's profile as a result of confusing privacy settings. However, in all the cases I observed in my fieldwork, the individuals being creeped were disliked by the people creeping them. To have their information used in this way was not how users had intended. Since the information is not being used as intended by participants -- or indeed, in the positive manner suggested by the term Friend -- creeping is a violation of contextual information flow.

More broadly, creeping speaks to a disconnect between the aims of Facebook Inc.'s designers and its actual use. As I discussed in Chapter 5, it appears that Zuckerberg truly believes he is making the world a better place by improving communication and understanding between people through openness, transparency and authenticity. And yet, creeping among study participants suggests the opposite is happening. Even those who engaged in creeping did not find the experience entirely positive or rewarding. Penny was ambivalent, telling me "Yeah I hate it, but I also love the fact that I can go spy on someone," while Ben shared with me that he would often find himself creeping people's photos for hours, only to find himself regretting it later. In encouraging openness by default without a change in contemporary Western culture and society, Facebook enables people to violate each other's social privacy with the aim of ridicule and judgement rather than increased understanding and compassion. In the same vein as the New Communalist's gift economy, Zuckerberg has also stated that he believes sharing information on Facebook is akin to a gift. In a sense this is also true here -- creeping is an unintended gift of entertainment, but entertainment at the expense of other people and their privacy.

What this disconnect suggests is a failure of technological utopianism to improve the world through technology alone. By ignoring the social, cultural and economic factors that shape behaviour online, the technology of Facebook can only go so far in creating positive change. In expecting the technology of Facebook to radically change the world without changing these other factors as well, Zuckerberg has -- perhaps inadvertently -- fostered an antisocial, privacy violating activity.

Context Collapse

Creeping, and its consequences for privacy, are further facilitated and complicated by context collapse, sometimes called "context collision," or "context fuck" by study participants. Context collapse is the flattening and merging of all life's social boundaries in terms of contexts, identities and relationships -- such as personal and professional identities and contacts -- into one larger context. It is an "all friends in one-place solution" (Brandtzæg et al., 2010, p. 1007) which is reflective of the cybernetically inspired belief that flattened social hierarchies are beneficial to society.

The result is that users must navigate multiple yet undifferentiated social contexts; audiences; and sets of social norms with a single profile and identity. In the context of identity management as privacy, context collapse is a key example of a social privacy threat. The ongoing management and renegotiation of identities and relationships within a context collapse can be described as "boundary turbulence" (Stutzman & Kramer-Duffield, 2010). In this section, I examine the architectural causes of context collapse on Facebook in terms of binary Friendship; unified identity and the management of space. I then provide three examples of context collapse from my fieldwork.

On Facebook, context collapse arises from three specific architectural features. The first is Friendship as a binary privacy control, where, by default, users are required to essentially make an all or nothing privacy decision whereby all accepted Friends are given the same level of informational access, regardless of social contexts or hierarchies. As Grimmelmann, writing about problems with privacy on Facebook, describes:

.... social network sites require explicit representation of social facts. Offline, I can think of you as "my friend Bob from work" and loosely associate with that hook my various memories of a stressful preparation for an important presentation, a water-balloon fight at the company barbeque, and the way you covered for me when I was sick. All of these thoughts are implicit. I don't need to articulate precisely our relationship or what goes into it; you're just Bob, and I can make decisions about how much to trust you or what to invite you to in an ad-hoc, situational manner, on the basis of all sorts of fuzzy facts and intuitions. But Facebook reifies these social facts into explicit links: we're contacts, or we're not. Everything is explicit and up front—at the cost of flattening our entire relationship into a single bit (Grimmelmann, 2009, p. 1172).

Embedded in this flattened, binary nature of relationships, is an assumption of equal trust levels for all Friends, who in turn, are granted equal informational access. However, everyday social life for most individuals is not egalitarian. Different relationships contain different power dynamics and degrees of intimacy. Some people have power and influence in one's life, such as employers or landlords. Some people one sees everyday, but are still acquaintances rather than close friends, as is the case with co-workers or store clerks. Relationships with others exist on a loose, generally unspoken hierarchy. Depending on one's relationships with those present, one behaves in different ways, revealing or concealing different aspects of one's life:

...businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child... In each case, the sort of relationship that people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have (Rachels, 1975, p. 328).

In artificially flattening social hierarchies, Facebook's design creates an "equivalence between ties that is not representative of their inherent variable strength. This presents a challenge for disclosure regulation, as ties of varying strength have different maintenance requirements" (Stutzman & Kramer-Duffield, 2010). Put simply, Facebook's design does not facilitate the management of varied trust levels or social contexts.

The second architectural feature which contributes to the context collapse on Facebook is the singular, unified profile to which, by default, all Friends are given access -- again, regardless of social context or hierarchy (Stutzman & Kramer-Duffield, 2010). In this way, a user's various identities and ways of behaving which are relative to life contexts, such as work and home, are collapsed into one. Even the relatively coarse controls around Friendship do not offer a way around this context collapse via a unified identity. At the time of my fieldwork, Facebook offered a "limited profile" which was a list Friends could be put on that would prevent certain Friends from seeing select profile elements, such as the wall. This feature, however, was infrequently

used (none of my participants discussed ever discussed it) likely because it allows for no degree of plausible deniability. Anyone on limited could tell they were on limited by the fact that they could see the wall of the user in question. This feature has since been replaced by Friends lists, which allow multiple lists that can each be customised to show different profile elements. Critically, however, as with the original limited profile, profile elements are either on or off. This means users on a restricted list can deduce, from seeing a profile with missing profile elements, that they are on a restricted Friends list. The result is potential social or professional embarrassment. The third contributing factor of context collapse is Facebook's lack of physical cues. Conventionally, many notions of privacy are tied to notions of physical space and place -- place being a space imbued with cultural or social meanings, such as private or public, professional or personal. As Palen and Dourish argue, "Our most familiar ways of managing privacy depend fundamentally on features of the spatial world and of the built environment, whether that be the inaudibility of conversation at a distance, or our inability to see through closed doors." (Palen & Dourish, 2003, p. 2) Many social cues tied to privacy also are physical, such as interpersonal space and physical touch. Indeed, different places have different meanings and "behavioral frames" which indicate to people what behavior is appropriate and acceptable (Dourish & Harrison, 1996, p. 3).

Physical space divides up public and private places and thus expectations about when one has or does not have privacy. For example, what goes on in the home is often seen as private, whereas anyone engaging in an activity in a public space, such as the street or a park, should not be surprised if other people are aware of their actions.

Likewise, physical spaces can help one determine who might be listening. As Grimmelmann describes, "We don't say private things when the wrong people are listening in. To know whether they might be, we rely on social and architectural heuristics to help us envision our potential audience." (Grimmelmann, 2009, p. 1162) In this way, physical contexts -- such as the home, a temple or an office building -- combine with social cues and hierarchies to act as guides which can be deployed to navigate the multiple and overlapping social contexts encountered in everyday life. In a sense,

space can be seen as a physical (or analogue) privacy control that can be used to manage and regulate one's privacy.

However, in electronic "spaces" such as Facebook, there are no physical boundaries to delineate different spaces, contexts and behavioural expectations. On Facebook and other digital spaces, then, "our ability to rely on these same physical, psychological and social mechanisms for regulating privacy is changed and often reduced" (Palen & Dourish, 2003, p. 2). Further, as privacy researcher Zynep Tufekci outlines, it is also difficult to know who might be privy to the information shared online:

...in technologically mediated sociality, the audience has been obscured. We can no longer see who is looking, nor, sometimes, can we even make an educated guess. If one is in a street corner, a classroom, the beach, or a bar, the audience is limited by walls, doors, and distance. Although it is possible that there may be unexpected members within the audience, the presence of others is much more transparent than it is on the Web (Tufekci, 2008, p. 22).

Taken together, Facebook's unified identity; binary Friendship; artificially flattened social hierarchies; and lack of physical cues create a collapse contexts which create friction for users trying to manage their identities, reputations and self-presentations. In the next three examples from my fieldwork, I show the social privacy challenges faced by study participants.

During my fieldwork, Facebook Inc. began to crack down on younger users, forcing anyone who appeared to be under 18 into high school networks, ostensibly to protect their privacy. Penny was 26 at the time, but someone at Facebook Inc. decided she looked much younger. Penny received an email which informed her that if she did not join a high school network, she would be removed from Facebook. Since Penny had long since graduated from high school, it would be impossible for her to join such a network. In response, her friends created a group to support her, complete with a photo of her pretending to chug a beer as visual evidence that she was over 18.

This photo was an in-joke among her friends, since she rarely drinks. Without this context, it would appear Penny was quite into drinking and partying. Eventually Facebook Inc. realised Penny was not in high school. However the group remained and was forgotten about.

Since Penny had not started the group, she had no control over her name and potentially incriminating photo being used together. A few years later, during my fieldwork, Penny had applied to move into a new apartment. The landlord did a background check on her, including a Facebook search, which revealed the drinking photo. Rather than rejecting her application outright, the landlord called Penny to ask about it, and she was able to explain the story behind it. He then accepted her application and she moved into the new apartment.

Not only was Penny was lucky to be given the opportunity to contextualise the photo, she was lucky to have an explanation that mollified the landlord. However, her situation does raise unresolved questions about the privacy implications of Facebook's radically transparent sociality. For example, if the photo did indeed reflect the drinking habits of Penny, would it be morally acceptable for her landlord to reject her on those grounds? Legally, drinking when one is 26 is not against the law in Canada. An argument I often encountered during my fieldwork, particularly in the mainstream press, was if an individual is fired or otherwise faced social or economic hardship from drinking photos on Facebook, they have no one but themselves to blame. Yet, as Penny and my early example of photo tagging show, individuals are not always responsible, nor can they entirely control their digital identities.

Overall, this example not only shows the potential real life risks of context collapse - where a photo intended for one audience is seen by another -- but also shows that forcing functional equality on Facebook does not actually make individuals equal in any real social, economic or cultural sense. Regardless of their Friendship status on Facebook, Penny's landlord still holds a degree of power over her by controlling, to some extent, where she can and cannot live.

Penny's example shows some of the potential privacy risks created by context collapse whereby information is taken out of context or seen by unintended audiences. As Ben told me in an email about a situation he dealt with where he worked, which was an online community for global youth, context collapse can create tension between one's personal and professional identities, thereby threatening free speech:

On Feb 1, 2008 9:41 AM, Ben <ben@***.org> wrote:

So we actually had this situation at work...

Our coordinator for the Middle East region (which INCLUDES Israel) is a jordanian-canadian... Great girl, really trying her best...

But a few weeks ago on Facebook, she joined a group called "Facebook, delist israel because it is not a country!" that is filled with quite a bit of borderline hate-speech. And not that I'm defending israel in a no-fault kind of way, but the reality is that she manages our relationship with the WHOLE region, and she has not only friended other staff on fbook, but also online community members.

I wrote the boss a note about how problematic it is, and how, while it might seem like we're meddling in her private life, having someone who holds those views in that position is incredibly problematic for a number of reasons, and we really need some kind of policy on the personal/professional division/where exactly it lies.

The situation Ben describes is a not only complicated, but was relatively uncommon before Facebook came into mainstream usage. The coordinator has a right to free speech and expression in her private life. However, as Facebook's architecture does not provide a mechanism for her to manage her multiple identities, a conflict emerges. Facebook's context collapse makes the coordinator's views public across the various social contexts of her life. As such, would be unprofessional for her employer to simply ignore the situation, as they could more easily do if the coordinator held these beliefs in private.

Ben, too, faced a similar professional/personal context collision. Indeed, one of the reasons for including Ben in my study was that we had both worked at the same organization when Facebook started to become popular in our office, and then Toronto at large. Together we had experienced the shift and then collision of Facebook as a clearly personal, social space to one which merged contacts from all aspects of our professional and personal lives.

As an early adopter of Facebook, Ben had used Facebook primarily for socialising with friends and peers from university, rather than professionally. His profile and public wall conversations reflected this identity. When Facebook was opened for the rest of the world, everyone at his work place began Friending him. His professional identity and social identity collided. Ben told me he felt especially awkward when a police officer he knew professionally sent him a Friend request:

The guy who runs the anti-drug education strategy just added me to Facebook, and I don't know what to do, because he's a nice guy, but he's 50 and it's a total context fuck...Not that I'm a drug fiend or anything. But, I mean, my statutes are fairly regularly about binge drinking.

These situations show how context collapse could potentially threaten one's professional identity by providing professional contacts with information that is inappropriate for a work setting. Further, as the coordinator at Ben's office showed, context collapse can unintentionally give one's employer contextually inappropriate information about oneself. As Baym has argued, Facebook's focus on friendship may give people the sense they are communicating mostly with actual friends, while forgetting how public or searchable their activities are. And then "When a profile is accessed by an unexpected viewer the results can be embarrassing or life-altering. Information posted in a SNS can be used outside of context with strong negative consequences, including lost jobs, revoked visas, imprisonment, and tarnished reputations " (Baym, 2010b, p. 389). In sum, when a privacy feature assumes everyone trusts each other equally, it ultimately becomes a social privacy threat

where users are forced to choose between saving face or saving privacy.

Management and Resistance

Returning to Fiske (1989), one of the things I have demonstrated in this chapter is that -- in order to maximise the social benefit of Facebook while minimizing their loss of privacy -- users make their own out of Facebook, pushing and reworking the boundaries where they are able. A useful way of understanding, more specifically, what boundaries can be pushed and reworked and which are largely fixed, is a model from the field of education that describes the three different modes of information is instilled in students: the the formal, the hidden and the null curriculum (Eisner, 1985; Pelletier, 2008).³⁹ The formal curriculum is the obvious, fixed lesson plan, such as which mathematical concepts will be covered in a given semester. The hidden curriculum is what is implied through the structure and system of the educational system. It consists of appropriate classroom behaviour, how to interact with the teacher and so on. It can also include knowledge about ways to game or subvert the system, such as the strategies deployed by a teacher's pet. This curriculum is learnt largely informally and invisibly through experience. Finally, the null curriculum is what is not taught in a curriculum, and thus, what messages are implicitly sent by that omission. For example, by teaching the history of Canada beginning with European colonists, the null curriculum is the history and culture of Canada's Aboriginal people, thereby implicitly sending a message about what is important and valid and what is not.

