The Pennsylvania State University

The Graduate School

Department of English

RHETORIC, SOCIAL MEDIA, AND PRIVACY

A Dissertation in

English

by

Michael J. Faris

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

December 2012

The dissertation of Michael J. Faris was reviewed and approved* by the following:

Stuart Selber
Associate Professor of English
Dissertation Advisor
Chair of Committee

John Selzer
Professor of English

Debra Hawhee
Professor of English

Robert Caserio
Professor of English

Lynette Kvasny
Associate Professor of Information Sciences and Technology

Mark Morrisson
Professor of English
Department Head

*Signatures are on file in the Graduate School

ABSTRACT

This dissertation investigates notions and practices related to privacy in social media environments. I argue for a social and rhetorical understanding of privacy in social media environments, involving attention to how the affordances of digital media affect how privacy is practiced in these environments. For example, the aggregation of data in digital media means that control over access to information is thoroughly distributed throughout one's social network online: one's privacy is as much dependent upon others' practices and user settings as it is on one's own.

In order to explore privacy in these environments, I analyze popular discourses about privacy online, user interfaces, and user practices related to privacy in these environments. I explore four concepts interrelated to privacy: materiality, identity, intimacy, and sociability. Chapter 2 explores the material practices of managing privacy in public spaces using objects, including mobile phones and laptops, arguing that despite popular narratives that users do not have a sense of place when cocooned behind devices, that people use these devices in contextual ways in order to engage in their environments and manage privacy.

Chapter 3 explores how identity shifts in online environments: Identity now becomes a series of digital traces that people use in order to construct others' identities through their private information posted in various locations online. Private information is now externalized and less secure online. Chapter 4 explores the moral panic around sexting, the sharing of nude or sexually provocative images and text through text messages on mobile phones. This chapter argues that the moral panic blames young girls and women for their indiscretions disproportionately compared to those who violate privacy by forwarding images on. Privacy is incredibly gendered, and our culture has yet to extend the sorts of expectations and rights of privacy to women and girls as it extends to boys and men.

In Chapter 5, I argue that grand narratives about declining sociability ignore the situated material and embodied practices of sociability in environments. I argue that in order to understand how shifts in privacy practices affect sociability, scholars need to attend to the specific architectures and embodied practices of users within specific ecologies. This project concludes with a heuristic for digital literacies of privacy in social media environments, outlined in the concluding chapter. I argue for a set of practices that involves functional, critical, and rhetorical literate practices that can be practiced in a variety of contexts.

TABLE OF CONTENTS

LIST OF FIGURES vi

LIST OF TABLES vii

ACKNOWLEDGEMENTS viii

Chapter 1 Introduction: Rhetoric, Social Media, and Privacy 1

Chapter 2 Materialities and Mobilities of Technologies and Private Spaces in Coffee Shops 76

Chapter 3 The Digital Traces of Identity Online 124

Chapter 4 "When Privates Go Public": The Public Pedagogy of Digitized Intimacy 174

Chapter 5 We Live in Public: On Sociability and Situated Practices 220

Chapter 6 Conclusion: Toward a Digital Literacy of Privacy 257

Appendix Tyler Clementi and Dharun Ravi: A Timeline of Events 274

Works Cited 278

LIST OF FIGURES

Figure **1-1**: Screen captures of the opening image from the iPhone app Girls Around Me (left) and a map with women's Facebook profile pictures charted on it from the app (right) (Source: Brownlee). 2

Figure **2-1**: Laptop users working in a coffee shop (Source: Joel Washing, Flickr, Creative Commons: http://www.flickr.com/photos/joelwashing/2104633476) 76

Figure **2-2**: The storefront of Snakes & Lattes Board Game Café (Souce: Jennifer Yin, Flickr, Creative Commons, http://www.flickr.com/photos/bittermelon/6102404602/) .. 88

Figure **2-3**: View from the entrace of Snakes & Lattes Board Game Café (Source: Jennifer Yin, Flickr, Creative Commons, http://www.flickr.com/photos/bittermelon/6102403858/) 89

Figure **2-4**: An iPhone screenshot of pictures uploaded to Instragram using the hashtag #snakesandlattes (taken by author, June 2012) 97

Figure **2-5**: Tom Pappalardo's cartoon exhibiting how difficult it is to display (and thus know) what someone is doing behind a screen (Source: Pappalardo) 114

Figure **3-1**: A screenshot of Tyler Clementi's initial post to JustUsBoys. Using the screen name "cit2mo," he explained his roommate's use of the webcam and asked for advice from other forum users (Source: R. Miller, "Is Nothing Sacred?") 148

Figure **3-2**: A screenshot of Dharun Ravi's Twitter stream (Source: O'Connor, "How a College Kid") 149

Figure **4-1**: The cover of the May 2009 issue of *Reader's Digest* (Source: Matt M., Flickr, Creative Commons, http://www.flickr.com/photos/macq/3485243622) 174

Figure **5-1**: Josh Harris as "Luvvy" (Source: http://www.indiepixfilms.com/) 236

Figure **5-2**: A view of the toilets at Quiet (Source: weliveinpublicthemovie.com) 241

Figure **5-3**: The dining table at Quiet (Source: weliveinpublicthemovie.com) 242

Figure **5-4**: A camera shot of Josh Harris inside the communal shower at Quiet (Source: weliveinpublicthemovie.com) 242

LIST OF TABLES

Table **2-1**: A Heuristic for Responses to Virtual Mobility. 116

Table **4-1**: Summary of Surveys of Teenagers' and Young Adults' Sexting Practices..... 194

ACKNOWLEDGEMENTS

This project would not have been possible without the guidance and patience of my chair and adviser, Stuart Selber, who encouraged me throughout the process of planning and writing this dissertation, gave helpful feedback, and, importantly, provided sage advice at every stage in the process. Stuart Selber's patience with my writing and advice at key moments (getting started, organizing the dissertation, presenting it to the committee, and so forth) was invaluable. I also greatly appreciate his timely feedback on drafts, which was always encouraging but also challenged me to articulate ideas that I had too quickly glossed over in previous drafts.

I would also like to thank my other committee members, Jack Selzer, Debra Hawhee, Robert Caserio, and Lynette Kvasny, all of whom provided helpful feedback and brainstorming ideas during the proposal stage and offered wonderful questions, criticisms, and insights as I discussed this project with them and during the defense. I also appreciate Jack Selzer and Debra Hawhee's guidance and mentorship as I developed (and continue to develop) as a scholar, both in and outside of the classroom. Other teachers at Penn State have also been helpful in my development because of their courses. Cheryl Glenn, Keith Gilyard, Xiaoye You, Rosa Eberly, Stephen Browne, Jack Selzer, Debra Hawhee, and Stuart Selber all provided encouraging and stimulating atmospheres in their classes, introducing me to scholarship, scholarly conventions, approaches to problems, and research and writing conventions and practices that will continue to inform my work for decades to come.

I am extremely appreciative of the Center for Democratic Deliberation for the fellowship during the 2011-2012 academic year that provided funding for conference travel related to the dissertation, an office for writing, and a wonderful support networking in my writing group.

Thank you to Director J. Michael Hogan. Cheryl Glenn also led a very helpful writing group with the other CDD fellows, whose feedback I found insightful and useful as I revised chapters. The feedback from Cheryl Glenn; CDD fellows Heather Adams, Bonnie Sierlecki, and Adam Perry; and Rock Ethics Institute fellow Eric Miller was extremely useful as I moved early drafts of chapters (with little sense of cohesion or argument) into the final drafts you read here.

My colleagues in the English Department were especially wonderful throughout my time at Penn State—both as I wrote this dissertation and as I thought through other rhetorical and scholarly situations. Heather Adams, Ersula Ore, Adam Haley, and Andrew Pilsch were especially helpful in providing advice and safe spaces to explore problems, either face-to-face, over the phone, or through social networking sites like Twitter and Facebook.

Of course, this project would not have been possible without the new and developing writing and social spaces created by companies like Facebook, Twitter, Google, Yahoo, and others. While I have certain ambivalences about these spaces (ambivalences that perhaps do not fully reveal themselves in the dissertation), these spaces have been useful not only as sites of analysis, but also as sites for thinking through the problems I discuss in my dissertation. My social network on Facebook and Twitter have been helpful because participants have shared resources and engaged in conversations with me that have informed my perspectives on social media.

My students too have been influential in helping me think through social issues related to privacy and technology. Students in the spring 2011 section of English 245: Introduction to Lesbian, Gay, Bisexual, Transgender, and Queer Studies were amazing and thoughtful, and I especially appreciate their patient discussions about intimacy and sociability throughout the term.

Writing isn't possible without physical spaces to write in, and I am very appreciative of the many physical spaces in State College that were accessible to me to sit for hours, drink coffee,

and research and write this dissertation. The employees at some of these establishments have become more than just baristas and servers; they have also become friends. Special thanks to the employees and owners of Webster's Café, Starbucks, and Saint's. An additional shout out goes to Brian and Ellen at Chumley's, an establishment that helped make State College a home.

Chapter 1

Introduction: Rhetoric, Social Media, and Privacy

In early 2012 the Russian app developer i-Free Innovations released a new iPhone and iPad app called Girls Around Me in Apple's App Store. Girls Around Me, as the name suggests, was a location-based app that offered users a map of their surrounding area with pictures of local women plotted onto the map (alternatively, a user could opt to find men instead of women). The app drew on the public application programming interfaces (APIs) for Google Maps, Facebook, and Foursquare in order to map the publicly available Facebook profiles of local people who had checked into a location using Foursquare, a social media service that allows users to share where they are located by "checking in" at places (see Figure **1-1**). Simply by tapping on a profile picture plotted onto the map, a user could see someone's publicly available Facebook pictures and name, know how long ago they had checked in at the location, and send a message to their Facebook account.

When *Cult of Mac* blogger John Brownlee wrote about the app in March 2012, he explained how the app worked and stressed the need for readers to educate their friends about privacy settings on social networking sites. Importantly, he stressed that the developers of Girls Around Me likely saw this as a harmless app, not a device for stalkers and rapists, and that the app did not violate Apple's policies for the App Store. Rather, the app's existence points to the difficulties in managing privacy on social networking sites. Facebook users might not be aware that their profile is public, nor that their profile information is available through Facebook's API. Additionally, they may not realize that by linking their Foursquare account to their public Facebook profile, that they make this aggregated data more readily available: These data points,

when publicly available, can be aggregated into other applications, services, and databases legally and quite easily.

Figure **1-1**: Screen captures of the opening image from the iPhone app Girls Around Me (left) and a map with women's Facebook profile pictures charted on it from the app (right) (Source: Brownlee)

After Brownlee's blog post circulated on various social networking sites, Foursquare pulled access to its data from the application, and the developers followed up by removing the application from Apple's App Store, citing the necessity to fix bugs in the app that led to error messages. They also stressed that their intentions were not to violate Facebook and Foursquare users' privacy, but rather to allow users to find public "hot spots" nearby (Kafka). Despite the app developers' claimed good intentions, Brownlee and various others called the app "creepy" and a "wake-up call about privacy."

Girls Around Me is situated in a long line of technological developments over the last decade or so that have led scholars and the popular media to attend to changing practices and technologies related to privacy. In their contribution to *Into the Blogosphere*, rhetoric and writing scholars Carolyn Miller and Dawn Shepherd explore how practices related to the public/private distinction shifted in the use of blogs, which remediated diaries in publicly available settings. The popular press has focused on various privacy concerns, including fears that youth are in danger of sexual predators on sites like MySpace and Facebook (e.g., B. Stone), and that employers were now searching Facebook profiles of potential employees for incriminating photos and posts (e.g., "Online Party Crashers"). And recently, rhetoric and writing scholars Gina Maranto and Matt Barton explore the implications of teachers possibly sharing information on sites that administrators may find inappropriate, or that might harm their ethos with students—just to cite a few examples.

This dissertation explores the rhetorical dimensions of privacy in social media environments, analyzing the rhetorical forces the help to constitute notions and practices of privacy in social media contexts**.** Rather than understand privacy as something that needs to be protected or as something that users online are "giving up," as many popular discourses portray it, I argue that privacy is something that is rhetorically and materially practiced. Additionally, I argue that privacy—along with its counterpart publicity—is something that is argued about and needs to be argued about. My focus in this project is on *social* aspects of privacy, rather than *institutional* aspects of privacy. Put differently, I am interested in how users of social media sites practice and understand their privacy in regards to social relations, rather than how their privacy might relate to institutions like corporations and the government. While certain institutional forces are certainly a cause of great concern for privacy—the buying and selling of data, the U.S. PATRIOT Act, the current threats to women's bodily and decisional privacy through attempts to limit their reproductive freedom, and subpoenas for companies like Twitter and Facebook to hand

over data in court cases—I bracket these institutional concerns in order to focus on social aspects of privacy in everyday life. This is not to say that social and institutional privacy are not highly interrelated—after all, it is only possible to use sites like Facebook because users provide so much information that advertisements can be targeted to specific users based on interests. But a focus on social aspects of privacy online enables scholars and teachers in rhetoric and writing to consider the social dynamics involved in reading and writing in social media environments.

Popular discourses tend to focus on protecting privacy online, or on people's lack of ability or attention to privacy in new media environments. As Browlee puts it, we need a "wake up call about privacy" online. Randall Stross, in his 2009 *New York Times* business column, writes that "the popularity of Facebook and other social networking sites has promoted the sharing of all things personal" to the point that "disclosure becomes the norm and privacy becomes a quaint anachronism." But privacy is not an anachronism online, or "dead" as many would claim, but is instead managed in relationship to publicity. Users of social media sites may share more private information and activities than before, but that sharing is always in tension with their own desires for privacy. Sharing information is never completely giving up one's privacy—it is the situated and rhetorical negotiation of visibility and withdrawal, disclosure and reticence (see Blatterer). A rhetorical approach, then, helps to situate how users share information and manage their privacy in digital environments by attending to the situatedness of an encounter with an interface. In other words, a rhetorical approach to privacy practices places privacy practices in context.

Privacy is, admittedly, difficult to define. As Daniel Solove, one of the most eminent legal scholars on privacy, explains, "privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogation" (*Understanding Privacy* 1). Because the concept is in

"disarray," as Solove puts it, it becomes difficult to articulate privacy problems, often "lack[ing] a compelling account of what is at stake when privacy is threatened" (2). Additionally, without a compelling and thorough understanding of privacy, it becomes difficult to understand privacy as a set of practices, leading large cultural shifts in privacy practices to appear improper, ill conceived, or foolish. Thus, in the first decade of the twentieth century, popular discourses were quick to blame youth for their indiscretions online, claiming blankly that they were sharing everything. Privacy is often understood in a limited sense as an individual property, as a right, which also leads these discourses to be concerned that we should protect privacy and that digital media are threats to privacy.

Because privacy can encompass so much more than simply protecting privacy or giving up information online, I draw on Solove, Judith Wagner DeCew, and Helen Nissenbaum in articulating privacy as a cluster concept that involves information privacy, spatial and bodily privacy, and expressive privacy, or the ability to express oneself and develop one's identity (DeCew 75-77). Understanding the concept in this way helps to investigate the various aspects of privacy as it is understood and practiced in digital media environments. For example, from a rhetorical perspective, we can see how Girls Around Me might be problematic because not only does it involve informational privacy (users have provided information to Foursquare and Facebook that they have made publicly available), but it also involves spatial privacy: Users of Girls Around Me now have access to Facebook profiles (which can be understood as an extension of the self) and the ability to make unwanted advances by sending Facebook messages. Further, a user of Girls Around Me can violate a woman's anonymity in a public space by going to the bar, restaurant, or club she is at.

A knee-jerk reaction to Girls Around Me would respond that Facebook and Foursquare users clearly don't understand privacy on these sites and have foolishly, ignorantly, or lazily made their profiles public. Discourses of control and protection abound when it comes to digital

privacy, and digital users are often to blame for not protecting their own privacy. This blame extends particularly to girls and women. In his blog post on Girls Around Me, Brownlee explained that the women featured in the app had "neglected" to make their Facebook profiles private "out of ignorance, apathy, or laziness." When Boston resident and self-described "health social media nerd" Marie Connelly discovered she was featured in the Girls Around Me image on Brownlee's post, she critiqued him for his blaming rhetoric, defending her choice to make her accounts public. She explained that she benefited from the social connections she had gained because of those decisions, and articulated a cogent critique of the rhetoric of risk and blame so ubiquitously used in privacy discussions:

> I don't believe that having a public persona online needs to be a risky enterprise, and it seems like plenty of people are able to manage that without being attacked, stalked, or otherwise targeted. If we're saying that's only true for one half of the population, then I don't think this is really a conversation about internet privacy as much as it's a conversation about whether it's safe to be a woman and live in public. (Connelly)

Importantly, discourses and practices related to privacy are gendered (as well as raced, classed, sexualized, and marked by different cultural norms and power differences), making the social and political aspects of privacy incredibly important to explore.

Why should rhetorical scholars care about privacy practices in digital environments? As more and more of us are online, using social media, how we manage privacy and relate to each other in these environments becomes increasingly important. As our students are probably the most frequent users of these sites, and as we ask students to engage in public rhetoric online, it is important to consider various understandings and practices related to privacy in digital environments. I take this stance because privacy is not just an individual good, but rather a public good, in that it helps to facilitate autonomy and sociability in a variety of ways. As numerous

privacy scholars have argued, privacy is important for creating social distance, for developing autonomy and performing identities, and for allowing for intimacy because people can determine what to share with whom (see Moore; Nagel; Murphy; Fried; Gerstein). Without strong understandings of privacy, both as a set of norms and as a descriptor of behaviors, it becomes hard to determine what is good for helping to facilitate identity development and performance online, how people build relations online, and what is useful for healthy public discourse. Privacy is important for identity construction, developing intimacy, and creating sociability.