Developing a formal literacy of Facebook means picking up a basic understanding of its explicit and obvious features as well as its official rules, as outlined in the Terms of Service. It is an understanding of Facebook that is in line with how Facebook Inc. would like its users to behave. In Fiske's model, it is a hegemonic use of the site. The null curriculum, on the other hand, is what is outside of discussion. In other words, what is not permitted or avoidable. For example, users are given the choice, at the formal literacy level, to accept or reject a Friend request. It is a choice on a simple, rather meaningless level. What users are not given is a choice about having to make

39. Thank you to Jason Nolan for this connection.

this choice. Thus, what is not permitted is the avoidance of this choice altogether. More broadly, this lack of any real choice denies users of any meaningful engagement with privacy decisions or the everyday consequences of Friendship decisions. If one is to use Facebook, one must continually make the choice -- is this person my friend, yes or no? It is at the level of the hidden curriculum and the literacies that go with navigating it, however, where users can push boundaries within the constraints of Facebook's architecture, as described in Fiske's model of popular cultural production. It is these hidden literacies which I draw out more in this section.

As I touched on in the previous chapter, there are social benefits that come participation through disclosure on Facebook (Tufekci, 2008). At the same time, non-participation in Facebook, especially for younger users, can be socially costly (Thompson, 2008). Accordingly, users seek to optimise and balance these social benefits with their privacy. For this reason, experienced users, such as the early adopters in my study, have become literate in the hidden curriculum of Facebook. This hidden literacy of Facebook is not created by Facebook Inc., but rather by users, as manifest in the user culture on and around Facebook. As such, experienced users of Facebook can go beyond the officially sanctioned uses of the site to rework and push the boundaries of what is and is not permitted. In this way, users engage in subversive privacy practices both to protect their own privacy, optimise social benefits and sometimes violate the privacy of others.

One of the main subversive ways that users attempt to protect their social privacy is the use of an alias. Pablo, an newspaper editor, told me his boyfriend used "Awesome Andrew" as his Facebook name. The name he used as his last name is his real first name, but obviously "Awesome" is not. Other participants will use a real first name, and then the first initial of their last name, or will use an entirely made up last name. The goal of this activity is to make it difficult for people to find them via search, or to attribute their Facebook activities to their "real" identities. The use of names in this way actually violates Facebook's ToS, which stipulates that users must use their real names and identities when using the site. Occasionally (although to a lesser extent as of late), Facebook will delete accounts for this reason. Indeed, Facebook

Inc.'s CEO, Mark Zuckerberg, casually revealed in a 2005 interview that they had algorithms crawling the site, performing various tasks such as analysing how "real" users were, in order to detect fake accounts (Stanford University, 2005).

Beyond my fieldwork, other evidence suggests this type of privacy enhancing activity is not uncommon. boyd (2007b) observed similar behaviour in her larger ethnographic study on teenaged MySpace users who will use fake names, birthdays or other information in order to protect their privacy on the site. Peterson (2009) reported analogous behaviours in his work with college-age Facebook users. Further, privacy regulators and advocacy groups, such the Information and Privacy Commissioner of Ontario, have advocated for the use of pseudonyms and multiple or partial identities as critical privacy management tools (Cavoukian, 2008), especially for children and youth (Steeves, Milford, & Butts, 2010).

Another method used to enhance social privacy is to delete wall posts and photo tags which would otherwise be kept and publicly displayed indefinitely. Pablo told me he took the time to clean his wall once a week because he did not like other people reading them. While this strategy does not violate the ToS, Facebook's design -- which is aimed at making as much communication visible as possible -- is not conducive to this sort of activity. Each wall post and tag must be deleted manually, and as mentioned, Facebook does not provide any method to pre-screen tags before they are applied.

Creeping, as I outlined earlier in this chapter, can be seen as another subversive or resistive use of Facebook. In contrast to the other examples which I have provided thus far, creeping is not a privacy enhancing activity, rather it is one which violates privacy. However, in the context of Facebook's discourse of radical transparent sociality as a facilitator of empathy and the betterment of society more broadly, creeping -- especially when it occurs between individuals who dislike each other -- can be seen as a way of using Facebook that is counter to the ideals of its creators. In this way, users are reworking Facebook for their own purposes.

Conclusion

In the previous chapter, I demonstrated that Facebook Inc.'s project of radically transparent sociality is not only embedded in its site architecture but also informs the company's policies and deployment strategies. In this chapter, I described -- using examples from my fieldwork -- what occurs at the intersection of Facebook's radically transparent sociality and the lived, everyday realities of users. I showed how Facebook Friendship collapses privacy choices with social choices, thereby challenging the management of both. I demonstrated how other features -- such as livestreaming and phototagging -- challenge the ability of users to manage their identity on Facebook, particularly around what is known and disclosed about them. Finally, I outlined how context collapse creates situations whereby users have information appropriate to one context shared in another inappropriate context. Taken together, the examples in this chapter show how Facebook's radically transparent sociality makes it challenging for users to manage what, when and how disclosures are made about them, as well as who is making those disclosures. Overall, Facebook creates unfamiliar and uncomfortable social privacy threats which tend to take precedence over the vague institutional privacy threats posed by Facebook. At the same time, since users derive a variety of benefits from using Facebook -- as I will examine more in the next chapter -- users engage in resistive practices to help optimise social benefits as well as their privacy.

Taken broadly, the evidence that I have presented in this chapter calls for a rethinking how individuals might understand and enact privacy, especially in the context of a world where the technologies drive individuals towards openness rather than closure. When applied in the context of the privacy paradox, the evidence in this chapter shows the young people in my study did care about privacy. The use of Facebook is not necessarily a choice free of coercion, nor are the reasons for sharing information on the site simply about self-obsession or exhibitionism. Thus, arguments that youth do not care about privacy are simplistic and obfuscate larger discursive issues. This is examined more fully in the next chapter.

Chapter Eight: Rethinking Privacy in the Age of Facebook

In this thesis, I have examined privacy on Facebook from a layered perspective which connects the history, discourse and architecture of Facebook with its everyday use. I began with a survey of the history and scholarship of both privacy and social network sites. From there, I examined, through an historical overview of technology culture in the Californian Bay Area, the discursive underpinning of Facebook, particularly with respect to privacy. This historically rooted context provided a lens with which to make sense of Facebook's privacy architecture, policies and corporate culture. Using this lens, I outlined how the discourse of Facebook Inc. has informed its privacy architecture and policies. In Chapter 7, I drew on Fiske's model of popular culture to show how 20-something users take up and negotiate Facebook in their everyday lives. I illustrated some of the privacy challenges and consequences for users when one of their primary communication tools furthers Facebook Inc.'s project of radically transparent sociality.

In Chapter 1, I outlined the dominant frames which have informed much of the research on privacy and SNS. Historically, early users of Facebook and MySpace have been youth (boyd & Hargittai, 2010; Raynes-Goldie, 2011). Accordingly, most of the research thus far has implicitly or explicitly focused on youth. Thus, an important launching point for this thesis was the privacy paradox, a common narrative within the early research on youth, SNS and privacy. The paradox has two related strands of thought. The first strand suggests that while young people claim they are concerned about their privacy, their behaviours on SNS, particularly with respect to privacy settings, suggest otherwise (Barnes, 2006; Utz & Krämer, 2009). The second strand suggests that young people are unaware or unconcerned about their privacy, thereby leading them to make what appear to be irresponsible privacy choices (Albrecht-slund, 2008; Barnes, 2006; Utz & Krämer, 2009). This second strand of thought is sometimes used as an explanation for the first. However, instead of accepting this

conclusion, I saw this paradox as a call for a deeper investigation. Are "risky" privacy behaviours, such as sharing too much information with the wrong people, always a result of lack of privacy awareness or concern? What other factors might lead to a discrepancy between user concerns and user behaviours?

In Chapter 2, I provided a chronological overview of the changes and key moments in the technological development of, and academic research on, internet technologies. I paid particular focus on the elements necessary for the development of Facebook: the increasing overlap of online and offline relationships and identities, combined with the general domestication of the internet. As I showed in Chapter 6, Facebook both required and leveraged these shifts to achieve its radically transparent goals, the development of which I covered in Chapter 5. As I illustrated with examples from my fieldwork in Chapter 7, Facebook Inc.'s radically transparent sociality challenges the social privacy of users -- that is, the management of identity and other disclosures. As I demonstrated, far from being unaware or unconcerned, study participants negotiated and balanced disclosure with privacy as best they could within the constraints of the site.

In Chapter 3, I presented a literature review of the essential research on SNS and privacy. As I showed, for a variety of reasons, the vast majority of work has been done on young users -- that is, users under the age of 30. Accordingly, a literature review of SNS and privacy reflects a focus on youth and the privacy paradox. I concluded my literature review with more recent research which examines a variety of reasons as to why the privacy paradox was problematic (Albrechtslund, 2008; Lampe et al., 2008; Livingstone, 2008; Tufekci, 2008). Notably, a significant portion of the evidence in support of a reconsideration of the privacy paradox relied on the modification of privacy settings as a metric. For example, in 2009, Utz and Krämer, revisited the privacy paradox and found that younger users were now more diligent about who they shared with, and accordingly, made their privacy settings more restrictive. Lampe et. al (2008) also noted that use of privacy controls have increased significantly from 2006 to 2008, while danah boyd and Eszter Hargittai (2010) reported a similar increase between 2009 and 2010. Overall, in the same way that Utz and

Krämer propose, these findings should be seen as "snapshots" in an ever changing privacy landscape as SNS continue to rapidly evolve.

In this chapter, I bring together the various layers examined in this thesis -- the history, discourse, architecture and consequences of Facebook -- to examine how radically transparent sociality might help to explain the observations that created the notion of the privacy paradox, thereby helping to contextualise these historical snapshots. In the first part of this chapter, building on the information presented thus far, I further analyse how a number of factors -- largely out of the hands of users -- challenge meaningful privacy choices on Facebook. In the second part of this chapter, I deepen my discussion of social privacy both as a concept and as a privacy management strategy, concluding with the implications for understandings of privacy in the age of Facebook. Overall, as Nissenbaum (2010) demonstrates in her extensive literature review, paradoxical privacy behaviour on SNS is not only observed in youth, but in adults as well. Accordingly, the approach of her examination of such behaviour is not specific to youth. Thus, in line with Nissenbaum's approach, I conclude that these factors are important for understanding privacy choices on Facebook for users of all ages.

Limiting Factors

As I discussed in the introduction, the modification of one's privacy settings is commonly used as a metric to evaluate levels of privacy concern and behaviour (e.g. boyd & Hargittai, 2010; Lenhart, 2009; Utz & Krämer, 2009). The implication of this metric is that privacy settings are the principle mode of privacy management on SNS. The other, less commonly examined approach is opting out all together (e.g. Bigge, 2006; Grimmelmann, 2009). While these two factors may indicate privacy concern, they do not necessarily ensure the protection of a user's privacy. There are two main reasons for this potential disconnect in privacy behaviours and outcomes, as described in the privacy paradox. The first of which is Facebook's confusing privacy settings and policies. The second is the social benefits of participation on Facebook.

Privacy Settings and Policies

In Chapter 4, I outlined the drawbacks of Facebook's privacy settings and policies. In Chapter 7, I showed the social privacy challenges created by Facebook's radically transparent architecture. While Facebook's formal privacy settings may allow users some degree of control over the disclosure of their personal information, these settings do not protect users from larger social privacy threats created by the clash between radically transparent sociality and everyday life. These threats include context collapse, creeping and the loss of identity control. Since these threats arise from the fundamental design of Facebook, there is no way for users to resolve these conflicts within Facebook's privacy settings. Indeed, as I have shown, Facebook's project of radically transparent sociality means the company has no interest in resolving these social privacy threats -- rather their project is the very root of these threats. Accordingly, Facebook's privacy settings can be described as relatively weak.

In addition to being relatively weak, Facebook's privacy settings are further drained of functional power through Facebook Inc.'s continual iteration of its privacy designs and policies whereby the boundaries of what Facebook defines as public or private are in constant flux. Information a user thinks is protected one day can become exposed without their knowledge the next. For example, in 2009, Facebook Inc. changed gender, profile photo, name, geographic region, networks, and list of Friends to be recategorised as "publicly available to everyone" (Opsahl, 2010). In removing some privacy settings all together in the course of this recategorisation, Facebook also removed the ability for users to make that information private again. Even though Zuckerberg has told users that Facebook Inc. has created "extensive privacy settings" which give users "even more control over who you share your information with" (Zuckerberg, 2006), his company's actions tell a different story. While users have a modest degree of control over enabled by their privacy settings, ultimately, Facebook Inc. can and will override those settings to suit its goals of radically transparent sociality.

As I touched on in Chapter 4, the changing nature of the site was a problem for the Canadian Privacy Commissioner's investigation of Facebook. Accordingly, it is likely also a problem for the average user. In fact, it was a problem I saw repeatedly with

Toronto study participants. All participants were unclear as to how Facebook's privacy controls actually worked; what functions were available and who could see what under which circumstance. This observation has been supported by other researchers. In her ethnographic work with American teens, boyd found the same result: "Over and over again, I interview teens (and adults) who think that they've set their privacy settings to do one thing and are shocked (and sometimes horrified) to learn that their privacy settings do something else" (boyd, 2008d).

Further complicating these limited and somewhat misleading privacy choices is the lack of feedback provided by Facebook's architecture regarding the potential consequences of those decisions. Practically, this means that users alter privacy settings on one page, while engaging in social interaction on another. In so doing, it becomes difficult for users to visualise how the configuration of their privacy settings will actually play out, thereby separating privacy choices from privacy consequences.

While users can make largely binary choices about their social privacy, in terms of what information they wish to share and with whom they wish to share it with, they are given no control over their institutional privacy in their use of Facebook. For example, as previously noted, there is no way to stop one's personal information from being collected by Facebook Inc. Indeed, the very functioning of ICT (information communication technologies) involves the input and storage of information into a computer system. In this way, Facebook users cannot control what information is being collected about them; how it is being stored; if or how it is being aggregated and what other companies or institutions may be given access to it. Taken together, Facebook's privacy settings may provide users a false sense of security, thereby obfuscating potentially larger social privacy threats such context collapse, creeping, loss of identity control as well as institutional threats such as data mining and surveillance.