Privacy is arguably in a moment of "crisis" in the public imagination. Perhaps more accurately, we might say that privacy is one of the *topoi* that citizens turn to, or one of the commonplaces they rely on, in order to represent and understand new technologies and their place in social relations. Rick Altman argues that when a new technology is created and adapted, "we find a *crisis of identity*, reflected in every aspect of the new technology's socially defined existence" (19). Altman calls for a "crisis historiography" that understands that new media are not simply composed of their technological components, but are instead defined in historically and socially contingent ways, "depend[ing] on the way users develop and understand them" (16). This does not mean that the technological components of new media are not deeply infused with social values (Winner); rather, how new media are discussed reveal and influence our understanding and anxieties around them.

By exploring practices and interfaces in addition to popular discourses, I follow two recent turns in rhetorical studies developed over the last decade. The first, an ecological approach to rhetoric, revises the long-held model of rhetor-message-audience for rhetorical action, instead understanding rhetoric as the situated, embodied engagement of a rhetor in an environment. Marilyn Cooper, Sid Dobrin, Jenny Edbauer, Barbara Warnick, and Collin Brooke have been influential to my understanding of rhetorical action as the use of words and tools to engage with our environments (Cooper, "Linked to the Matrix" 17, 29). Cooper is clear that "ecology" is not

just a new way to say "context": context has typically be understood as static and unchanging, something that a rhetor can fully comprehend or assess. Ecological approaches to rhetoric understand that environments are constantly changing and never static ("The Ecology of Writing" 368). This certainly applies to digital environments: Not only do services like Facebook often upgrade their features, but because users approach them for different purposes and at different moments in time, when others on the network are interacting in various ways, the interface is always under constant revision. Thus, we cannot analyze interfaces like we do texts. As Collin Brooke argues, turning to the interface for analysis means taking into account perspectives and practices of users (132).

The second strand of rhetorical scholarship that informs my approach here is the turn to rhetorics of everyday life. Following scholars like Ralph Cintron, Martin Nystrand, John Duffy, and John Ackerman, I attend to "the rhetorical character and dynamics of language in mundane contexts" and "the ways that individuals and groups use language to constitute their social realities, and as a medium for creating, managing, or resisting ideological meanings" (Nystrand and Duffy viii, ix). That is, I am concerned with the everyday use of language (and images) by users in their practices on sites like Facebook, Twitter, Foursquare and on various devices—their desktop or laptop computers, their cell phones for texting, their webcams for sharing video, their smart phones for network capability—in various places and contexts. How do users approach these sites, services, and devices and practice privacy in these environments? What does this mean for their social relationships?

One key argument of this dissertation is that managing one's privacy in social media environments constitutes a highly literate set of activities. Calling managing one's privacy online a "literacy" does not mean I advocate an ideal set of practices with certain levels of disclosure, visibility, reticence, and privacy online. A central problem with the term *literacy* is the historical weight it carries as a tool for enforcing proper behavior and privileged Western values (see

Wysocki and Johnson-Eilola). Instead, I follow literacy scholars over the last 30 years who have argued that literacy is contextual and social, not a simply the autonomous, mechanical encoding of symbols, but the use of language to engage in social situations embedded within cultural practices (e.g., Street 2; Grabill 24; Yagelski 9-10). Duffy extends this perspective by arguing that literacy practices are not just *social*, but *rhetorical*: Among other aspects, literacy practices and education help to shape the world, "promot[ing] a vision of the world and the place of learners within it," both constraining human freedoms and offering possibilities for change as social action ("Other Gods" 43; see also "Letters to a Fair City"). To argue that managing privacy online requires a highly literate set of activities, then, is to argue that managing privacy in digital settings is rhetorical, the use of symbols to engage in an environment.

The literacy practices and activities needed to manage privacy online are perhaps most exemplified in Facebook's interface for its privacy settings. In 2010, the *New York Times* reported in a dense infographic that a user would need to navigate 50 settings with 170 options in order to manage their privacy settings on Facebook (Gates). In a flow chart, the infographic shows how users would need to navigate to various different pages within Facebook in order to adjust these settings. Separate pages are available for contact settings, ads, personal information, search settings, and third-party applications. Users also need to navigate to individual photo albums in order to adjust their privacy settings for those. This infographic reveals the complexities of being able to manage one's privacy—among other users, from non-users, and for third party apps—on one single web site. Though now dated (Facebook has since updated its interface for managing privacy), the infographic reveals the complex reading and writing activities involved in managing privacy, especially for a long-time user who might want to change various settings: A user could spend hours navigating multiple pages in order to change the privacy settings for each photo album, create lists of friends who have limited access to posts, select who can have access to contact information, and so forth. A colleague of mine, for instance, spent hours teaching herself

how to navigate these pages and change her settings after she discovered her students could see publicly available images of her family through Google searches. And another, frustrated with how much time it would take to change his privacy settings for various social groups on Facebook, expressed that it might be easiest to just delete his account and start over. No wonder, then, that researchers have found that users were confused by Facebook's settings and were often either sharing or hiding personal information in ways they hadn't intended (Madejski, Johnson, and Bellovin).

Because privacy is both discussed in popular discourses and practiced in digital environments, I approach privacy and digital media through three methods: I explore how privacy and digital technologies are discussed in both public and disciplinary discourses, including newspapers, magazines, technology blogs, and scholarly approaches; how certain technological interfaces afford and make possible, as well as limit and shape, certain behaviors and conceptions of privacy; and how privacy is practiced by social media users in specific contexts and ecologies.

In order to explore the dynamics of privacy in digital environments, I turn to four sets of rhetorical practices in the body of this dissertation. Each of these sets of practices has caught public attention in some way, through moral panics or what Reynolds calls a "discourse of crisis" (*Geographies* 24). In chapter 2, I explore the uses of mobile devices in public spaces, which have often been responded to by a discourse of crisis that claims public spaces are dying and that users have lost a sense of place as they traverse digital elsewheres. Turning to these practices and the discourses about them affords me the opportunity to explore the *materiality* of privacy and how people use devices in their rhetorical ecologies in order to manage their availability—to create private spheres or to build relations with others.

In chapter 3, I turn to the case of Tyler Clementi, the gay Rutgers undergraduate who committed suicide in 2008. The case gained national attention because his roommate, Dharun Ravi, had spied on him using a webcam the same week as Clementi's suicide, and the situation

became a national story about invaded privacy and the dangers of cyberbulying. Attending to the various discourses before Ravi and Clementi met, during Ravi's spying, and after Clementi's suicide allows me to explore how *identity* is changing online, particularly through the digital traces left by posting private information online. Identity online becomes a matter of researching and building a digital identity about others based on searches for the various digital evidence provided online.

I then turn to the moral panic around "sexting," the sending of sexually suggestive or explicit images, videos, and texts via mobile phones, in Chapter 4, exploring how the "public pedagogy" (Giroux, *Abandoned Generation* 38) of sexting is gendered, disproportionately blaming girls and young women for sending a sext. Rhetorics of protection serve to blame victims, particularly girls and women, for making themselves vulnerable, or attempting mediated *intimacy* through digital environments, instead of focusing on the ethics of sharing others' private photos or videos.

In Chapter 5, I turn to *sociability* by exploring the 2009 Sundance award winning documentary *We Live in Public*, a film that chronicles the rise and fall of 1990s dot com millionaire Josh Harris and his experiments on surveillance, privacy, and digital media. This film and Harris's experiments are understood as a "warning shot" by producer Ondi Timoner and by reviewers for the dangers of lost privacy in social media settings. In this chapter I argue that Harris's experiments and the film ignore how bodies are actually practiced in social media environments. In fact, most claims about *sociability* on social networking sites tend to ignore actual, situated practices, and I conclude by calling for attending to the situated, embodied engagements with environments in order to explore sociability online.

This dissertation focuses on four concepts related to privacy through analyses of discourses, interfaces, and practices related to social media environments: *materiality* (Chapter 2), *identity* (Chapter 3), *intimacy* (Chapter 4), and *sociability* (Chapter 5). These four concepts are

intricately related to privacy and are central to a comprehensive understanding of the importance of privacy to rhetoric because they reveal how privacy is a central aspect of how we live our lives, online and off. While I use these concepts to frame discussions in each chapter, making analytic distinctions among the terms, I stress that they are intricately tied to each other and coalesce to encompass many aspects of the complex and dynamic ways that privacy functions.

Throughout this dissertation, I call attention to the materiality of privacy—that is, how it is not just about information, but is an embodied practice in relation to space and place. Rhetorical scholars have recently turned to the material and bodies, including rhetorical understandings of spaces and geographies (e.g., Reynolds, *Geographies*; Ackerman; Dickinson), the materiality of writing (e.g., Haas, *Writing Technology*), the involvement of bodies in aesthetic engagements with texts (e.g., Wysocki), and the connections between rhetorical education and bodily training (e.g., Hawhee, "Rhetorics, Bodies, and Everyday Life"). Among those scholars, Nedra Reynolds and Christina Haas both explain that privacy is a material practice (as I will discuss later in this chapter). A focus on information privacy and digital communication can often lead to ignoring how privacy is materially practiced—not just a disembodied engagement with a screen that takes us away from our bodies and the places we are residing in, but rather a fully engaged, embodied experience and interaction with both screens and physical environments. Indeed, as I explore in chapters 2 and 5, bodies as they are practiced are often ignored, even by those who claim, as literary critic Zadie Smith does, that we are losing a sense of our bodies as we reduce our identities to data online. This sort of view relies on a belief that bodies are experienced, but we need to understand bodies as things we practice.

In this chapter, I begin by discussing the three terms central to this project: *social media*, *privacy*, and *rhetoric*. I define social media as the type of digital media that encourages many-to-many communication, in contrast to personal one-to-one media and broadcast, or one-to-many communication. Importantly, social media have certain technological affordances that allow for

shifts in privacy practices in contrast to privacy in spaces or in print: Information is easily aggregated, is recorded (perhaps indefinitely), is easily replicated and searched, and can thus easily reach more people. Additionally, the technological features that Nissenbaum explains make threats to privacy easier in digital environments: the monitoring and tracking, aggregation and analysis, and dissemination and publication of data (20). From there, I turn to disciplinary understandings of privacy, exploring how rhetorical scholars have approached privacy in previous scholarship before advancing a notion of privacy as a cluster concept. I then discuss what I mean by rhetorical ecologies, drawing on a growing body of scholarship that understand rhetorical action as an embodied engagement with one's environment.

In the remainder of the chapter I begin to develop my argument about the social and rhetorical dimensions of privacy by explaining the four ways in which privacy is rhetorical—the term frames debates, it is used as a commonplace in order to make arguments, privacy is a set of practices in environments, and environments encourage certain understandings and practices of privacy. I then turn to Facebook, perhaps the paradigmatic social media site, in order to explore one way in which privacy is increasingly social online: While discourses about privacy, including Facebook's privacy policy, stress control over information, control over access to information is actually distributed throughout one's online social network. That is, others' privacy settings and practices help to determine how accessible your expressions and information are online. Because Facebook is so immensely popular and because privacy policies on the site have changed so many times since its beginning in February 2004, the site has been the focus of much mass media attention over the last decade or so. I turn to these popular discourses, exploring three strands that will recur in my analyses throughout this project: nostalgia for face-to-face communication, a moral crisis about youth's anti-social activities, and the coordination of this moral crisis with a literacy crisis.

"Social Media" and Technological Features that Affect Privacy Practices

The term *social media* is often used to describe a wide variety of digital media, most often in contrast to broadcast media (e.g., books, newspaper, radio, film, television shows) and one-to-one communication (e.g., letters, telegraphs, telephone conversations). The term is admittedly misleading, as all media are social in that they mediate relationships between and among people. In many ways, the term *social media*, like its associated term *social networking site*, is used without a clear definition. I define *social media* loosely and broadly as *digital media that encourage through their designs the practices of many-to-many communication*. That is, social media is characterized not by broadcasting from one source to a mass audience, or by one-to-one communication, but by the possibility of many communicating to many in a digital environment. A good example is Twitter, a service that allows users to post messages, or "tweets" of 140 characters or less. While in a sense users broadcast these tweets to their followers, it is more accurate to say this is an environment for many-to-many communication. A user's tweets are embedded in a stream of tweets from many users (those he or she follows), making an environment where reading and writing occur concurrently: As I post to Twitter I am also reading communication from my followers.

In this dissertation, then, I use the term *social media* out of rhetorical convenience because it is a recognized term deployed in popular and scholarly discourses to describe the types of digital media I am concerned with in this project. Social media holds an uncomfortable place in many people's imagination, as it disturbs the previous dichotomy between broadcast and personal communication. Clay Shirky notes that the distinction between broadcast and personal communication blurs with social media and leads to confusion about the nature of messages: "since we're so unused to communications media and broadcast media being mixed together, we think everyone is now broadcast" (87). However, social media users are often not broadcasting an

impersonal message, but also might not be sending personal one-to-one communications; instead, social media calls into question an old assumption about media: that we can tell the distinction between a personal and an impersonal message simply by the type of medium in use (87). Social media, then, are defined by the ways in which they encourage many-to-many communications that may be personal or impersonal (or both, sometimes at the same time). Because readers may be unfamiliar with many aspects of social media, here I'll describe social media, provide some examples, and discuss some of the technological features that are important to issues of privacy on these sites and services.

Social media is often defined by certain characteristics that distinguish them from other digital media. Though they use the term "social network sites" instead of "social media," Danah Boyd and Nicole Ellison's definition is useful in describing some typical characteristics of social media.[1] They explain that social networking sites "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). Importantly, the structure of those profiles, connections, and ways for traversing the system can vary widely from one social media service to another. Thus, a wide variety of services or websites can count as social media:

- Social networking sites, like MySpace, Facebook, Google Plus, and Friendster, which allow users to create a profile and to connect their profile to other users through creating lists of "friends" (which are mutual connections). Some social networking sites, such as Facebook and Google Plus, include a homepage that aggregates updates from your

[1] Boyd and Ellison use "social network site" instead of "social networking site" because they feel that "networking" mischaracterizes these sites as the word "emphasizes relationship initiation, often between strangers," whereas many social media sites are used among already established social circles.

friends into one page, and most include features that allow for private messages between users or in groups.

- Location-based services, such as Foursquare and Gowalla, which include user profiles and lists of mutual friends. These sites are generally used to "check in" at a location, involve rewards (often "points") for checking in, and allow users to see where their friends are located if they've checked into a place.
- Blogging services, like Blogger, LiveJournal, and Xanga (now defunct), which allow users to keep a blog and develop lists of either friends or blogs they follow.
- Microblogging services, like Twitter and Tumblr, which are similar to blogging services except that posts are typically shorter and features are usually included for replying to content (instead of leaving a comment on a blog post) and reposting others' content.
- Sites for sharing and discussing specific types of media that users are consuming, like Goodreads (for sharing book reviews) and Last.fm (for sharing what you're listening to), which typically include profiles, lists of books or musicians that users like, and the ability to follow or friend other users and comment on their reviewers or profiles.
- Online dating services, like OKCupid, Skout, and Grindr, which can be used for meeting romantic partners or for casual sexual encounters. These sites or mobile phone apps allow users to create profiles, search through others' profiles, and send private messages. Some allow for uploading various content (particularly photos) that other users can comment on, and many offer the option to mark other users as friends.
- Photo-sharing services, like Flickr, Instagram, and Twitpic, which provide a platform for users to share photos, either publicly or with those who follow them or are friends. While some of these services can be used on their own, others were created to be integrated into other services. Twitpic, for instance, requires a Twitter account and creates a tweet (140-character missive) that describes and links to the picture a user posts.

- Video-sharing sites, like YouTube and Justin.tv, where users upload videos, have profiles and channels (that list all their videos), create lists of friends or channels to follow, and comment on videos. Some, like Justin.tv, include the option to broadcast live with simultaneous chat features, while others, like YouTube, require pre-recorded videos to be uploaded.

What these sites and services generally share is the ability to create profiles, build a network, and traverse through others' profiles and content. Increasingly, these sites can be accessed from both computers and mobile phones that have network connectivity, as many of these services have mobile apps. Additionally, many of these services allow integration, meaning that content can be optionally or automatically loaded from one site onto another. For example, Instragram, a photo sharing service that allows users to upload and alter photos by applying a filter, has the option to also post the photo to Facebook and Twitter. This integration is possible because of APIs, which allow developers to use the code of a service to connect two services (which is what made the iPhone app Girls Around Me also possible), and because of how micro-content is coded, allowing for videos or images to be easily embedded in other sites using HTML code (and increasingly, by clicking links like "post" or "share").

Digital technology on these sites allow for content to be more visible, more easily shared, and more easily searched, affordances that affect shifts in privacy practices online. Danah Boyd explains that social media sites have four features that affect sociability: 1) the persistence of data and expressions, in that communication on these sites is recorded and archived; 2) the replicability of content, meaning that content is easily duplicated and posted elsewhere within a service or between services; 3) the scalability of content, meaning that the visibility of a user's content and network is great and that content can easily reach a broad audience; and 4) the searchability of content, which allows users to search and find profiles and content quite easily ("Social Network Sites as Networked Publics" 45-48). Importantly, these features allow for

invisible and convergent audiences, meaning that content might be available on some of these sites to audiences without the awareness of the individual poster. This aspect of convergent and invisible audiences is particularly true for sites that allow for more visibility, or for sites where users' various social lives converge (for instance, on Facebook, where many people friend family members, friends, acquaintances, and co-workers).