Facebook's Terms of Service (ToS) and privacy policies are another area of concern. As I showed in Chapter 4, Facebook's ToS is long, confusing and written in a legal language that is hard for the average user to understand. Consequently, even if users hit the "agree" button, they are not always aware what they are agreeing to when they

join Facebook or use the site to share personal information. For example, as I showed in Chapter 4, it is a surprise to most users that their user photos can be used in Facebook advertising. While legally users have given their consent, the application of Nissenbaum's contextual integrity here shows why the repurposing of photos in this matter is a privacy violation. Users upload photos of themselves for the purposes of identity articulation and social interaction, not for advertising. Thus, the contextual expectations of users has been violated. Within these factors in mind, it is unreasonable to entirely blame users for a lack of awareness about the privacy implications of Facebook use. As, CIPPIC has argued, Facebook Inc. does not obtain meaningful consent.

Overall, Facebook Inc. does not facilitate or enable meaningful privacy choices or consent. Given the false sense of security provided by Facebook's privacy settings combined with the site's confusing and ever-changing nature, it is possible -- and even understandable -- that even users who privacy concerned might inadvertently or accidentally disclose personal information.

Social Costs and Benefits

People want to be on Facebook. As I showed in Chapter 6, there were significant social benefits for college and university students who were the early users of Facebook. However, the mass adoption of Facebook beyond these communities has also made the site a social necessity for many. In line with the model of network effects, Facebook becomes exponentially more useful as its number of users increases. Indeed, the Canadian Privacy Commissioner's 2009 report on Facebook described social network sites as a "cultural phenomenon" whose popularity had "exploded" around the world (Denham, 2009). Even in 2005 -- three years before my study -- Acquisti and Gross' Facebook study reported that social network sites had "moved from niche phenomenon to mass adoption" (Gross & Acquisti, 2005).

In this context, having a Facebook account becomes all the more essential for getting and staying in touch with one's friends, acquaintances and co-workers. There are social benefits for those on Facebook, such as being easier to reach or being included in

social gatherings. For example, in one of the first conversations that I had with study participant James regarding Facebook, he told me how one of his friends was upset because he had deactivated his account. James' friend did not appreciate that when organizing events (which she always did through Facebook), she had to make an extra effort to individually email James an invitation. She also told him she liked Facebook because she found that the people she knew changed their e-mail addresses and mobile numbers frequently enough that it became difficult to keep track of. However, she observed, people tended to keep their Facebook profiles updated with their real contact information. Further, any invites or messages sent through Facebook would be automatically relayed from the a user's most up-to-date e-mail inbox. As this example suggests, the sheer number of individuals on Facebook who use it as their primary communication tool make it logistically beneficial to one's social life to participate.

Conversely, just as there are social benefits to being on Facebook, as James' example touches on, there are can also be significant social costs involved in Facebook refusal. As Facebook's user base exceeds 750 million (Carney, 2011), the ensuing network effects mean that a refusal of Facebook is also a refusal of the norms of social behaviour in one's group. In James' case, this might mean the accidental exclusion from social events. More broadly, Facebook refusal can result in a degree of social isolation. The inability to participate in the daily discussions and gossip carried out by one's social group through Facebook makes it difficult to keep up one with one's peers. Chris Hughes, one of Facebook's co-founders, told John Cassidy, a reporter for the New Yorker: "If you don't have a Facebook profile, you don't have an online identity... It doesn't mean that you are antisocial, or you are a bad person, but where are the traces of your existence in this college community? You don't exist online, at least. That's why we get so many people to join up. You need to be on it" (Cassidy, 2006, p. 6). For Ryan Bigge (2006), Hughes' comments reflect a "narrative of inevitability" that describe "a false choice, a sociotechnical scenario devoid of agency." Thus, according to Hughes, the costs of non-participation are so high that it is not a matter of *if* you will join Facebook, but *when*. In this line of reasoning, the use of Facebook is no longer even a choice -- it is a social necessity.

Perhaps even more concerning is that individuals who are non-users of Facebook -- either due to a lack of interest or because of privacy concerns -- can face increased privacy risks by way of friends and acquaintances. Facebook's design allows users to tag non-users in photos. At the time of my fieldwork, users were also asked to provide the non-user's email address (Denham, 2009). The non-user would then receive an email inviting them to join Facebook in order to see the photo they had been tagged in. In so doing, Facebook -- without obtaining the non-users consent -- gathers an individual's name, photo and email address. Further, unless the non-user actually joins Facebook, they are unable to remove the photo tag. This feature not only violates the social privacy of non-users by allowing them to be tagged in potentially incriminating or embarrassing photos, it also violates the institutional privacy by exposing their information to Facebook Inc. This feature, combined with the potential social cost of opting out, Facebook not only limits the privacy choices available to users once they join the site, it limits the social *and* privacy choices of non-users.

Network effects combined with a user's desire for social inclusion constrain the amount of choice a user has about participating or not participating on Facebook. Once on the site, Facebook's privacy settings functionally limit what users can and cannot control about what they disclose. In some cases, Facebook Inc. has even rendered null the privacy choices of users as it iterates the architecture of its privacy settings. Thus, even though the careful management of one's privacy settings or opting out entirely are presented as effective privacy management tools, the factors outlined in this section reveal their limitations. In the context of the privacy paradox, these limitations provide another reason -- beyond lack of awareness or concern -- where users may have permissive privacy settings or appear to expose too much of their personal information. Facebook Inc.'s goal of radically transparent sociality has resulted in the creation of numerous social and institutional privacy challenges for users of Facebook. As I have shown in this section, users may disclose information either by mistake or in exchange for social benefits. Thus, disclosures are not always voluntary or freely made. Taking into account these factors, it is not a paradox for a user to, on the one hand, express privacy concerns but then, on the other, not be able to carry them out. Thus, in the same way that the privacy paradox describes a seem-

ing disconnect between privacy attitudes and behaviours, there can exist a disconnect between privacy intentions and outcomes. As I have shown in this section, it is a disconnect which, unlike the privacy paradox, is not always caused by ignorance or unawareness on the part of the user.

Social Privacy

As discussed in Chapter 3, privacy can have a varied set of meanings which can depend on social, cultural and developmental factors. As with legal or regulatory definitions of privacy, the privacy paradox relies on a conception of privacy which does not take into account social privacy. Historically, governmental or arms-length privacy regulators have been focused on privacy in terms of data protection, or institutional privacy, which itself relies on the classical conception of privacy a total withdrawal, or "the right to be left alone" (Warren & Brandeis, 1890). Zynep Tufekci (2008) has argued that the application of this conception of privacy to the use of SNS has led to many of the misunderstandings of youth behaviours.

Within this definition of privacy, it might seem logical to conclude that individuals with permissive privacy settings or who reveal "too much" online are either unconcerned about their privacy or unaware of the potential risks of their activities. In this section, building on evidence from my fieldwork in the previous chapter, I provide another metric beyond the adjustment of privacy settings with which to understand and evaluate privacy behaviours: that is, concern and activity around social privacy. I begin by examining showing how social privacy behaviours and activities do indicate privacy concern, as well as how they -- combined with other factors relating to Facebook -- might obfuscate or diminish institutional privacy concerns. Second, building on Chapter 7, I present the management of social privacy in terms of the optimisation of disclosure and the implications for evaluations of privacy concerns.

Even though elements of social privacy are identified in the literature, there is no clear distinction between social and institutional privacy. Palen and Dourish provide some insight as to why this might be the case:

Privacy regulation is complicated, and has a range of functions, from maintaining comfortable personal spaces to protecting personal data from surreptitious capture. Both social and design studies of technology often unknowingly conflate these functions, and consequently fail to provide satisfying analytical treatment (Palen & Dourish, 2003).

Further, since definitions of privacy -- particularly legal definitions -- tend to be conflated institutional privacy, social privacy can get overlooked. Despite this lack of distinction and deeper examination, social privacy threats resulting from SNS are becoming more common as more users begin to use them. Accordingly, the findings of my research suggest that users are more concerned with the immediate threats of social privacy, even though they do not use that term to describe their concerns. My findings were also supported by a Norwegian study which extended and tested my model of social privacy (Brandtzæg et al., 2010, p. 1025).

Given the focus on institutional privacy, users concerned with social privacy but not institutional privacy may appear to be privacy unconcerned. Overall, social privacy threats obfuscate institutional privacy concerns for users, while a traditional institutional privacy focus obfuscates the concern users have for social privacy. Thus it is critical that both types of concerns are taken into account, especially as SNS use becomes widespread. Indeed, as Brandtzæg et al. (2010) found in their research mentioned above: "a striking finding is that with the introduction of different social groups, the younger and older generations have introduced social privacy as an important user need" (p. 1018). In this section I first analyse the conflict between social and institutional privacy, both as concepts and as categories of concern, and how this conflict can shed light on the privacy paradox. I then describe how, in this privacy landscape, privacy management becomes about the optimisation of disclosure rather than the classical conception of privacy as withdrawal.

Social Versus Institutional privacy

In Chapter 7, I showed how Facebook's radically transparent sociality created unfamiliar and frustrating privacy situations for participants. I identified these as threats to social privacy, as distinct from institutional privacy. These social privacy threats -- context collapse, creeping and loss of identity control -- can be seen as the result of Facebook Inc.'s attempted imposition of its technologically utopian values on the everyday social lives of its users. Since technology alone cannot change social, cultural or economic factors, Facebook alone cannot make the world radically transparent. The result of is a collision between Facebook's utopian privacy goals with existing social, cultural and economic norms. Instead of encouraging empathy or understanding as Zuckerberg believes Facebook would, participants experienced social privacy consequences in the form of social embarrassment, at best or the potential loss of employment, at worst. As Nissenbaum (2010) has argued, privacy violations in the age of social media are caused by a "schism between experience and expectation" thereby resulting "radical change in the flows of personal information" (p. 231).

Drawing on evidence from my fieldwork, I demonstrated the importance and everyday immediacy of these social privacy concerns for study participants. Social privacy threats occupied the attention of participants at the expense of other types of privacy concerns. While they generally did not use the word "privacy" to describe their concerns, all study participants did -- to varying degrees -- have issues with various aspects of social privacy while using Facebook. Further, in line with Fiske's notion of popular culture, I found that participants engaged in practices which, within the constraints of the site, somewhat reworked Facebook to better suit their own purposes -- either to mitigate their privacy concerns or to violate the privacy of others. For example, some participants would periodically delete wall posts or use pseudonyms, while others would exploit the privacy defaults of geographic networks to creep people they did not like. Additionally, in discussions about their use of Facebook, study participants would frequently tell stories about frustrating or difficult social privacy situations that arose from their use of Facebook, such as not knowing what to do when they were being Friendened by someone they did not trust.

Taken together, these concerns and activities suggested that study participants are not only concerned about privacy, they are actively mitigating these concerns as best they can within the constraints of Facebook. As Facebook's privacy settings are relatively weak, the subversive strategies deployed by users to protect their privacy -- such as using an alias or periodically deleting content -- suggest a level of privacy literacy well beyond that required to simply adjust one's privacy settings. These activities also indicate that social privacy awareness and protection can be used as a more accurate, or at least a more nuanced metric for privacy evaluation on Facebook.

Conversely, even though participants were very much concerned, aware and proactive about managing their social privacy, the same level of rigour was not observed with respect to their institutional privacy. Facebook's project of radically transparent sociality provides some explanation as to why participants had such a one-sided privacy focus. In encouraging users to abide by radically transparent sociality in a society whose cultural norms and social structures still rely on some measure of privacy, Facebook -- inadvertently or otherwise -- creates confusing, unfamiliar and frustrating social and privacy situations for users that became the main preoccupation of users and the focus of their attention. For example, Facebook Friendship conflates social choices with privacy choices, thereby forcing users to choose between saving face or saving privacy -- a particularly challenging situation for users when power dynamics are involved. It is these immediate and tangible consequences of social privacy threats that tends to overwhelm institutional privacy concerns.

Moreover, Facebook's radically transparent architecture facilitates this focus on social privacy at the expense of institutional privacy. As noted earlier in this chapter, Facebook's privacy settings are all social privacy settings -- that is, controlling one's information relative to Friends. These controls give users a somewhat false sense of privacy, which distract from Facebook Inc.'s potentially harmful activities. For example, in many conversations I had throughout my fieldwork, individuals would tell me their privacy was not at risk because they did "not share very much on Facebook." What they did not realise was that Facebook Inc. is silently tracking a wide variety of user activity, such as which profiles a user views the most (Douglas, 2007; Stanford University, 2005). The immediate and tangible nature of social privacy threats posed

by one's Friends combined with privacy settings which are entirely designed around social privacy management make it easier to ignore or be entirely unaware of how Facebook Inc. might be violating one's institutional privacy in the personal information it gathers. As Jason Nolan, director of the Experiential Design and Gaming Environments Lab in Toronto, remarked to me in a discussion about my research for this thesis: "We are too busy watching each other to notice we are being watched." Overall, as a concept, social privacy can help to explain why users may appear unconcerned or unaware with respect to privacy, when the reality is far more nuanced.

Social Privacy Management

Writing for the New York Times, journalist Clive Thompson (2008) observed:

Young people today are already developing an attitude toward their privacy that is simultaneously vigilant and laissez-faire. They curate their online personas as carefully as possible, knowing that everyone is watching -- but they have also learned to shrug and accept the limits of what they can control.

Thompson points to the fundamental privacy challenge for SNS users where, in the same way described by Fiske's notion of "making do" with the materials of popular culture, users must attempt to balance the benefits of disclosure with the benefits of privacy, all within the constraints of Facebook's limited architecture. It is a challenge which has been described by Brandtzæg et al. (2010, p. 1007) as the privacy dilemma. In their words: "...if privacy is protected, then sociability and content sharing will be compromised, whereas if sociability and content sharing are promoted, then privacy will suffer." It is this dilemma which Zuckerberg has intentionally leveraged in order to encourage more sharing on his site -- he gave users the minimum amount of privacy required to share the maximum amount of information, as described in Chapter 6.