These affordances and the structures of social media are spreading to other digital media that in the past worked more like one-to-one communication. For instance, chat clients are increasingly functioning like social media, allowing for group chats instead of individual conversations between two users. While some chat clients have always allowed for multi-user chats—ICQ, the first chat client available Internet wide, provided this feature—the feature is increasingly common and being developed for chat clients that previously did not have this feature. Google's chat feature, integrated into its email system and its social networking site Google+, now allows for multi-user text chat and video chat. Another digital media, Short Message Services (SMS) on cell phones, commonly referred to as texting, is becoming increasingly like social media. Whereas a mass text could be sent from mobile phones in the past, Apple's iPhone now has a feature that allows users to reply all when they are mass texted. Increasingly, the abilities for groups to communicate with each other is becoming easier as many-to-many communications are becoming easier in digital environments.

Helen Nissenbaum offers a different schema for approaching privacy concerns in digital environments, one that focuses on the technological functions that make threats to privacy more possible than it might be in physical spaces. Facebook serves as a paradigmatic social media site, as it is currently the largest service, with over 845 million active users as of December 31, 2011 ("Fact Sheet") and draws more web traffic in the United States than either Google's or Yahoo's services ("Facebook Inches"). Additionally, it has drawn the most media attention over the last few years for privacy concerns online. Facebook is exemplary for its uses of technological

features that allow for the sorts of challenges to traditional understandings of privacy. Three technological functions, as Helen Nissenbaum outlines them, converge in Facebook in ways that afford threats to privacy:

1) *Monitoring and tracking* online involves the automated collection of data through a variety of mechanisms and for a variety of possible purposes—for example, surveillance for control, data collection for marketing. Whereas in offline situations monitoring and tracking requires much material and invasive technologies, online it can be automated to the point that "Every interaction is like the credit card purchase," including IP addresses, clicks on links, cookies, and more (Nissenbaum 28, chapter 1). Facebook and other social networking sites use monitoring and tracking in order to direct advertisements to users and to understand their user base in order to make the platform more user-friendly or to develop new features for the site. Additionally, Facebook's interface makes it easier for users to monitor and track each other; for example, users "Facebook stalk" each other in order to learn more about new acquaintances or potential dating partners (Raynes-Goldie).
2) *Aggregation and analysis* refers to the ability to store, retrieve, organize, and analyze information quickly and easily. This ability is made possible by recent technological developments in cheap computer memory, faster processing power, networked computers that allow for fast and easy transfer of information, and analytic developments in information science (Nissenbaum, chapter 2). These developments, which are implemented on Facebook, allow for the aggregation and analysis of data in a multitude of ways, so that advertising can be directed at users, friends can be suggested, and the News Feed can deliver updates on Facebook's homepage. Users also make use of aggregation, finding new friends more easily, creating friends lists, making use of the News Feed, and more.

3) *Dissemination and publication* speaks to ease in the ability to post and spread information, especially online (Nissenbaum, chapter 3). This can be as simple as the ability to quickly post a Facebook status update, to write on a wall, or to post pictures, but also speaks to the ease in replicating and disseminating information: clicking the "share" button on Facebook, the ability for videos to go viral, for information to be shared and quickly be posted on various pages, sites, and forums. Facebook is paradigmatic of the technological ability to quickly post, publish, and spread information.

These categories are not meant to be discrete; in reality, they often overlap. For instance, the aggregation of data also allows for ease in tracking and monitoring of others, as information can be aggregated into one more accessible place (such as a user's Facebook wall). But for analytic purposes, the categories are helpful in understanding how the technologies that make Facebook possible also make threats and violations to traditional understandings of privacy more possible.

Disciplinary Views of Privacy: Five Strands

While various scholars in rhetoric and composition have examined privacy issues, their approaches have typically, with a few exceptions, been ancillary to larger studies, or have discussed privacy in rather limited ways. In the field, privacy is generally discussed in one of five ways: 1) The first way rhetorical scholarship has discussed privacy is as a material practice in relation to place or space. This strand of scholarship sees the public/private distinction as embedded in how we understand place and space and influential to material practices. (Reynolds, *Geographies*; Haas, "Materializing"). 2) A second strand of scholarship understands the public/private distinction as a dichotomy that shifts with the development of new media. Scholars in this area explore how the ways that people have historically and currently discussed and used new communication technologies have shifted understandings and practices of the public/private

distinction (Baron; Miller and Shepherd; Marvin; Stubbs; Blake). 3) A third group of scholars understands privacy as an aspect of ethics that needs to be respected and protected. While these scholars also understand privacy as a shifting and contextual notion, they largely focus on how activists argue for protecting their privacy online, how researchers need to respect others' notions of privacy, and how a strong critical literacy online involves protecting one's privacy online (McKee and Porter; Markel; Gurak, *Persuasion and Privacy*, *Cyberliteracy*). 4) In another approach, feminists in rhetorical studies have explored the historical and current gendered nature of the public/private dichotomy, understanding privacy as feminized: it has long meant the domestic and the personal, and has thus been undervalued in rhetorical scholarship. Feminist rhetorical scholars have argued that the public/private distinction needs to be disrupted or re-imagined in order to revalue the rhetorical contributions of women (Ede, Glenn, and Lunsford; Glenn). 5) Finally, rhetoric and composition scholars have approach privacy and the private as a threat to public rhetoric: Private lives expressed in public can lead to the validation of private, authentic identities rather than and opportunity to change identities and discuss public issues (Couture; Dobrin, "Going Public"). These five strands of rhetorical scholarship contribute to a rather dynamic understanding of privacy in relation to rhetoric.

The first strand of rhetorical scholarship that addresses privacy explores how it relates to material practices and conceptions of space and place. Christina Haas and Nedra Reynolds have perhaps been most influential in helping rhetorical studies understand the public/private dichotomy; they see it as influential to material practices, particularly in relationship to place and space. Haas's study of the material representations of the public/private dichotomy in a court injunction at an abortion clinic in Ohio reveals how the public/private distinction is often invoked and discussed in spatial terms, making the delineation "a kind of material practice" ("Materializing" 232). Her analysis of how "public" is described in terms of the metaphor of "place" by Hannah Arendt, Jürgen Habermas, Nancy Fraser, the U.S. Supreme Court, and the

specific injunction she studies reveals how privacy becomes understood in spatial terms, as a material space not to be violated. For example, Haas shows how the Supreme Court has increasingly spatialized privacy, defending it in terms of a "zone or privacy" that is protected from government "intrusion" (230-231). Reynolds's study of reactions to cell phone uses in *Geographies of Writing* contributes similarly to the material understanding of the public/private distinction. Reynolds argues that cell phone use in public confuses people's notions of public and private because of our material understanding of certain places and spaces as being public or private. She explains, "It is not the technology that is the culprit but ideas about space that cause the attitudes toward cell phone use" (22).

While Haas and Reynolds focus on the materiality of privacy, a second strand of rhetorical scholarship focuses more on conceptions of privacy and the shifting notions of the public/privacy distinction in relationship to developing new media. These studies contribute to an understanding that shifting notions of privacy are hardly anything new, but that notions of privacy shift in specific historical contexts, not solely because of new technologies, but because of how these technologies are used, discussed, and understood. In his broad-sweeping study of the adoption of new communication technologies, Dennis Baron makes the point that "each new communication technology remixes our notions of public and private, bringing the public world into previously private space and exposing the private to public scrutiny" (xv). That is, new communication technologies disrupt boundaries between public and private, sometimes by making private lives more accessible to others, or by making public communication more available in private spaces. Carolyn Marvin, Katherine Stubbs, and Erin C. Blake all contribute to this understanding of shifting notions of publicity and privacy through analyses of historical developments of new media. Blake's analysis of the uses of the zograscope reveals how it allowed for the enjoyment of public space within the private sphere of the home in eighteenth-century England (20), and Stubbs's analysis of literature about the telegraph in the nineteenth

century shows anxieties about women's increased publicity and visibility as telegraph operators (98-100). Marvin's thorough analysis of the dramas around the adoption of telephones and electricity reveals how these new technologies challenged the boundaries between public and private knowledge, allowing for the exposing of family secrets (64, 68), but also how these technologies were domesticated in order to protect the intimate sphere of domestic life (76-80). More recently, Carolyn Miller and Dawn Shepherd explore how blogs blur the distinctions between privacy and publicity, as they argue that blogs are a genre that allow for the validation of a private self in public. These historical and contemporary studies assist us in understanding how communication technologies and their uses affect conceptions and practices of the public/private distinction in situated ways.

The third stand of rhetorical scholarship that addresses privacy explores it in terms of ethics: as something that should be respected or protected. These studies often understand that privacy can be understood differently by different people or in different contexts, but often approach privacy as something that activists seek to protect, that students need to protect from companies online, and that researchers need to respect. Laura J. Gurak's 1997 study of online activism protesting the development of the Lotus Marketplace and Clipper chips and their invasion of privacy explores how online activists were interested in protecting their privacy. While her study contributes greatly to understanding the rhetorical features of community ethos and delivery online (*Persuasion and Privacy* 5) and she admits to the vague and complicated nature of the term *privacy* (46), Gurak understands privacy largely as something to be protected. Her later project on cyberliteracy also focuses on privacy as something to be protected: teaching online literacy, she argues, can help "Internet users to question the privacy issue: to reject sites that don't have clear privacy policies and to lobby their representatives for more comprehensive approaches to privacy and technology" (*Cyberliteracy* 12). In a chapter on "Privacy and Copyright in Digital Space," Gurak focuses on protecting privacy from data collection through

cookies and being aware of laws and critical of laissez-faire economic models that give companies a lot of freedom to use information they have collected (110-127). Similarly, in his analysis of websites' privacy statements, Mike Markel shows how many websites obfuscate their privacy policies and are unethical according to a rights model of ethics. In perhaps the richest exploration of privacy, Heidi A. McKee and James E. Porter's *The Ethics of Internet Research* explores how notions of privacy are culturally specific and that those notions may lead to researchers having different expectations of privacy than those they are studying (46). They urge readers to not let Internal Review Board procedures and perspectives cloud the ethical conundrums of differing notions of privacy online (41). Their rich discussion is useful in problematizing notions of "published" as "public" (77), but like other studies on privacy, their book focuses solely on privacy as something that should be respected or protected.

The fourth strand of rhetorical scholarship that addresses privacy comes from feminists who question and attempt to disrupt the gendered aspects of the public/private distinction. Feminists have long questioned the gendered nature of the terms *public* and *private*, which have historically equated public with the rational, the market, and politics (and thus masculine), and private with the emotional and domestic (and thus feminine). In their exploration of how feminism and rhetoric intersect and transform each other, Lisa Ede, Cheryl Glenn, and Andrea Lunsford discuss how the public/private distinction becomes a double-bind for women seeking transformative, feminist change: In order to gain ethos, feminists must adhere to stylistic standards of Western academic prose, which devalues the personal; but in order to effect change, a turn to the personal is important (423-424). Ede, Glenn, and Lunsford also explore how women have been excluded from public venues and how more private means of delivery have been devalued in the field. In the words of Barbara Biesecker, "Rhetoric is a discipline whose distinctive characteristic is its focus on *public* address, a realm to which women as a class have historically been denied access" (qtd. in Ede, Glenn, and Lunsford 430). Glenn makes the

historical nature of the public/private dichotomy and its affect on rhetorical studies clear in her book *Rhetoric Retold*. In order to explain an aspect of the reasons women have been excluded from the rhetorical tradition, Glenn outlines the ancient Greek dichotomy of the *idios*, or the private realm that included the *oikos*, the domestic sphere, and the *polis*, the public realm of rhetoric (1). According to Glenn, women have been silenced and made invisible within the rhetorical tradition in part because of the field's (masculine) value in the public and because the *idios* remains "seldom-examined" (1). This feminist strand of rhetorical scholarship explores how the public/private dichotomy is gendered and related to power: the exclusion of women from public discourse and the devaluing of private discourses (like letter writing and translation).

The fifth strand of rhetorical scholarship that addresses privacy approaches private discourse as the type of discourse that is harmful to public discourse because the sharing of private lives in public causes us to focus on identities, promoting self-authenticity, rather than on issues and the possibility for changing identities. In her introductory chapter to *The Private, the Public, and the Published: Reconciling Private Lives and Public Rhetoric*, Barbara Couture argues that the "increased fusing of the private and public does not bode well for public rhetoric; it does not lead to expression that contributes to the public good," and in fact "obliterates the possibility of public rhetoric" because we don't relate to each other in ways that are productive for changing ideas and identities (2-3). As Couture explains, the impetus to share private lives in public and the conflation of private and public causes very real problems for identification and communication, demanding "that the audience absorb, deny, refuse or obliterate difference" (4). Put differently, the sharing of private identities in public changes the nature of rhetoric in public: Instead of developing "some shared understanding of what it is to be human," rhetors instead focus on identities (4). And that focus on identities does not allow for debate about identity; public rhetoric needs to be a place where identities are "challenged, changed, and expanded by virtue of contact with others in a public forum" (8). In another approach, Sid Dobrin argues that

writing assignments that ask students to express their feelings as private feelings is "abhorrent." It is disempowering for students because they need the opportunity "to make decisions about their public discourse participation," not express their feelings as private in ways that reinforce self-authenticity ("Going Public" 229). Dobrin isn't against self-expression; rather, he is against the sort of sharing of private lives that doesn't place those private moments in relation to public discourse—that is, the sharing of private lives in public that serves as therapy or reinforces the notions of "students' own true self" (226).

In my review of these five strands, I am not claiming that there is anything necessarily wrong with any of these approaches. In fact, I find them useful as rhetorical studies begins to contemplate the rhetorical nature of privacy, especially in relationship to new media technologies. These scholars have begun to develop an understanding of the material and social dimensions of privacy and stress the very real and important necessities to respect and protect privacy as an ethical imperative for researchers and users of technologies. What I would contend, though, is that studies of privacy in rhetoric have not yet investigated fully the rich and complex nature of privacy, especially its social complexities in social media environments and practices in these environments.

What is Privacy in a Digital Age? A Cluster Concept of Privacy and Common Misconceptions

Privacy has become such a concern in digital settings and yet many are unsure what to do about it. Various commentators have been concerned that privacy is in fact dead online. In their response to Mark Zuckerberg's explanation of privacy changes on Facebook in 2010, the blog *ReadWriteWeb* hyperbolized his claims about the changing nature of privacy, paraphrasing him inaccurately in a post titled "Facebook's Zuckerberg Says The Age of Privacy is Over" (M.

Kirkpatrick). Michael Arrington on *TechCrunch* has argued that people shouldn't be concerned about privacy on Facebook: They like Facebook, and, well, "The fact is that privacy is already really, really dead" because individuals have already given up so much information to corporations. Others have also chimed in that privacy is now dead (see, for example, Garfinkel; see also Solove, "Speech, Privacy, and Reputation on the Internet" 20-21, for further critiques of this claim). In her analysis of terms of service documents for virtual worlds, online games, and social networking sites such as Facebook, Debra Halbert argues that "in virtual worlds, there is by definition no privacy" and that the term is "an antiquated concept" in these spaces.

What exactly *is* privacy, and can it still exist online? Those who claim that privacy is dead or antiquated mistake changing practices in relationship to privacy for privacy's end, and while technological changes and uses of technologies have certainly made protecting privacy more difficult, "It is still possible to protect privacy, but doing so requires we rethink outdated understandings of the concept," in the words of Daniel Solove ("Speech" 20). I follow Solove, Judith Wagner DeCew, and Helen Nissenbaum in understanding privacy as a "a broad and multifaceted cluster concept" (DeCew 61) that involves control over accessibility to and the flow of information, access to one's body and personal spaces, the ability to express oneself for identity development—all for "relief from a range of kinds of social friction" (Solove, "A Taxonomy" 484). As Solove explains, privacy isn't a coherent concept, but is rather more a Wittgensteinian term: a cluster of concepts that share resemblances with each other (*Understanding Privacy* 42-44). It is important to keep in mind that any specific content is not automatically or *a priori* considered private. Instead, it is determined to be private in specific contexts and depending on one's perspective. For instance, a Facebook wall post may be private in the context of a parent-child relationship if the parent is not in the child's network but is not private to the rest of the child's social network. Privacy, then, is a social and contextual concept that helps to facilitate identity formation and relationships with others.

Privacy has a contextual quality that is understood and practiced differently in different social, historical, and cultural contexts. For Western culture, privacy and the private have a long intellectual history, including Aristotle's famous distinction between the *polis*, or the public arena open to all free citizens, and the *oikos*, the private sphere of the home. Liberal tradition that the private life must be protected by the state develops in John Locke's 1690 *Second Treatise on Government*, where he argued that the state was necessary to protect private ends (see Habermas 3; DeCew 10-11). More recently, the concept of a right to privacy emerged in response to new, developing communication technologies. Samuel D. Warren and Louis D. Brandeis's 1890 article "The Right to Privacy" offered the groundwork for incorporating a right to privacy into tort law. Written in response to developing high-speed cameras and the increased circulation of newspapers, Warren and Brandeis argue that these new technologies "have invaded the sacred precincts of private and domestic life" (76). They thus argue for a right to privacy rooted in common law meant to protect "inviolate personality" (82). State tort laws and federal constitutional law followed throughout the twentieth century, often in response to new communication technologies like telephones, polygraph tests, HIV tests, cell phones, and video surveillance (see DeCew, Ch. 1). As Dennis Baron, Carolyn Marvin, Carolyn Miller and Dawn Shepherd, Erin C. Blake, Katherine Stubbs, and various other scholars of communication technologies have shown, new communication technologies often encourage shifts in practices of privacy and publicity, often resulting in anxieties about those shifts.