Accordingly, in this privacy landscape, the management of privacy -- in particular social privacy -- becomes about the optimisation of disclosure. This type of privacy

management acknowledges that there can be social and economic benefits to disclosure or publicity. These benefits might arise from a well-maintained public persona which can enable individuals to build stronger social ties or secure new employment. Accordingly, participants did not aim for privacy as total withdrawal in the classic sense. Rather, they sought the optimization of privacy versus disclosure.

For example, Penny told me about how her younger sister meticulously monitored the photos that were taken of her, and then, which of them were shared on Facebook. She also closely watched what photos she was tagged in, untagging any that were unflattering. She would even preemptively warn Penny not to post "ugly" photos of her. In another interview, I took some photos of Lee which he liked because they conveyed the image of himself he wished to portray. He later asked me to email him the photos so that he could use one as his Facebook profile photo. In both cases, participants wanted to be seen on Facebook and were careful to manage -- within the constraints of the site -- the image they presented.

Other researchers report similar results with respect to privacy management on social media. Tufekci's 2008 study notes that youth see a benefit to sharing and having public identities, whereby privacy becomes a "process of optimisation between disclosure and withdrawal" (Tufekci, 2008, p. 20). This process of optimisation has also been described by Marwick (2010) as micro-celebrity, while Kelly Ladd (2009, p. 9), who wrote her Master's degree on identity and SNS, uses the term "self-curation" or "the gathering together of signs that represent an individual's identity that are then publicly exhibited." Jaron Lanier (2010), who has criticised Facebook Inc. and the system of beliefs behind it, notes this trend in describing the activities of "successful" users of Facebook:

They tend to their doppelgangers fastidiously. They must manage off-hand remarks and track candid shapshots at parties as carefully as a politician. Insincerity is rewarded, while sincerity creates a lifelong taint (p. 71).

Fundamentally, then, social privacy management and the optimisation of disclosure is about contextual integrity -- that is, the management of the appropriate flow of personal information within one's various life contexts. In deploying Nissenbaum's contextual integrity heuristic -- a concept which has informed my understanding of privacy throughout this thesis -- the privacy paradox is no longer a paradox. In the conclusion to her *Privacy in Context*, Nissenbaum (2010) uses her model to explain why paradoxical behaviour is in fact not paradoxical:

In the case of social networking sites, what others have seen as evidence that people (particularly "today's youth") do not care about privacy, or are simply illogical in their expectations, is altered by the [contextual integrity] heuristic, which reveals that if researchers and commentators would only acknowledge and pay attention to the complex norms that govern the flow of information in the social, professional, ethnic, age-cohort contexts in which social network sites are embedded, they would discover that participants are anything but illogical (there are exceptions, of course) and anything but indifferent to privacy (exceptions to this, too) (Nissenbaum, 2010, p. 227).

Instead of understanding privacy as the expectation that information will be disclosed to the appropriate parties in the appropriate contexts -- as Nissenbaum's contextual integrity supposes -- the privacy paradox assumes an expectation of privacy as total withdrawal. As Nissenbaum argues, the application of her heuristic revolves the privacy paradox.

As I have shown in this section, the privacy paradox model does not take into account that there are benefits to disclosure, such as relationship and reputation building. Indeed, it is these factors which make SNS appealing to youth in the first place. As Leslie Regan Shade notes, youth employ social media to engage in identity play, self-validation and social interaction (Shade, 2008). In the context of privacy as withdrawal, any disclosure on the part of a user can be characterised as a poor or risky privacy decision. A Facebook user, then, can engage in social privacy management and still appear unconcerned or unaware according to these privacy metrics. Thus,

privacy research may mistakenly confuse disclosure with lack of awareness or privacy concern.

Conclusion

Upon first glance, it may appear that privacy behaviours on Facebook are comprised entirely of the choices freely made by users. In this chapter, I have shown that this is not actually the case. Through the site's architecture of radically transparent sociality combined with its broader social influence and network effects, Facebook Inc. shapes and limits which choices can or cannot be made about privacy. At the same time, in the manner similar to Fiske's popular culture whereby individuals rework hegemonic cultural products to suit their own needs, Facebook users negotiate and push the site's privacy constraints as far as they can in order to "make do" with the choices available (Fiske, 1989, p. 4). Thus, privacy choices and behaviours are determined by an uneven interplay between the users *and* designers of Facebook.

In this chapter, I showed how Facebook, through its relatively weak and ever changing privacy settings combined with the high cost of non-participation, limits meaningful privacy choices for users. In this context, users may have privacy concerns about Facebook, but still participate out of social necessity -- participation which requires the sharing of personal information. Indeed, the less information a user shares, the less social benefit they derive from Facebook. Once on the site, Facebook's ever dynamic privacy controls do not always ensure against unwanted exposure of their personal information.

I also demonstrated why, as a result of the unfamiliar and frustrating situations created by the collision of radically transparent sociality with conventional privacy norms, participants tended to focus on social privacy issues over institutional ones. Moreover, in a system where information sharing is economically and socially rewarding, users do not see the benefit in privacy as total withdrawal. Rather, they seek to optimise privacy with disclosure as best they can within the limits of Facebook's radically transparent system. Within that optimisation participants engaged in subversive practices. Rather than trusting or relying on Facebook, participants took privacy into

their own hands, thereby suggesting a sophisticated level of privacy awareness. For example, considering Facebook Inc.'s privacy track record, the use of a pseudonym is actually a far more effective means of managing one's privacy. Facebook can override settings or expose information, but if that information is provided under an alias, privacy consequences can be far less dire. As Thompson (2008) suggests, users are take a simultaneously "vigilant and laissez-faire" approach to their privacy. For the reasons described in this chapter, such a strategy is not paradoxical, but entirely reasonable.

This analysis shows that not only were participants aware of some of the ways in which their privacy was being threatened, they were active in managing and mitigating these threats as best they could. Moreover, this analysis provides potential insights into why studies based on the definition of privacy as withdrawal might have concluded that youth were irresponsible or unaware of privacy threats. Taken together, the concept of social privacy and the optimisation of disclosure represent important metrics for the evaluation of privacy concerns on SNS.

In sum, this chapter addresses how the privacy paradox is likely not actually a paradox. The privacy challenges which I described in this chapter arise as a result of Facebook Inc.'s project of radically transparent sociality. In other words, these threats are created by users reacting to Facebook's architecture. I outlined a number of reasons why, as a result of Facebook's confusing and ever changing settings, users can still be concerned about privacy but still have permissive privacy settings. I also demonstrated how the sharing of personal information on SNS has social benefits, and thus cannot automatically be equated with a lack of knowledge or concern about privacy. Since disclosures can result by mistake or through a degree of social coercion, it can be said that a perceived incongruence between attitudes and behaviours -- as described by the privacy paradox -- is produced out of an architecture that creates significant constraints on the capacity of users to protect their privacy and still enjoy the social benefits of Facebook. If any one group can be described as uniformly unconcerned about privacy, it is not youth. It is those at Facebook Inc. As more adults

pick up Facebook as part of their everyday social lives, they too will be faced with the same architecturally-created challenges.

Conclusion

Our revolution will not be in gathering data -- don't look for TV cameras in your bedroom -- but in analyzing the information that is already willingly shared (Hunter, 1995, p. 294).

This thesis marks a systematic opening up and peeling back of Facebook's various layers. At the heart of these layers is Facebook Inc.'s radically transparent sociality, a discourse fundamental to any comprehensive understanding of Facebook, whether from the perspective of privacy, identity or sociality. This discourse has a number of implications which extend beyond the issue of privacy into the broader society and culture at large.

The first of these implications concerns methodological approaches in internet studies and related disciplines. In this thesis, I have used a recontextualised ethnographic approach that, unlike most studies thus far, examines both users of social media as well as the companies which create them. The revelation of this discourse of Facebook, by virtue of the approach taken in this thesis, demonstrates the critical importance of methodologies which examine both the users of social media as well as the companies behind them. Overall, an understanding of privacy behaviours and attitudes was greatly enhanced and fleshed out by the identification of Facebook's radically transparent sociality.

Beyond academic research, the second implication is the broader social consequences of radically transparent sociality. As I have shown, radically transparent sociality is inherently technologically deterministic. As such, it assumes that the world can be made better simply by a change in technology. In this mode of thought, Facebook Inc. believes that it can bring empathy, equality and understanding to the world simply through its imposition of radically transparent sociality on culture and society. However, in reality, it is a discourse which denies -- or presumes to negate, simply by virtue of its imposition on society -- the consequences for users of well established social, cultural or economic norms, biases and hierarchies of power. Despite what

those at Facebook Inc. might believe, Facebook cannot make the world better simply because everyone uses it. As shown in Chapter 7 and 8, the intersection of Facebook as a technology with the social, cultural and economic factors does not result in utopia. Instead, it results in negative social situations; problematic relationships; unwanted social surveillance and negative judgements. Worse still, Facebook's privacy architecture can result in very real threats to the physical safety and financial stability of users. Or stated differently, Facebook's radically transparent sociality denies is that the consequences of transparency are highly contextually dependent.

For example, for some individuals such as Mark Zuckerberg himself, abiding by radically transparent sociality has very little risk. As technologist Anil Dash observed in an interview with the New York Times:

If you are twenty-six years old, you've been a golden child, you've been wealthy all your life, you've been privileged all your life, you've been successful your whole life, of course you don't think anybody would ever have anything to hide... (Vargas, 2010, p. 8)

While Zuckerberg may think radically transparent sociality just as well for everyone else as it as for him, this is not the case. The norms and hierarchies in which we all live intersect with technology to impact individuals in ways. In contrast, radically transparent sociality assumes that everyone is equal and similarly-minded. While this seemingly egalitarian approach may appear beneficial, it does not allowed for the unintended consequences of existing biases and hierarchies. As a result, some individuals can actually be put at personal or economic risk by unexpected disclosure of their personal information.

These risks are clear in the numerous examples of individuals being passed over for new employment or let go from existing positions as a result of unwanted or unexpected disclosures on Facebook. Less well known are the risks attached to the disclosure of one's sexual orientation. For example, a gay man living in certain areas of the world -- such as Uganda or parts of the United States, where it is not safe to be openly gay -- would, if forced to abide by radically transparent sociality, face a high

risk of bodily harm. This risk is not hypothetical. Jernigan and Mistree (2009) found that it was not difficult to accurately determine a Facebook user's sexual orientation simply by looking at that user's list of Friends. LGBTQ users, for example, tend to have more LGBTQ friends. Consequently, users may be unwillingly revealing their sexual orientation. Since Facebook has removed the ability of users to hide their list of Friends, queer Facebook users who are concerned about their safety are faced with a tough choice: delete their accounts and risk social isolation, or stay on Facebook and risk physical harm and/or job loss. Similarly, women can also face a greater safety risk as a result of unwanted or unexpected disclosures arising from the use of a site informed by radically transparent sociality (e.g. Jacobs, 2010). Thus, when a radically transparent social technology such as Facebook enrolls individuals from all walks of life, the result can be very immediate and tangible threats to the safety of members of that society.

What is especially disconcerting is that -- based on my extensive review of the literature; combined with discussions with journalists; academics, policy makers and Facebook users -- most individuals are unaware of Facebook Inc.'s goal of radically transparent sociality. As such, they may share information on the site assuming Facebook Inc. would have no interest in disclosing it. The true consequence of radically transparent sociality then, is an involuntary reduction in the privacy of millions of users, which can literally put them in harm's way. It is not the empathetic and caring utopia that Zuckerberg seems to imagine.

Even more broadly, the third implication of my findings concerns the future of radically transparent sociality and Western society. Facebook and other radically transparent social systems become increasingly common among adults, so too do the risks they face. In a sense then, the privacy threats and challenges faced by youth as outlined in this thesis can be seen as an early indication of what might be soon faced by users of all ages in the developed world.

Indeed, as I showed in Chapter 6, Facebook Inc.'s slow but strategic move from a niche student-only SNS to a site open to anyone with an email address can be viewed as both reflective and anticipatory of this mass adoption of SNS across the demo-

graphic spectrum. As Zuckerberg has stated, he wants to make the world more open and transparent for *everyone*. In Chapter 5, I showed that the discourse of Facebook did not emerge in isolation. Rather, it came out of the historically rooted culture of the Californian Bay Area. It is perhaps unsurprising, then, that Zuckerberg is not the only influential Silicon Valley technologist imagining such a radically transparent future. Kevin Kelly (2007), whose ideas I introduced in Chapter 5, has spoken about a similar future in his prediction for the web over the next ten to fifteen years.

There's like a billion social sites on the web. Each time you go into there, you have to tell it again who you are and [who] all your friends are. Why should you be doing that? You should just do that once, and it should know who all your friends are. So that's what you want, all your friends are identified, and you should just carry these relationships around. All this data about you should just be conveyed, and you should do it once and that's all that should happen. And you should have all the networks of all the relationships between those pieces of data. That's what we're moving into - where [the internet] sort of knows these things down to that level... *what it's doing is sharing data, so you have to be open to having your data shared, which is a much bigger step than just sharing your webpage or your computer* [italics mine]. And all of these things that are going to be on this are not just pages, they are things. Everything we've described, every artifact or place, will be a specific representation, will have a specific character that can be linked to directly... [the internet of things where a] physical thing becomes part of the web so that we are in the middle of this thing that's completely linked, down to every object in the little sliver of a connection that it has.

If Kelly's prediction seems like a stretch, consider Facebook's Open Graph, which launched only three years later:

Users reading articles on CNN.com, for example, can see which articles their Facebook friends have read, shared, and liked. Eventually,

the company hopes that users will read articles, visit restaurants, and watch movies based on what their Facebook friends have recommended, not, say, based on a page that Google's algorithm sends them to. Zuckerberg imagines Facebook as, eventually, a layer underneath almost every electronic device. You'll turn on your TV, and you'll see that fourteen of your Facebook friends are watching "Entourage," and that your parents taped "60 Minutes" for you. You'll buy a brand-new phone, and you'll just enter your credentials. All your friends -- and perhaps directions to all the places you and they have visited recently -- will be right there. For this plan to work optimally, people have to be willing to give up more and more personal information to Facebook and its partners (Vargas, 2010, p. 7).