These shifting practices of privacy point to the need to understand privacy as contextual, as rhetorical. As Lloyd L. Weinreb explains, privacy is contingent on communities, within communities, and on circumstances (42). Nissenbaum offers the concept of *contextual integrity* to help show the contextual nature of privacy: Privacy norms vary from context to context, dependent upon "the types of information in question; the respective roles of the subject, the sender (who may be the subject), and the recipient of this information, and the principles under

which the information is sent or transmitted from the sender to recipient" (127). In many ways, Nissenbaum's framework of contextual integrity for privacy map onto rhetorical understandings of communication.

Five common conceptions about privacy often get in the way of thinking about privacy as contextual and a cluster concept, especially in online settings: 1) it is often understood in relation to its counterpart publicity, as that which is not public; 2) relatedly, it is often understood in terms of secrecy or undocumented information; 3) it has been understood as the ability to control information about oneself; 4) people focus mostly on information privacy, sometimes at the expense of issues of access to the self or expressive privacy (especially in our information age); and 5) many consider privacy solely in terms of freedom from a Big Brother style surveillance.

Common Conception #1: Privacy as Not Public

The public/private distinction often limits our ability to understand privacy in nuanced, contextual, and social ways. As Jeff Weintraub explains, privacy often brings to mind the public/private distinction, which is often understood in terms of either visible versus withdrawn or hidden or collective versus individual. Thus, when people discuss privacy, they often either explicitly or implicitly invoke public, making it seem as though if something is not fully individual, it must be collective, or if something is not fully withdrawn and hidden, it must be visible to all (4-5). These dichotomies are limiting in fully understanding privacy, as they ignore the contextual and nuanced nature of privacy and rely on binaries that might not be useful given a particular context.

Despite objections to the public/private distinction, the dichotomy still holds strong for many considerations of privacy. In his influential article "Privacy, morality, and the law," W. A. Parent defines privacy as "the condition of not having undocumented personal knowledge about

one possessed by others" (269). He argues that information that is documented in the public record (such as periodicals) cannot be called private, and that invasions of privacy only occur when undocumented information about someone is accessed. Anything that is not both personal and undocumented "cannot without glaring paradox be called private" (271). However, this conception is not sensitive to differing technologies and does not take into account what a society or group decides is documented and considered public (Moore 217-218). Nissenbaum offers the example of Lotus Marketplace: Households, a planned CD-ROM database by Lotus Development Corporation and Equifax, Inc. that would aggregate data for marketers and mail-order companies in the 1990s, to show how documented, public information can still be considered private by individuals. Faced with a public outcry (an estimated 30,000 email complaints), Lotus cancelled the project, but the resistance to the database shows that publicly available information can still be considered private (Nissenbaum 119-120; see Gurak, *Persuasion and Privacy*, for a discussion of Internet activism in this situation). For a more recent example, many people are disturbed to find that Web sites like spokeo.com and pipl.com aggregate publicly available data into one database. These Web sites take publicly available information, such as contact information from public Facebook profiles, and aggregate them into larger databases, making one's past and present addresses, phone numbers, and family members more accessible. Many find these sites an affront to privacy not because the information isn't already public, but because it is aggregated into a new place that makes it more easily accessed. In another example, as Maranto and Barton explain, students may see a teacher viewing their Facebook profile, even if it is public, as an invasion of their privacy.

Common Conception #2: Privacy as Secrecy

The common understanding that privacy is secrecy depends on this public/private distinction, and limits a robust understanding of privacy because it depends on this either/or dichotomy. The view that private information must be secret is still pervasive in law. Courts often contend that once information is no longer secret—once it is accessible to others—it is no longer considered private. This view fails to take into consideration access to information, especially how information can be aggregated easily and made differently accessible to more people (Solove, "A Taxonomy" 505-511). However, we know that secrets can be told and still be viewed as private. Solove explains that "Information about an individual [. . .] is diffused in the minds of a multitude of people and scattered in various documents and computer files across the country" (*The Digital Person* 43). That is, private information can still be shared and does not have to be considered secret. How and to whom information is concealed, revealed, or accessed matters: One might post their prior jobs on Facebook, but wouldn't want this information aggregated in a directory on another Web site. Privacy needs to be understood as contextual.

Common Conception #3: Privacy as Control over Information

The fact that information can be shared yet still be viewed as private leads to the next common perception of privacy that limits our ability to consider the concept in its full complexity: We often conceive of privacy as the ability to control information. But, as Nissenbaum explains, privacy is not simply a "right to control information about themselves," but instead "ensuring that it flows *appropriately*" (2). Definitions of privacy that rely on control over information fail to take into account the fact that just because someone shares information, their privacy is not being invaded or violated (Parent). They might not have control over the information, but they are

probably concerned about how that information travels. Taking into account access allows for the consideration of how people share information and expect it to flow. Telling someone something in a face-to-face conversation is different from revealing that information in an email, which is different from a hand-written letter: We have different expectations about how that information will flow. Thus, an important aspect of privacy is not merely control over information (though this is important as well), but control over how information is accessed and how information flows. So, again, privacy is always contextual: We must understand privacy in terms of the context it is in as to whether something is perceived to be private or not—or to whom and how it is desired to be private.

This distinction over control is perhaps what most clearly separates privacy concerns from property concerns. One's privacy is about limiting access to one's self, behavior, information, or spaces, whereas property is defined by ownership, and thus control over information and material goods. We do not own behaviors that we do not wish others to observe or know about, nor do we own our bodies (DeCew 54). As Jean L. Cohen argues, an important development in the understanding of personal privacy in the twentieth century was that privacy was differentiated from personal property. As she further explains, we "must replace the possessive-individualist conception of the relation of self and body" with an embodied understanding of privacy in which bodily integrity is privileged as protected by privacy and central to one's identity (159). Privacy, then, is not about control over property. The distinction between privacy and property also helps us see why users are likely to give up intellectual property rights to information (say, pictures on Facebook), but can still view these pictures as contextually private (say, outside the gaze of parents). Users chose to give up their control over information—Facebook now has that control—but have not given up their ability to manipulate access to that information.

Common Conception #4: Privacy as Solely Information Privacy

My mentioning of bodies above leads to another factor that limits a critical understanding of privacy: the focus on information. Understandably, social media sites focus on information; that is what they are collecting and disclosing. However, as DeCew argues, focusing solely on information ignores other aspects of the cluster concept of privacy: access to the self, including physical bodies and spaces, and expressive privacy, which she describes as protecting "a realm for expressing one's self-identity or personhood through speech or activity" (77). Understanding privacy solely in terms of information misses much of what else could be considered private in contexts: our bodies, our homes, and our activities. These aspects are important, especially for considering our inviolability and for considering the social aspects of privacy. Expressive privacy allows for the development of autonomy and for building relationships with others outside by limiting social control from others over decisions, speech, and behavior. It cannot always be reduced to information (a simple example of this would be that people may know that a couple is having sex, but that couple would not want others watching them have sex). Thus, as we consider how social media sites like Facebook conceive of privacy and encourage or discourage certain practices related to privacy, we should be cognizant not only of how information is collected and flows, but also concerns about access to the self and access to activities and speech. For instance, viewing a wall post or the joining of a group on Facebook as solely information, rather than also as an activity or expression, might miss the desired expressive privacy for that activity—the ability to make decisions free from interference or pressure. Facebook's chat feature allows for other users to know when and for how long someone is on the site—and to have access to not just that information, but that person's time as well. Or, to take the example I opened this dissertation with: A reason Girls Around Me seems so creepy is it provides the opportunity to invade both physical and virtual spaces. By knowing where someone is, without their knowledge, one can

also invade their personal physical space, even if they are in a public venue. And, by allowing users to send Facebook messages, the app allows for an invasion of privacy from unwanted messages.

Common Conception #5: Privacy as Freedom from Big Brother

Last, a critical approach to privacy is discouraged by common perceptions of surveillance, especially the metaphor of George Orwell's Big Brother, a concept Solove critiques for its failure "to focus on the appropriate form of power": The metaphor focuses on surveillance rather than data collection and manipulation. Surveillance is practiced and depends upon judgment and control of what is observed, but most collected data is not used to control others, but to study and exploit them (*The Digital Person* 34-35). Instead of the Big Brother metaphor, Solove draws instead from Franz Kafka's *The Trial* in order to understand privacy concerns: "Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process" so that individuals don't have "meaningful participation in decisions about our information" (38, 39). In short, the Big Brother metaphor of surveillance is misleading in digital settings because the real problem is not that there is one corporation or government surveilling us, but rather that we do not quite know how information is collected or for what purposes. Furthermore, surveillance isn't conducted so that others can control us—it is conducted in order to understand and exploit us.