While the convenience described here by Zuckerberg and Kelly can be appealing, this thesis has shown that users cannot trust designers who abide by radically transparent sociality to protect their privacy. At the same time, the privacy landscape and culture in the Western world is changing. Intentionally or accidentally, coerced or otherwise, we as a society, have gotten used to less privacy. As Ryan Bigge (2010), one of the first to critically analyse SNS, has argued, openness is becoming the default social norm. Indeed, the very fact that 750 million people are on Facebook means that we are sharing more personal information than we ever have before. By virtue of the architecture of Facebook and social media more broadly, we are also having more information collected about us than ever before.

As dire as all this might sound, it also calls to us to remember that social network sites do not have to be designed in such a way as to inherently threaten the privacy of users. Just as I have shown throughout this thesis, Facebook is not the way it is because of some fundamental nature of SNS technology. Rather, Facebook's radically transparent sociality is a result of the belief system baked into it by its creators.

Indeed, there are a number of examples which exist as counterpoints to Facebook. LiveJournal is an interesting historical example. While I was doing my undergraduate work from 2000 to 2004 in Toronto and Kingston, Ontario, LiveJournal was used

amongst my peers in the same way Facebook is today -- to augment physical interactions and nurture new relationships. I remember going to parties where, just like today, everyone had a LiveJournal account. Today, LiveJournal is no longer used by my peers, but still continues to be an important and vibrant space for a number of subcultural and creative communities.

What is most interesting, though, is contrast between Facebook and LiveJournal's privacy cultures. While they both provide similar services, each site is informed by a very different belief system. Facebook Inc.'s revenue model is advertising. In this model, users are not customers but unpaid digital labourers, creating value that Facebook can then sell to its real customers -- the advertisers. Thus, the user's needs, especially around privacy, come last. In contrast, LiveJournal was essentially created by users, for users (the community). LiveJournal was free to use and sustained by user donations and "freemium" accounts, where users paid a small fee to gain access to better features. Moreover, LiveJournal was based on an open source platform where much of the coding work was done by volunteers. Accordingly, until the site ownership changed in 2005, LiveJournal operated under an architecture and social contract which protected users in a number of ways, for example promising that the site would never sell a user's information or display banner advertising (LiveJournal, ND). As LiveJournal scholar Sarah Ford describes, LiveJournal had a strong privacy culture (Ford, 2010) which contrasts with Facebook's weak privacy culture.

More recently, leveraging the backlash against Facebook Inc.'s questionable privacy practices in 2010, a number of privacy-focused SNS startups emerged. Most notable, perhaps, was Diaspora which launched as a crowd-funded project by a group of American college students. Google also responded with its social privacy-oriented SNS Google+, which uses a feature called Circles that is aimed at helping users avoid the context collapse they experienced on Facebook. While these "Facebook killers" show that there is both the appetite and technical possibility for a privacy-focused SNS, all of these examples failed to gain mass traction.

So, where do we go from here? The difficulty in predicting the future, especially when it comes to technology, is a fact that haunts concluding remarks. ICQ was re-

placed by AIM and MSN Messenger as the IM of choice. Users abandoned Friendster in droves for MySpace, which in turn lost the battle for SNS dominance to Facebook. And yet, email has remained one of the most popular uses of the internet since the 1970s. The question remains: will Facebook eventually be tossed aside by its users as was the case with ICQ or Friendster, or has its unprecedented level of mass adoption firmly entrenched it as a communication platform along with email and text messaging?

As Fiske's model of popular culture suggests, we as individuals have a choice about how we engage with social media. Similarly, as the Social Shaping of Technology model reminds us, technology is only one factor which contributes to human progress. The other factor is us.

We are the ones we've been waiting for.

-- Hopi Elders

Appendix: Participants

The following is a list of participants whose personal information and experiences were mentioned in this thesis. The core group was 10, with 7 more participants beyond that who I either interacted with infrequently, or whose experiences/stories ended up being used to frame my understanding of my findings as a whole.

All names have been changed and some information has been withheld in order to protect the privacy of participants.

Name	Background	Participation
Lee	White male from Sudbury, Ontario, Canada. Mid-20s, sexual orientation undeclared. Heavy Facebook user.	At least one weekly meeting/activity in person, almost daily online.
Ben	Male from PEI, Canada of Scottish decent. Mid-20s, queer and working in technology and education. Early adopter of Facebook.	At least one weekly meeting/activity in person, almost daily online.
Lola	Straight female born in Toronto, parents from Hong Kong. Mid-20s, engineer.	At least one fortnightly meeting/activity in person, almost daily online.
Dan	Queer white male from Early 20s, born in the United States. University student. Early adopter of Facebook.	At least one weekly meeting/activity in person, almost daily online.
Kalvin	Mid-20s, friend of Lee	Multiple social events, 1-3 one-on-one interviews.

James	White, straight male. Early 20s, engineer.	Multiple social events, 1-3 one-on-one interviews.
Pablo	White, queer male. Newspaper editor.	Multiple social events, 1-3 one-on-one interviews.
Elizabeth	White, straight, female. Mid-20s, artist and teaching assistant. Late adopter of Facebook.	Multiple social events, 1-3 one-on-one interviews.
Julie	Mid-20s, friend of Elizabeth.	One interaction.
Penny	Straight female of Indian descent. Mid-20s, educator. Heavy user of Facebook.	At least one weekly meeting/activity in person, almost daily online.

Bibliography

- Acquisti, A., & Gross, R. (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. Proceedings from Privacy Enhancing Technologies Workshop, Cambridge, UK.
- Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, 13(3). Retrieved from <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949>
- Allen, A. L. (2000). Gender and privacy in cyberspace. *Stanford Law Review*, 52(5), 1175-1200. Retrieved from <http://www.jstor.org/stable/1229512>
- Allen, M. (2008). Web 2.0: An argument against convergence. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2139/1946>
- Allen, M. (2009). Tim O'Reilly and Web 2.0: The economics of memetic liberty and control. *Communication, Politics & Culture*, 42(2), 6-23.
- Allen, M. (2011). *What Was Web 2.0? Versions and the Politics of Internet History*. Proceedings from Oxford Internet Institute, Oxford.
- Allen, M. (2011). *Gaining a Past, Losing a Future: Web 2.0 and Internet Historicity*. Proceedings from 7th Australian Media Traditions Conference, Melbourne, Australia.
- Altman, I. (1975). *The Environment and Social Behavior: privacy, personal space, territory, crowding*. Belmont: Wadsworth Publishing Co.
- American Society of Cybernetics. (2000a). Chapter 2: Coalescence. Retrieved April 5, 2011 from <http://www.asc-cybernetics.org/foundations/history2.htm>
- American Society of Cybernetics. (2000b). Summary: The Macy Conferences. Retrieved April 5, 2011 from <http://www.asc-cybernetics.org/foundations/history/MacySummary.htm>
- Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479-497. Retrieved from [http://www.surveillance-and-society.org/articles2\(4\)/lateral.pdf](http://www.surveillance-and-society.org/articles2(4)/lateral.pdf)
- Andrew, A. M. (2008). Digital patient; CYBCOM discussion. *Kybernetes*, 37(2), 212-214. Retrieved from <http://www.emeraldinsight.com/journals.htm?articleid=1713931&show=abstract>
- Arnold, B. (2008). Social Network Services: Busted. Retrieved October 31, 2011 from <http://www.caslon.com.au/socialspacesprofile14.htm>

- Arrington, M. (2006). AOL Proudly Releases Massive Amounts of Private Data. Retrieved 5 December, 2009 from <http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>
- Arrington, M. (2008). Facebook Isn't A Social Network. And Stop Trying to Make New Friends There. Retrieved 5 December, 2009 from <http://www.techcrunch.com/2008/09/15/facebook-isnt-a-social-network-and-dont-try-to-make-new-friends-there/>
- Baloun, K. M. (2007). *Inside Facebook: Life, Work and Visions of Greatness*. Victoria, BC: Trafford.
- Barbrook, R. (2007). *Imaginary Futures: From Thinking Machines to the Global Village*. Ann Arbor: Pluto Press.
- Barbrook, R. (2005). The Hi-Tech Gift Economy. *First Monday, Special Issue #3*. Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1517/1432>
- Barbrook, R., & Cameron, A. (1995). The Californian. Retrieved from http://www.alamut.com/subj/ideologies/pessimism/califIdeo_I.html
- Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved from <https://projects.eff.org/~barlow/Declaration-Final.html>
- Barnes, S. B. (2006). A privacy paradox: Social Networking in the United States. *First Monday, 11*(9). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312>
- Baym, N. K. (1995a). From practice to culture on Usenet. *The cultures of computing*, 29-52.
- Baym, N. K. (2010a). Personal Connections in the Digital Age.
- Baym, N. K. (1995b). The Emergence of Community in Computer-Mediated Communication. In S. G. Jones (Ed.), *Cybersociety: Computer-Mediated Communication and Community*. Thousand Oaks: Sage.
- Baym, N. K. (2010b). *Social Networks 2.0*. West Sussex: Wiley-Blackwell.
- Beaver, D. (2007). Facebook Photos Infrastructure. Retrieved Sept 8, 2008 from <http://blog.new.facebook.com/blog.php?post=2406207130>
- Beckett, C. (2009). 'Digital natives': A Myth? *POLIS*. Retrieved from <http://eprints.lse.ac.uk/35789/1/digitalnatives.pdf>
- Beer, D. D. (2008). Social network (ing) sites... revisiting the story so far: A response to danah boyd & Nicole Ellison. *Journal of Computer-Mediated*

- Communication*, 13(2), 516-529. Retrieved from <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2008.00408.x/pdf>
- Bigge, R. (2006). The cost of (anti-)social networks: Identity, agency and neo-luddites. *First Monday*, 11(12). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1421/133>
- Bigge, R. (2010). Openness is becoming the default social norm. *The Toronto Star*. Retrieved from <http://www.thestar.com/news/insight/article/765130--openness-is-becoming-the-default-social-norm>
- Boneva, B. S., Quinn, A., Kraut, R. E., Kiesler, S., & Shklovski, I. (2006). Teenage communication in the instant messaging era. In *Computers, phones, and the Internet: Domesticating information technology* (pp. 201–218). New York: Oxford University Press. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.7470&rep=rep1&type=pdf>
- Bonfils, M. (2011). Why Facebook is Wiping Out Orkut in India & Brazil. *Search Engine Watch*. Retrieved from <http://searchenginewatch.com/article/2064470/Why-Facebook-is-Wiping-Out-Orkut-in-India-Brazil>
- Bourdieu, P. (1977). *Outline of a theory of practice* (R. Nice, Trans.). Cambridge: Cambridge University Press.
- boyd, d. (2006a). Identity Production in a Networked Culture: Why Youth Heart MySpace. Retrieved from <http://www.danah.org/papers/AAAS2006.html>
- boyd, d. (2007a). Why youth heart social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (pp. 119-142). Cambridge: MIT Press. Retrieved from <http://www.mitpressjournals.org/doi/abs/10.1162/dmal.9780262524834.119>
- boyd, d. (2008a). How Can Qualitative Internet Researchers Define the Boundaries of Their Projects: A Response to Christine Hine. In A. Markham & N. Baym (Eds.), *Internet Inquiry: Conversations About Method* (pp. 26-32). Los Angeles: Sage. Retrieved from <http://www.danah.org/papers/EthnoBoundaries.pdf>
- boyd, d., & Heer, J. (2006, January 4 - 7). *Profiles as conversation: Networked identity performance on Friendster*. Proceedings from Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Kauai, Hawaii.
- boyd, d. (2005). Autistic Social Software. In J. Spolsky (Ed.), *The Best Software Writing I* (pp. 35-45). Apress.
- boyd, d. (2008b). Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. *Convergence: The International Journal into New Media*

- Technologies*, 14(13), 13-20. Retrieved from <http://con.sagepub.com/cgi/content/abstract/14/1/13>
- boyd, d. (2008c). *Taken Out of Context: American Teen Sociality in Networked Publics*. PhD. University of California, Berkeley.
- boyd, d. (2006b). Friends, Friendsters and Top 8: Writing Community into being on social network sites. *First Monday*, 11(12). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336>
- boyd, d. (2007b). My Friends, MySpace: American Youth Socialization on Social Network Sites [video recording].: The Berkman Centre for Internet and Society.
- boyd, d. (2010). Facebook and 'radical transparency' (a rant). Retrieved from <http://www.zephoria.org/thoughts/archives/2010/05/14/facebook-and-radical-transparency-a-rant.html>
- boyd, d. (2008d). Putting Privacy Settings in the Context of Use (In Facebook and elsewhere). Retrieved from http://www.zephoria.org/thoughts/archives/2008/10/22/putting_privacy.html
- boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8). Retrieved from <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>
- boyd, d., & Jenkins, H. (2006). *MySpace and Deleting Online Predators Act (DOPA)*. Proceedings from MIT Tech Talk.
- boyd, d. (2007c). None of this is Real: Identity and Participation in Friendster. In J. Karaganis (Ed.), *Structures of Participation in Digital Culture*. New York: Social Science Research Council.
- boyd, d., & Ellison, N. B. (2008). Social network sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1). Retrieved from <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>
- Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *Journal of Human-Computer Interaction*, 26(11-12), 1006-1030.
- Breikss, C. (2011). Mind Blowing Canadian Facebook Usage Statistics. Retrieved October 27, 2011 from <http://www.6smarketing.com/canadian-facebook-statistics/>
- Brown, K. (2005). Snowball sampling: using social networks to research non-heterosexual women. *International Journal of Social Research Methodology*, 8(1), 47-60.

- Bruckman, A. (1992). Identity Workshop: Emergent Social and Psychological Phenomena in Text-Based Virtual Reality. Retrieved from <http://www.cc.gatech.edu/~asb/papers/identity-workshop.rtf>
- Buchanan, S. (2007). *Wig meets Web (2.0): harnessing the law to commercialise and protect your IP*. Proceedings from Web Directions South, Sydney.
- Bumgarner, B. A. (2007). You have been poked: Exploring the uses and gratifications of Facebook among emerging adults. *First Monday*, 12(11). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2026/1897>
- Burge, B. (2007). Technological Determinism/Cybernetic Humanism. Retrieved April 10, 2011 from <http://bananapeelproject.org/2007/12/08/technological-determinismcybernetic-humanism/>
- Business Insider. (2010). Mark Zuckerberg, Moving Fast And Breaking Things. Retrieved from <http://www.businessinsider.com/mark-zuckerberg-2010-10>
- Cammaerts, B. (2008). Critiques on the participatory potentials of Web 2.0. *Communication, Culture & Critique*, 1(4), 358-377. Retrieved from <http://eprints.lse.ac.uk/23770/>
- Carlson, N. (2010). How Does Facebook Make Money. Retrieved from <http://www.businessinsider.com/how-does-facebook-make-money-2010-5>
- Carney, J. (2011). Facebook Valuation: \$100 billion? Retrieved from http://www.cnbc.com/id/43379994/Facebook_s_Valuation_100_Billion
- Cassidy, J. (2006). Me Media. *The New Yorker*. Retrieved from http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy
- Cavoukian, A. (2008, May 28). *Privacy and Digital Identity: Implications For The Internet*. Proceedings from Identity in the Information Society Workshop, Lake Maggiore, Italy.
- CBC News. (1993). A Computer Network Called Internet.
- Chandler, D., & Roberts-Young, D. (1998). The Construction of Identity in the Personal Homepages of Adolescents. Retrieved from <http://www.aber.ac.uk/media/Documents/short/strasbourg.html>
- City of Toronto. (2011). Canada's High Tech Hub: Toronto. Retrieved from http://www.toronto.ca/business_publications/pdf/ICT-Report_March2011.pdf
- Clarke, R. (2001). Information wants to be free. Retrieved from <http://www.rogerclarke.com/II/IWtbF.html>
- Cohen, N. S., & Shade, L. R. (2008). Gendering Facebook: Privacy and

- commodification. *Feminist Media Studies*, 8(2), 210-214.
- Commonwealth Secretariat. (ND). Young People. Retrieved January 1, 2012 from <http://www.thecommonwealth.org/Internal/180392/>
- Critical Art Ensemble. (1998). *Flesh machine: cyborgs, designer babies, and new eugenic consciousness*. Autonomedia. Retrieved from <http://www.critical-art.net/books/flesh/>
- Curtain, R. (2001). Youth and employment: A public policy perspective. *Development Bulletin*, 55, 7-11. Retrieved from http://www.curtain-consulting.net.au/download_controlled/Youth%20&%20Development/youthpol.pdf
- Curtis, A. (1992). The Engineer's Plot *Pandora's Box*: BBC.
- Curtis, A. (2011). All Watched Over by Machines of Loving Grace: BBC.
- Dash, A. (2010). The Facebook Reckoning. Retrieved from <http://dashes.com/anil/2010/09/the-facebook-reckoning-1.html>
- Davies, T. (2008). Facebook groups vs. Facebook Pages. Retrieved September 7, 2008 from <http://www.timdavies.org.uk/2008/02/18/facebook-groups-vs-facebook-pages>
- de Certeau, M. (1984). *The Practice of Everyday Life* (S. Rendall, Trans.). Berkeley: University of California Press.
- DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithica, New York: Cornell University Press.
- Denham, E. (2009). Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act. Retrieved from http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm
- DiNucci, D. (1999). Fragmented future. *Print*, 53(4), 32. Retrieved from http://www.tothepoint.com/fragmented_future.pdf
- Donath, J., & boyd, d. (2004). Public displays of connection. *BT Technology Journal*, 22(4), 71-82.
- Douglas, N. (2007). Facebook employees know what profiles you look at. Retrieved from <http://valleywag.gawker.com/tech/scoop/facebook-employees-know-what-profiles-you-look-at-315901.php>
- Dourish, P., & Anderson, K. (2006). Collective information practice: exploring privacy and security as social and cultural phenomena. *Human-computer interaction*, 21(3), 319-342. Retrieved from <http://www.dourish.com/>

publications/2006/DourishAnderson-InfoPractices-HCIJ.pdf

- Dourish, P., & Harrison, S. (1996). *Re-Place-ing Space: The Roles of Place and Space in Collaborative Systems*. Proceedings from Computer Supported Cooperative Work, Boston, Massachusetts.
- Dunbar, R. (1998). *Grooming, gossip, and the evolution of language*. Cambridge: Harvard University Press.
- Dupuy, J. P. (2009). *On the Origins of Cognitive Science: The Mechanization of the Mind* (M. B. DeBevoise, Trans.). Cambridge: MIT Press.
- Dyson, E. (1997). *Release 2.0: A Design for Living in the Digital Age*. New York: Broadway Books.
- Eisner, E. W. (1985). *The Educational Imagination: On the Design and Evaluation of School Programs*. Upper Saddle River, New Jersey: Merrill Prentice Hall. Retrieved from <http://people.cehd.tamu.edu/~pslattery/documents/EducationallImagination.pdf>
- Elmer, G. (2004). *Profiling machines: Mapping the personal information economy*. Cambridge: MIT Press.
- Elon University School of Communications. (ND). Imagining the Internet: A History and Forecast. Retrieved 2011, September 26, from <http://www.elon.edu/predictions/>
- Evans-Prichard, E. E. (1973). *Witchcraft, Oracles and Magic Among the Azande*. Oxford: Oxford University Press.
- Facebook. (2011). Facebook Timeline. Retrieved August 10, 2011 from <http://www.facebook.com/press/info.php?timeline>
- Facebook. (2004a). Thefacebook Frequently Asked Questions. Retrieved September 5, 2008 from <http://web.archive.org/web/20040906031202/www.thefacebook.com/faq.php#13>
- Facebook. (2004b). Thefacebook Welcome to Thefacebook! Retrieved September 4, 2008 from <http://web.archive.org/web/20040212031928/http://www.thefacebook.com/>
- Facebook. (ND). Facebook News Feed Preferences. Retrieved September 21, 2008 from http://www.new.facebook.com/home.php#/feed_prefs.php
- Facebook. (ND). Facebook Statistics. Retrieved September 7, 2008 from <http://www.new.facebook.com/press/info.php?statistics=>
- (2009). Facebook faces criticism on privacy change. *BBC News*. Retrieved from <http://news.bbc.co.uk/2/hi/technology/8405334.stm>

- Facebook Inc. (2011). Press Room. Retrieved July 13, 2011, from <http://www.facebook.com/press.php>
- Facebook Inc. (2007). Leading Websites Offer Beacon for Social Distribution. Retrieved July 15, 2010 from <http://www.facebook.com/press/releases.php?p=9166>
- Fiske, J. (1989). *Reading the Popular*. Boston: Unwin Hyman.
- Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology*, 7(4), 185-200.
- Fono, D., & Raynes-Goldie, K. (2006). Hyperfriends and Beyond: Friendship and Social Norms on LiveJournal. In M. a. C. H. Consalvo (Ed.), *Internet Research Annual Volume 4: Selected Papers from the Association of Internet Researchers Conference*. New York: Peter Lang. Retrieved from <http://k4t3.org/publications/hyperfriendship.pdf>
- Ford, S. M. (2010). *By Invitation Only: LiveJournal Users' Conceptions of Access to Personal Content*. Proceedings from Internet Research 11.0, Gothenberg, Sweden.
- Foucault, M. (1972). *The Archeology of Knowledge*.
- Freiwald, S. (1996). Uncertain Privacy: Communication Attributes After the Digital Telephony Act. *Southern California Law Review*, 69.
- Fuchs, C. (2008). [Review of the book Wikinomics: How mass collaboration changes everything, by Don Tapscott & Anthony D. Williams]. *Journal of Communication*, 58(2), 402-403. Retrieved from <http://ijoc.org/ojs/index.php/ijoc/article/view/250/125>
- Fuchs, C. (2009). Information and Communication Technologies and Society: A Contribution to the Critique of the Political Economy of the Internet. *European Journal of Communication*, 24(1), 69-87.
- Fuller, M. (2003). *Behind the blip: Essays on the culture of software*. New York: Autonomedia.
- Fuller, M. (2005). Media Ecologies: Masterialist Energies in Art and Technoculture.
- Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research*, 9(5), 372-382. Retrieved from <http://www.emeraldinsight.com/journals.htm?articleid=863656&show=abstract>
- Gal, S. (2002). A Semiotics of the Public/Private Divide. *differences: a Journal of Feminist Cultural Studies*, 13(1).
- Gandy, O. H. (1993). *The panoptic sort: a political economy of personal information*.

Boulder: Westview.

- Gannes, L. (2007). Facebook aims to be Social OS. Retrieved September 30, 2008 from <http://gigaom.com/2007/05/24/facebook-aims-to-be-social-os-waiting-for-f8-the-big-launch/>
- Gavison, R. (1992). Feminism and the Public/Private Distinction. *Stanford Law Review*, 45(1).
- Wiki, G. F. (ND). Dreamwidth. Retrieved December 12, 2011 from <http://geekfeminism.wikia.com/wiki/Dreamwidth>
- Geertz, C. (2000). Deep Play: Notes on the Balinese Cockfight. In *The Interpretation of Cultures: Selected Essays*. New York: Basic Books.
- Goffman, E. (1959). *The Presentation of Self in Everyday Life*. New York: Anchor Books.
- Goldstein, B. (2007, November 30). The Diaries of Facebook's Founder. *Slate*. Retrieved from <http://www.slate.com/id/2178939/entry/2178940/>
- Griffiths, R. T. (2002). History of the Internet, Internet for Historians (and just about everyone else). Retrieved from http://www.let.leidenuniv.nl/history/ivh/frame_theorie.htm
- Grimmelmann, J. (2009). Saving Facebook. *Iowa Law Review*, 94, 1137-1206. Retrieved from http://works.bepress.com/james_grimmelmann/20/
- Gross, R., & Acquisti, A. (2005). *Information Revelation and Privacy in Online Social Networks (The Facebook case)*. Proceedings from ACM Workshop on Privacy and the Electronic Society (WPES), 2005, Alexandria, Virginia.
- Hampton, K. N., & Wellman, B. (1999). Netville On-line and Off-line: Observing and Surveying a Wired Suburb. *American Behavioral Scientist*, 43(3), 475-492. Retrieved from <http://homes.chass.utoronto.ca/~khampton/papers/wired-abs8b.pdf>
- Harvey, D. (2007). *A Brief History of Neoliberalism*. Oxford: Oxford University Press.
- (2011). Have You Met Ms. Jones? *Nurse Jackie* : Showtime.
- Hayles, N. K. (1999). *How we became posthuman: virtual bodies in cybernetics, literature and informatics*. Chicago: University of Chicago Press.
- Haythornthwaite, C., & Kendall, L. (2010). Internet and community. *American Behavioral Scientist*, 53(8), 1083-1094. Retrieved from <http://abs.sagepub.com/content/53/8/1083.full.pdf>

- Heller, N. (2010). You Can't Handle the Veritas: What Aaron Sorkin and David Fincher get wrong about Harvard—and Facebook. Retrieved from <http://www.slate.com/id/2269308/>
- Herring, S. C. (2002). Computer-mediated communication on the Internet. *Annual Review of Information Science and Technology*, 26, 109-168.
- Hine, C. (2003). *Virtual Ethnography*. London: Sage.
- Hodgkinson, T. (2008, January 14). With friends like these. *The Guardian*. Retrieved from <http://www.guardian.co.uk/technology/2008/jan/14/facebook>
- Hoffman, A. M., & Summers, R. W. (Eds.). (2000). *Teen violence: a global view*. Westport: Greenwood Press.
- Hoffman, A. (2009). *Oversharing: a Discourse Analysis*. Masters, Library and Information Science. University of Wisconsin-Milwaukee.
- Hunter, L. (1995). Public Image. In D. Johnson & H. Nissenbaum (Eds.), *Computers, Ethics and Social Values*. Englewood Cliffs: Prentice Hall.
- Ing, D. (2008). *Business Models and Evolving Economic Paradigms: A Systems Science Approach*. Proceedings from Proceedings of the 52nd Annual Meeting of the ISSS.
- Jacobs, H. (2010). F*ck you, Google. Retrieved from <http://gizmodo.com/5470696/fck-you-google>
- Jarrett, K. (2008). Interactivity is Evil! A critical investigation of Web 2.0. *First Monday*, 13(3), 34-41. Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2140>
- Jernigan, C., & Mistree, B. F. T. (2009). Gaydar: Facebook friendships expose sexual orientation. *First Monday*, 14(10). Retrieved from <http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/2611>
- Jones, S. H. (2005). Autoethnography: making the personal political. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (3rd ed.). London: Sage.
- Jones, S. G. (1995). Understanding Community in The Information Age. In S. G. Jones (Ed.), *Cybersociety: Computer-Mediated Communication and Community*. Thousand Oaks: Sage.
- Kagan, N. (2006). New Facebook Feature: Events & Groups Redesign. Retrieved September 21, 2008 from <http://okdork.com/2006/04/18/new-facebook-feature-events-groups-redesign/>
- Kagan, N. (2005). Facebook Events Announcement. Retrieved September 21, 2008 from <http://okdork.com/2005/12/11/facebook-events-announcement/>

- Kamaraguru, P., & Cranor, L. F. (2005). Privacy Indexes: A Survey of Westin's Studies. Retrieved from <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>
- Kaplan, S. (2009). Josh Harris and QUIET: We Live In Public. Retrieved July 4, 2011 from <http://post.thing.net/node/2800>
- Keen, A. (2006). Web 2.0: The second generation of the internet has arrived. It's worse than you think. *The Weekly Standard*. Retrieved from <http://www.weeklystandard.com/Content/Public/Articles/000/000/006/714fjczq.asp?pg=2>
- Keen, A. (2011, January 20, 2011). *Digital Vertigo: An Anti-Social Manifesto*. Proceedings from Digital Privacy Forum, New York.
- Kelly, K. (1994). *Out of control: The new biology of machines, social systems, and the economic world*. New York: Basic Books.
- Kelly, K. (1999). Nerd theology. *Technology in Society*, 21, 387-392. Retrieved from http://www.kk.org/writings/nerd_theology.pdf
- Kelly, K. (2007). Kevin Kelly on the next 5000 days of the web : TED.
- Kelly, K. (2008). Thinkism. Retrieved June 23, 2011, from <http://www.kk.org/thetechnium/archives/2008/09/thinkism.php>
- Kennedy, P. (2011). The Ideas of Stewart Brand *Ideas* : CBC Radio.
- Kesan, J. P., & Shah, R. C. (2001). Fool us once shame on you-fool us twice shame on us: what we can learn from the privatizations of the internet backbone network and the domain name system. *Washington University Law Quarterly*, 79(1), 89-220. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=260834
- Kessler, G. C., & Shepard, S. D. (1997). The portrayal of the network in the popular media, or what the non-techie person-on-the-street must think of us! *Communications Magazine, IEEE*, 35(5), 114-118. Retrieved from <http://www.garykessler.net/library/portrayal.html>
- Kiesler, S., Siegel, J., & McGuire, T. W. (1984). Social psychological aspects of computer-mediated communication. *American psychologist*, 39(10), 1123. Retrieved from <http://psycnet.apa.org/psycinfo/1985-27678-001>
- Kirkpatrick, D. (2010a). *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York: Simon & Schuster.
- Kirkpatrick, M. (2009). Why Facebook Changed its Privacy Strategy. Retrieved from http://www.readwriteweb.com/archives/why_facebook_changed_privacy_policies.php

- Kirkpatrick, M. (2010b). Facebook's Zuckerberg Says The Age of Privacy is Over. Retrieved from http://www.readwriteweb.com/archives/facebook_zuckerberg_says_the_age_of_privacy_is_ov.php
- Kornblum, J. (2006, September 11). Facebook will soon be available to everyone. *USA Today*. Retrieved from http://www.usatoday.com/tech/news/2006-09-11-facebook-everyone_x.htm
- Kurzweil, R. (2000). *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. New York: Penguin Group.
- Lacy, S. (2008). *Once You're Lucky, Twice You're Good: The Rebirth of Silicon Valley and the Rise of Web 2.0*. New York: Gotham Books.
- Ladd, K. (2009). *Textuality, Performativity and Archive: Examining the Virtual Body in Socially Networked Space*. Master of Arts. University of Toronto, Toronto.
- Lampe, C., Ellison, N. B., & Steinfield, C. (2008). *Changes in use and perception of facebook*. Proceedings from Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work.
- Langlois, G., Elmer, G., McKelvey, F., & Devereaux, Z. (2009). Networked Publics: The Double Articulation of Code and Politics on Facebook. *Canadian Journal of Communication*, 34(3). Retrieved from <http://www.cjc-online.ca/index.php/journal/article/viewArticle/2114>
- Lanier, J. (2000). One half a manifesto. *The Edge*. Retrieved from http://www.edge.org/3rd_culture/lanier/lanier_index.html
- Lanier, J. (2010). *You Are Not a Gadget: a Manifesto*. New York: Alfred A. Knopf.
- Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5). Retrieved from <http://cs.ucsb.edu/~ravenben/classes/276/papers/history.pdf>
- Lenhart, A. (2009). Adults and Social Network Websites. Retrieved from <http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx>
- Leslie, S. W. (1993). *The Cold War and American science: The military-industrial-academic complex at MIT and Stanford*. New York: Columbia University Press.
- Lessa, I. (2006). Discursive struggles within social welfare: Restaging teen motherhood. *British Journal of Social Work*, 36(2), 283. Retrieved from <http://bjsw.oxfordjournals.org/content/36/2/283>
- Lessig, L. (1999). The Architecture of Privacy. *Vanderbilt Journal of Entertainment Law and Practice*, 1.

- Lessig, L. (2000). The Death of Cyberspace. *Washington and Lee Law Review*, 57(2), 337-347.
- Levenson, M. (2008, June 27). Facebook, ConnectU settle dispute. *The Boston Globe*. Retrieved from http://www.boston.com/business/technology/articles/2008/06/27/facebook_connectu_settle_dispute/
- Lichtblau, E. (2003). U.S. Uses Terror Law to Pursue Crimes From Drugs to Swindling. *The New York Times*. Retrieved from <http://www.nytimes.com/2003/09/28/politics/28LEGA.html>
- Liu, H. (2008). Social network profiles as taste performances. *Journal of Computer-Mediated Communication*, 13(1), 252-275. Retrieved from <http://jcmc.indiana.edu/vol13/issue1/liu.html?ref=SaglikAlani.Com>
- LiveJournal. (ND). Social Contract [Accessed via the Internet Wayback Machine]. Retrieved January 2, 2012 from <http://web.archive.org/web/20040401175244/http://www.livejournal.com/site/contract.bml>
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393. Retrieved from <http://nms.sagepub.com/content/10/3/393.short>
- Locke, L. (2007). The Future of Facebook. *Time*. Retrieved from <http://www.time.com/time/business/article/0,8599,1644040,00.html>
- Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.
- Machin, D. (2002). *Ethnographic research for media studies*. London: Arnold.
- Madden, M., & Smith, A. (2010). Reputation management and social media. *Washington, DC: Pew Internet & American Life Project*. Retrieved May, 26, 2010. Retrieved from <http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx>
- March, W., & Fleuriot, C. (2006). *Girls, technology and privacy: is my mother listening?* Proceedings from Proceedings of the SIGCHI conference on Human Factors in computing systems.
- Mardham-Bey, K. (2012). Personal FAQ. Retrieved January 18, 2012 from <http://www.mirc.com/pfaq.html>
- Markoff, J. (2006). *What the dormouse said: How the sixties counterculture shaped the personal computer industry*. New York: Penguin.

- Marwick, A. (2005). *"I'm a Lot More Interesting than a Friendster Profile": Identity Presentation, Authenticity and Power in Social Networking Services*. Proceedings from Internet Research 6.0, Chicago, IL.
- Marwick, A. (2010). *Status Update: Celebrity, Publicity and Self-Branding In Web 2.0*. PhD. New York University, New York.
- Marwick, A. E. (2008). To catch a predator? The MySpace moral panic. *First Monday*, 13(6). Retrieved from <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2152/1966>
- Maugeri, A. (2004, September 20). TheFacebook.com faces lawsuit. *The Daily Princetonian*. Retrieved from <http://www.dailyprincetonian.com/archives/2004/09/20/news/10767.shtml>
- McCarthy, C. (2010). Facebook F8: One Graph to Rule Them All. Retrieved from http://news.cnet.com/8301-13577_3-20003053-36.html
- McDonald, P. (2009). Growing Beyond Regional Networks. Retrieved July 14, 2011 from <http://www.facebook.com/blog.php?post=91242982130>
- McFedries, P. (2011). Lifestreaming. Retrieved July 13, 2011, from <http://www.wordspy.com/words/lifestreaming.asp>
- McKeon, M. (2010). The Evolution of Privacy on Facebook. Retrieved June 17, 2011 from <http://mattmckeon.com/facebook-privacy/>
- Menser, M., & Aronowitz, S. (1996). On cultural studies, science, and technology. In S. Aronowitz(pp. 7-28). London: Routledge.
- Mezrich, B. (2009). *The Accidental Billionaires: The Founding of Facebook, a Tale of Sex, Money, Genius and Betrayal*. Toronto: Random House of Canada.
- Miller, D., & Slater, D. (2000). *The Internet: an ethnographic approach*. Oxford: Berg.
- Mills, C. W. (1959). *The Sociological Imagination*. Oxford: Oxford University Press.
- Morin, D. (2007). Goodbye Facebook Courses, Hello Platform Courses. Retrieved September 5, 2008 from <http://blog.new.facebook.com/blog.php?post=4314497130>
- Needleman, R. (2008). Google's View: Three Trends in social networking. *Cnet News*. Retrieved from http://news.cnet.com/8301-17939_109-9970053-2.html
- Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17, 559-596.

- Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
- Noy, C. (2008). Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of social research methodology*, 11(4), 327-344. Retrieved from <http://www.informaworld.com/index/783428219.pdf>
- O'Brien, L. (2007). Poking Facebook. *02138*, p. 66. Retrieved from <http://www.02138mag.com/magazine/article/1724.html>
- O'Dell, J. (2011). Facebook's Ad Revenue Hit \$1.86B for 2010. Retrieved from <http://mashable.com/2011/01/17/facebooks-ad-revenue-hit-1-86b-for-2010/>
- O'Neill, N. (2008a). The Facebook Stalking Tool. Retrieved from <http://www.allfacebook.com/2008/05/the-facebook-stalking-tool/>
- O'Neill, N. (2008b). Facebook Connect is Facebook Redesigned. Retrieved July 16, 2011 from <http://www.allfacebook.com/facebook-connect-is-facebook-beacon-redesigned-2008-09>
- O'Reilly, T., & Battelle, J. (2009, October 20-22). *Web squared: Web 2.0 five years on*. Proceedings from Web 2.0 Summit, San Francisco.
- O'Reilly, T. (2006). Web 2.0 Compact Definition: Trying Again. Retrieved from <http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html>
- O'Reilly, T. (2005). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Retrieved from <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html>
- Office of the Privacy Commissioner of Canada. (2009). Facebook agrees to address Privacy Commissioner's concerns. Retrieved August 31, 2011, from http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm
- Ong, W. J. (1982). Orality and Literacy: The Technologizing of the World. In. New York: Routledge.
- Onufrijchuk, R. (1993). Introducing Innis/McLuhan concluding: The Innis in McLuhan's "system". *Continuum: The Australian Journal of Media & Culture*, 7(1), 43-74. Retrieved from <http://www.mcc.murdoch.edu.au/ReadingRoom/7.1/Onuf.html>
- Oosthoek, S. (2009, January 23). Registered with the do-not-call list? Expect more calls, says consumer watchdog. *CBC News*. Retrieved from <http://www.cbc.ca/technology/story/2009/01/23/donotcall.html>
- Opsahl, K. (2010). Facebook's Eroding Privacy Policy: A Timeline. Retrieved January 14, 2012 from <https://www.eff.org/deeplinks/2010/04/facebook->

timeline

- Orlowski, A. (2010). Facebook founder called trusting users dumbf*cks. Retrieved from http://www.theregister.co.uk/2010/05/14/facebook_trust_dumb/
- Palen, L., & Dourish, P. (2003). *Unpacking "privacy" for a Networked World*. Proceedings from CHI 2003, Fort Lauderdale, Florida.
- Parks, M., & Roberts, L. (1998). Making MOOsic: The development of personal relationships on line and a comparison to their off-line counterparts. *Journal of Social and Personal Relationships*, 15. Retrieved from <http://www.geser.net/moo.htm>
- Parry, W. (2005). Patriot Act vs. homeless. *The Associated Press*. Retrieved from <http://community.seattletimes.nwsources.com/archive/?date=20050701&slug=patriot01>
- Pearlman, L. (2007). Facebook Ads. Retrieved October 27, 2008 from <http://blog.facebook.com/blog.php?post=6972252130>
- Pelletier, K. (2008, January/February). Keep Out! *Philosophy Now*. Retrieved from http://www.philosophynow.org/issue65/Keep_Out
- Petersen, S. M. (2008). Loser generated content: From participation to exploitation. *First Monday*, 13(3), 3. Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2141/1948>
- Peterson, C. (2009). *Saving Face: The Privacy Architecture of Facebook*. Senior Thesis. University of Massachusetts-Amherst.
- Philips, S. (2007, July 25). A Brief History of Facebook. *guardian.co.uk*. Retrieved from <http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia>
- Pickering, A. (2010). *The Cybernetic Brain: Sketches of Another Future*. Chicago: University Of Chicago Press.
- Platt, C. (2000). Steaming Video. *Wired*. Retrieved from <http://www.wired.com/wired/archive/8.11/luvvy.html>
- Pohflepp, S. (2008). *The Valley and the Sky*. Masters. Royal College of Art, London.
- Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010). *Using social networks to harvest email addresses*. Proceedings from Proceedings of the 9th annual ACM workshop on Privacy in the electronic society.
- Ptolemy, R. B. (2009). *Transcendent Man* : Ptolemaic Productions.
- Putnam, R. (2000). *Bowling Alone: The Collapse and Reivival of the American*

Community. New York: Simon & Schuster.

Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, 4(4), 323-333.

Raice, S. (2011, July 14). Is Facebook Worth \$100 Billion? *Wall Street Journal*. Retrieved from <http://online.wsj.com/article/SB10001424052702304584404576442950773361780.html>

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1-4). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432>

Raynes-Goldie, K., & Fono, D. (2009). Wiki Use by Political Parties: A case study. In *Online Deliberation: Design, Research, and Practice*. Stanford: CSLI Publications. Retrieved from http://odbook.stanford.edu/static/filedocument/2009/11/15/Chapter_16._Raynes-Goldie_and_Fono.pdf

Raynes-Goldie, K. (2011). *Annotated bibliography: Digitally mediated surveillance, privacy and social network sites*. Proceedings from Cybersurveillance and Everyday Life: An International Workshop, Toronto.

Reah, D. (1998). *The language of newspapers*. London: Routledge.

Rheingold, H. (2000). *The virtual community: Homesteading on the electronic frontier*. Cambridge: MIT Press. Retrieved from <http://www.rheingold.com/vc/book/>

Rice, R. E., & Love, G. (1987). Electronic emotion: socioemotional content in a computer-mediated communication network. *Communication research*. Retrieved from <http://psycnet.apa.org/psycinfo/1988-16422-001>

Richards, C. (1999). CMC and the connection between virtual utopias and actual realities. *Javnost The Public*, 6(4), 11-22. Retrieved from http://www.javnost-thepublic.org/media/datoteke/1999-4-richards_.pdf

Rogers, R. (2004). Information politics on the Web.

Rogers, R. (2009). *The end of the virtual: digital methods*. Amsterdam University Press. Retrieved from <http://books.google.com/books?hl=en&lr=&id=ZHFis5sEAicC&oi=fnd&pg=PA5&dq=The+End+of+the+Virtual:+Digital+Methods&ots=kL5meQN6r0&sig=6A0XX5gkEHmlCyeYxS14x2cez4c>

Rotenberg, M. (2011, January 20, 2011). *Keynote Presentation*. Proceedings from Digital Privacy Forum, New York.

Ryan, J. A. (2008). *The Virtual Campfire: An Ethnography of Online Social*

Networking. Wesleyan University, Middletown, Connecticut.

- Samuelson, R. J. (2006). A Web of Exhibitionists. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/19/AR2006091901439.html>
- Schaefer, S. (2012, January 16). Report: April Showers Could Bring May Facebook IPO. *Forbes*. Retrieved from <http://www.forbes.com/sites/steveschaefer/2012/01/16/report-april-showers-could-bring-may-facebook-ipo/>
- Schaller, R. R. (1997). Moore's law: past, present and future. *Spectrum*, 34(6). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=591665
- Scharmen, F. (2006). "You must be logged in to do that!": *Myspace and Control*.
- Schauer, B. (2005). Experience Attributes: Crucial DNA of Web 2.0. *Adaptive Path*. Retrieved from <http://www.adaptivepath.com/ideas/e000547>
- Schiffman, B. (2007). Status Update: Facebook Is Letting Users Drop the "Is". *Wired.com*. Retrieved from <http://blog.wired.com/business/2007/11/status-update-f.html>
- Scholz, T. (2008). Market Ideology and the Myths of Web 2.0. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2138/1945>
- Scholz, T., & Hartzog, P. (2008). Trebor Scholz and Paul Hartzog: Toward a critique of the social web. *Re-Public*. Retrieved from <http://www.re-public.gr/en/?p=201>
- Schonfeld, E. (2009). Facebook Photos Pulls Away from the Pack. Retrieved from <http://techcrunch.com/2009/02/22/facebook-photos-pulls-away-from-the-pack/>
- Segal, B. (2008). *Social Media In Canada: Web 2.0*. Proceedings from CaseCamp, Toronto.
- Shade, L. R. (2008). Internet Social Networking in Young Women's Everyday Lives: Some Insights from Focus Groups. *Our Schools, Our Selves*, 65-73. Retrieved from http://www.policyalternatives.ca/sites/default/files/uploads/publications/Our_Schools_Ourselves/8_Shade_internet_social_networking.pdf
- Sheller, M., & Urry, J. (2003). Mobile Transformations of 'Public' and 'Private' Life. *Theory, Culture & Society*, 20(3), 107-125.
- Sherman, R. (2007). *Class Acts*. Berkeley: University of California Press.
- Silver, D. (2008). History, Hype, and Hope: An Afterward. *First Monday*, 13(3-3). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2143/1950>

- Smith, J. (2009). Facebook now lets advertisers use your picture. Retrieved December 12, 2011 from <http://www.dailyfinance.com/2009/07/17/facebook-now-lets-advertisers-use-your-picture/>
- Smith, J. (2007). Facebook Friends Lists let you manage your 'friends' more effectively. Retrieved September 21, 2008 from <http://www.insidefacebook.com/2007/12/19/facebook-friend-lists-let-you-manage-your-friends-more-effectively/>
- Smith, J. (2008). Live Notes From Mark Zuckerberg's Keynote at f8 Developer Conference. Retrieved 5 September, 2008 from <http://www.insidefacebook.com/2008/07/23/live-notes-from-mark-zuckerbergs-keynote-at-f8-developer-conference/>
- Smith, M. R., & Marx, L. (1994). *Does Technology Drive History?: The dilemma of technological determinism*. Cambridge: MIT Press.
- Solove, D. J. (2007a). "I've got nothing to hide" and Other Misunderstandings of Privacy. *San Diego Law Review*.
- Solove, D. J. (2007b). Privacy in an Overexposed World. In *The Future of Reputation*. Yale University Press. Retrieved from <http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text/futureofreputation-ch7.pdf>
- Sprenger, P. (1999). Sun on Privacy: 'Get Over It'. Retrieved October 5, 2011 from <http://www.wired.com/politics/law/news/1999/01/17538>
- Sproull, L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communications. *Management science*, 1492-1512.
- Staff (2003, November 6). M*A*S*H*. *The Harvard Crimson*. Retrieved from <http://www.thecrimson.com/article.aspx?ref=349866>
- Staff (2007). FBI abused Patriot Act powers, audit finds. *The Guardian*. Retrieved from <http://www.guardian.co.uk/world/2007/mar/09/usa>
- Stanford University. (2005). Mark Zuckerberg Discusses TheFacebook : Stanford Technology Ventures Program.
- Steeves, V. (2008). If the Supreme Court were on Facebook: Evaluating the reasonable expectation of privacy test from a social perspective. 50(3), 331-347. Retrieved from <http://utpjournals.metapress.com/index/r4q238245745qk5r.pdf>
- Steeves, V., Milford, T., & Butts, A. (2010). Summary of Research on Youth Online Privacy. *The Office of the Privacy Commissioner of Canada*.
- Stein, L. A. (1999). Challenging the computational metaphor: Implications for how

- we think. *Cybernetics and Systems*, 30(6), 473-507.
- Stelter, B., & Arango, T. (2009, May 3). Losing Popularity Contest, MySpace Tries a Makeover. *The New York Times*. Retrieved from <http://www.nytimes.com/2009/05/04/technology/companies/04myspace.html>
- Stites, R. (1991). *Revolutionary dreams: Utopian Vision and Experimental Life in the Russian Revolution*. Oxford: Oxford University Press.
- Stumpel, M. (2010). *The Politics of Social Media: Facebook: Control and Resistance*. Masters. University of Amsterdam, Amsterdam.
- Stutzman, F., & Kramer-Duffield, J. (2010). *Friends only: examining a privacy-enhancing behavior in facebook*. Proceedings from Proceedings of the 28th International Conference on Human Factors in Computing Systems.
- Stutzman, F. (2006). *An Evaluation of Identity Sharing in Social Network Communities*. Proceedings from iDMAa and IMS Code Conference.
- Stutzman, F. (2005). When the gates to the walled garden are thrown open. Retrieved September 21, 2008 from <http://fstutzman.com/2005/11/29/when-the-gates-to-the-walled-garden-are-thrown-open/>
- Sudweeks, F., & Simoff, S. K. (1999). Complementary Explorative Data Analysis: The reconciliation of Quantitative and Qualitative principles. In S. Jones (Ed.), *Doing Internet Research*. London: Sage.
- Swisher, K. (2007). A Well-Deserved Court Loss for Facebook. Retrieved from <http://allthingsd.com/20071201/a-well-deserved-court-loss-for-facebook/>
- Teitel, E. (2011, November 1). Can teens escape embarrassment on Facebook? *Maclean's*. Retrieved from <http://www2.macleans.ca/2011/11/01/the-new-paparazzi/>
- Terranova, T. (2003). Free Labor: Producing Culture for the Digital Economy. *Electronic Book Review*. Retrieved from <http://www.electronicbookreview.com/thread/technocapitalism/voluntary>
- Wag, T. (2007). Can a Facebook app possibly be useful? Retrieved October 1, 2008 from <http://valleywag.com/tech/facebook/can-a-facebook-app-possibly-be-useful-303819.php>
- Thompson, C. (2008). Brave New World of Digital Intimacy. *New York Times Magazine*. Retrieved from <http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html>
- Thompson, M. (2011, October 26). *Awareness, Understanding, and Individual Decision-Making*. Proceedings from Organisation for Economic Co-Operation and Development Conference: The Evolving Role of the Individual in Privacy

- Protection 30 Years after the OECD Privacy Guidelines, Jerusalem, Israel.
- Thomson, N. F. (2009). *Social Networking and the Employment Screening and Evaluation Process*. Proceedings from International Academy for Case Studies, New Orleans.
- Timoner, O. (2009). *We Live in Public* : Interloper Films.
- Truscello, M. (2006). Behind the Blip: Essays on the Culture of Software (review). *Cultural Critique*, 63. Retrieved from http://muse.jhu.edu/journals/cultural_critique/v063/63.1truscello.html
- Tsotsis, A. (2010a). Mark Zuckerberg: Can't Stand the Heat? Take Off the Hoodie. Retrieved from http://blogs.sfweekly.com/thesnitch/2010/06/just_watch_spiderman.php
- Tsotsis, A. (2010b). Zuckerberg's Bizarre Facebook Insignia Revealed, And What It Means. Retrieved from http://blogs.sfweekly.com/thesnitch/2010/06/bizarre_facebook_insignia_reve.php
- Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36.
- Turkle, S. (1994). Constructions and reconstructions of self in virtual reality: Playing in the MUDs. *Mind, Culture, and Activity*, 1(3), 158-167.
- Turkle, S. (1997). *Life on the Screen: Identity in the Age of the Internet*. New York: Touchstone Books.
- Turkle, S. (2004). *The Second Self: Computers and the Human Spirit*. Cambridge: MIT Press.
- Turner, F. (2005). Where the counterculture met the new economy: The WELL and the origins of virtual community. *Technology and Culture*, 46(3), 485-512. Retrieved from <http://www.stanford.edu/~fturner/Turner%20Tech%20&%20Culture%2046%203.pdf>
- Turner, F. (2006). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network and the Rise of Digital Utopianism*. Chicago: The University of Chicago Press.
- Umpleby, S. A. (2001). What Comes After Second Order Cybernetics? Retrieved from http://www.gwu.edu/~umpleby/recent_papers/2001_what_comes_after_second_order_cybernetics.htm
- Urban Dictionary. (2011). Creeping. Retrieved June 27, 2011, from <http://www.urbandictionary.com/define.php?term=creeping>

- Utz, S., & Krämer, N. (2009). The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2). Retrieved from <http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1>
- van Bree, P. (2010). Californian Ideology 2.0, A First Farewell. Retrieved from <http://mastersofmedia.hum.uva.nl/2010/10/05/californian-ideology-2-0-a-first-farewell/>
- Van Dijck, J., & Nieborg, D. (2009). Wikinomics and its discontents: a critical analysis of Web 2.0 business manifestos. *New Media & Society*, 11(5), 855. Retrieved from <http://nms.sagepub.com/content/11/5/855.short>
- Vargas, J. A. (2010). The Face of Facebook. *The New Yorker*.
- Vitak, J., Ellison, N. B., & Steinfield, C. (2011). *The Ties That Bond: Re-Examining the Relationship between Facebook Use and Bonding Social Capital*. Proceedings from 44th Hawaii International Conference on System Sciences, Kauai.
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- Weintraub, J. (1997a). The Theory and Politics of the Public/Private Distinction. In J. Weintraub & K. Kumar (Eds.), *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy* (pp. 1-42). Chicago: Chicago University Press.
- Weintraub, J. (1997b). Public/Private: The Limitations of a Grand Dichotomy. 7(2), 13-24.
- Wellman, B. (1993). An egocentric network tale: comment on Bien *et al.* (1991). *Social Networks*, 15(4), 423-436. Retrieved from <http://homes.chass.utoronto.ca/~wellman/publications/egocentric/egocentric.pdf>
- Wellman, B. (2004). *The glocal village: Internet and community*. Proceedings from Ideas.
- Wellman, B., & Gulia, M. (1999). Net Surfers Don't Ride Alone: Virtual Communities as Communities. In M. Smith & P. Kollock (Eds.), *Communities in Cyberspace* (pp. 331-366). London: Routledge.
- Wellman, B. (1997). An Electronic Group is Virtually a Social Network. In S. Kiesler (Ed.), *Culture of the Internet*. Mahwah: Lawrence Erlbaum. Retrieved from <http://www.chass.utoronto.ca/~wellman/publications/electronicgroup/electronicgroup.pdf>
- Wiener, N. (1949). *Cybernetics: or, Control and Communication in the Animal and*

the Machine. New York: John Wiley & Sons.

Wiener, N. (1950). *The Human Use of Human Beings: Cybernetics and Society*. Boston: Houghton Mifflin.

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy*, 25(6), 865-899. Retrieved from <http://www.rcss.ed.ac.uk/technology/SSTRP.html>

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, 109(1), 121-136. Retrieved from <http://www.jstor.org/stable/20024652>

Winner, L. (1993). Upon opening the black box and finding it empty: Social constructivism and the philosophy of technology. *Science, Technology, & Human Values*, 18(3), 362-378.

Wolf, M. (1992). *A Thrice Told Tale*. Stanford: Stanford University Press.

Yarow, J. (2010). Facebook Employee: Mark Zuckerberg 'Doesn't Believe' In Privacy. Retrieved from <http://www.businessinsider.com/mark-zuckerberg-doesnt-believe-in-privacy-2010-4>

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, 24(5), 1816-1836. Retrieved from <http://linkinghub.elsevier.com/retrieve/pii/S0747563208000204>

Zimmer, M. (2008a). Preface: Critical perspectives on web 2.0. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2137/1943>

Zimmer, M. (2008b). The externalities of Search 2.0: The emerging privacy threats when the drive for the perfect search engine meets Web 2.0. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2136/1944>

Zimmer, M. (2010a). *The Laws of Social Networking, or, How Facebook Feigns Privacy*. Proceedings from Internet Research 11, Gothenberg, Sweden.

Zimmer, M. (2010b). Call for Panelists: On the Philosophy of Facebook. Retrieved January 27, 2010 from <http://michaelzimmer.org/2010/01/27/call-for-panelists-on-the-philosophy-of-facebook/>

Zimmer, M. (2008c). Facebook's Zuckerberg on Increasing the Streams of Personal Information Online. Retrieved from <http://michaelzimmer.org/2008/11/08/facebook-zuckerberg-on-increasing-the-streams-of-personal-information-online/>

Zittrain, J. (2009). *The Future of the Internet--and How to Stop it*. New Haven: Yale

University Press. Retrieved from <http://yupnet.org/zittrain>

Zoolers, A. (2009). Critical Perspectives on Social Network Sites. In R. Hammer & D. Kellner (Eds.), *Media/Cultural Studies: Critical Approaches* (pp. 602-614). New York: Peter Lang.

Zuckerberg, M. (2007). Our First 100 Million. Retrieved September 21, 2008 from <http://blog.new.facebook.com/blog.php?post=28111272130>

Zuckerberg, M. (2009a). Mark Zuckerberg Facebook. Retrieved from <http://www.facebook.com/markzuckerberg>

Zuckerberg, M. (2009b). Improving Your Ability to Share and Connect. Retrieved from <http://blog.facebook.com/blog.php?post=57822962130>

Zuckerberg, M. (2003). Harvard Face Mash The Process. Retrieved January 10, 2006 from <http://www.02138mag.com/asset/1140.pdf>

Zuckerberg, M. (2006). An Open Letter from Mark Zuckerberg. Retrieved August 15, 2011 from <https://blog.facebook.com/blog.php?post=2208562130>

Every reasonable effort has been made to acknowledge the owners of copyright material. I would be pleased to hear from any copyright owner who has been omitted or incorrectly acknowledged.