Surveillance in social networking sites can be further understood through Anders Albrechtslund's concept of "participatory surveillance" (a term also used by Mark Poster in chapter 3 of *The Mode of Information* to describe how users contribute information to databases to participate in their own surveillance). Albrechtslund uses the term to explain how a hierarchical understanding of surveillance, like the Big Brother metaphor, favors the person or

institution doing the surveillance: "The person under surveillance is reduced to a powerless, passive subject under the control of the 'gaze.'" But in social networking sites, he explains, surveillance among participants is not about creating powerless subjects, but instead "can be part of the *building* of subjectivity and of making sense in the lifeworld." Jason Farman adds that this participatory surveillance is reciprocal: participants are both watched and watchers. This reciprocity breaks down when one is solely a voyeur (who is not gazed upon) or when one is solely watched, which is "read as a loss of agency" (70). Participatory surveillance online allows for reciprocal identity construction and the ability to engage with each other. When reciprocity doesn't happen is when users have a sense for the need for privacy, to "create spaces in which reciprocity will be achieved with those who will read us as we 'write ourselves into being' rather than being interpellated as a particular type of subject (such as a consumer)" (Farman 72).

Understanding privacy as a cluster concept that involves how information flows, access to the self and activities, and decentralized surveillance points to the incredibly social nature of privacy—it is a concept that is integral in developing relationships. Relating to each other is perhaps the most important aspect of Facebook for most users. This social incentive for Facebook points to one of the key problems with privacy in social media settings: Users elect to disclose information because they see the social incentives as important. As various studies have shown, the social gratifications of Facebook use override many concerns over privacy: Teenage users especially (the subjects of many of these studies) value privacy greatly, but understand the social gratifications of Facebook as important enough to disclose information (Debatin et al.; Ellison, Steinfield, and Lampe; Livingstone; Tufekci). This social aspect of Facebook and other social media sites again points to a fundamental problem with the public/private distinction. This dichotomy is problematic when we approach the nuances of privacy as it is actually practiced because the dichotomy ignores issues of how and in what ways people, information, and activities are accessed, and further ignores the arena of the social. I understand the arena of the social as

spaces that seem both private and public. As Karen V. Hansen describes the social in her critique of the public/private distinction as market/state versus domestic, "the social captures a field of activities and relationships that transcend the boundaries of households but are not predominantly shaped by the logic of the state or the market" (293). The social activity on Facebook needs to be understood not as simply public or private, but as a social realm where information is never quite fully public or fully private. It is this social nature of privacy, as well as the affordances of digital technologies, that are less than clear in Facebook's privacy policy, which I turn to later in this chapter.

Rhetorical Ecologies and Technologies

Rhetorical theory has traditionally approached rhetoric through the interpretation of texts and their effects or potential effects for audiences. Increasingly, rhetorical critics and scholars are moving away from textual analysis to investigating the ecological nature of rhetorical action. As Jenny Edbauer argues, the traditional sender-message-receiver model of rhetoric is limited in that it ignores the codes and modes of circulation, processes of invention and writing, and the distribution and circulation of rhetoric. For Edbauer, an "ecological . . . rhetorical model is one that reads rhetoric both as a process of distributed emergence and an ongoing circulation process" (13). In other words, rhetorical action does not simply move from the rhetor to an audience in a static context, but rather is in constant motion in an environment that is constantly changing and in which texts are distributed and circulated in complex, unpredictable ways. As Marilyn Cooper persuasively argues, rhetorical action (in her analysis, writing) is "always an interaction with other beings and objects in our surroundings" that "involve both body and mind are only partly and sometimes intentional" ("Being Linked" 20, 17). Cooper was perhaps the first rhetorical scholar to propose an ecological approach to rhetoric, arguing in her 1986 *College English* article

"The Ecology of Writing" that "writing is an activity through which a person is continually engaged with a variety of socially constituted systems" (367).

Approaching rhetorical action as ecological, that is, taking place in an environment that is constantly in flux and changing, focuses on the dynamic nature of systems. Cooper explains that an ecological approach is not just a new way to say "context." Contexts are often presented as static and unchanging (especially in writing instruction); ecological systems, on the other hand "are constantly changing, limited only by parameters that are themselves subject to change over longer spans of time" ("The Ecology of Writing" 368). This means that not only are environments constantly changing, but that we should also understand rhetorical action as action that affects and changes those environments; rhetoric "changes social reality" (368). As Cooper explains, words and tools mediate our engagement with our environments ("Being Linked" 17, 29).

An ecological approach to rhetoric also necessitates attending to the specific features and affordances of media. Digital media makes rhetorical action different from print or oral rhetoric. For instance, Barbara Warnick calls for a "media ecology approach" (vii) that understands that "Web content is processed and experienced in ways different from other media" (27). She applies this approach to rhetorical analysis, arguing that rhetoric works differently in online spaces than it does in print or oral situations. She argues persuasively that we need to understand how products online are never quite finished in online environments, but are instead fragmented and co-produced by users (29-30). Warnick also argues that *ethos* functions differently online: Instead of being the product of the rhetor and his or her credibility, *ethos* is determined textually, as a product of circulation and other textual features (34-35).

Brooke goes further, arguing in a move I endorse that with digital media, we should shift our attention away from analyzing texts and products toward analyzing media interfaces. This shift toward interfaces has important implications for how rhetorical scholars approach new media and analysis. Brooke defines "the interface" as more complex than "the boundary or

contact point between people and machines"; instead, "interfaces are those 'ever-elastic middles' that include, incorporate, and indeed constitute their 'outside'" (24, quoting W. J. T. Mitchell). That is, interfaces are not just media we use to contact others, but are instead digital environments that incorporate and include users. A turn toward analyzing interfaces stresses the existence of multiple, varied experiences with interfaces, and a different approach of analysis for critics. Brooke argues that because of the dynamics of new media (e.g., frequent updates on blogs, continuously changing wikis), there is an "absence of shared experience [that] can become part of the infrastructure of the text" (11). Interacting with an interface can be a very individuated experience, as Steven Johnson notes in *Interface Culture* when he discusses his inability to talk with his friends about any shared understanding of the content of Michael Joyce's hypertext story *Afternoon: A Story*. Johnson writes that "Each reading had produced an individual, private experience" that resulted in each friend in the conversation talking about "very different stories" (qtd. in Brooke 11).

In this way, it is important to take into account the perspective of users, which Brooke describes as looking *from* (134). Interfaces are constantly changing because of technological changes and different encounters in particular moments, but also because users approach interfaces differently at different moments, depending on their comfort, familiarity, and purposes in approaching the interface. If we are "interested in examining the *activity* and *locations* of textual production" in environments (Dobrin and Weisser 578), then turning toward the interface and attending to how users understand and interact with them is crucial. As Brooke explains:

> The appeal of ecology as a conceptual metaphor is its ability to focus our attention on a temporarily finite set of practices, ideas, and interactions without fixing them in place or investing too much critical energy in their stability. In part, this appeal makes ecology the perfect unit of analysis for examining the

> interface, itself a momentarily situated encounter among users, machines, programmers, cultures, and institutions. (42)

In this way, literacy practices are rhetorical engagements with environments, necessarily involving ideologies and discourse communities. Sidney Dobrin and Christian Weisser explain, "writers enter into particular environments with a certain ideological code and then contend with their environments with a certain ideological code and then contend with their environments as best those codes allow. These environments have material, social, and ideological qualities" (576). Dobrin advocates an approach to literacy from an ecological perspective, explaining, "*Ecological literacy* refers to a conscious awareness and understanding of the relationships among people, other organisms, and the environments in which they live" ("It's Not Easy" 233). While his focus in discussing ecological literacy is on developing a literacy related to natural environments and understanding that "All texts . . . teach us something about places, about organisms, about relationships" (233), the concept is useful in exploring how literacy online also requires awareness of relationships among people, technologies, and interfaces.

The Rhetorical Dimensions of Privacy

We often think of privacy as a fundamental human right and as an *a priori* concept, as something that exists prior to ourselves, meaning that certain content or information is understood as automatically private and that what is private is static and unshifting. However, the reality of the matter is that privacy is a contested concept, one that shifts in meaning and practice over time in relation to various social factors, including new technological developments and cultural differences. Privacy norms and practices differ between and within cultures, and understandings of privacy shift even within situations depending on perspective. While privacy is often imagined as a property of the individual—his or her privacy rights, a quality that demands to be protected

by the state, by the self, and by others—it is in fact thoroughly social, mediated by language, objects, and places, up for revision and change in different situations and moments. To say that privacy is social and mediated by language and objects is also to say that it is thoroughly rhetorical, which is to say that it is open to possibilities. Here I draw on Aristotle, who in *On Rhetoric* explains that rhetoric is not about what *is* (that is, what is necessarily true), but is instead about the realm of the possible or probable (42). That is, privacy is not simply some concept that exists before practices, but is rather something that is practiced differently in different ecologies, understood differently from various perspectives, argued about in order to make claims about the common good, and practiced differently in order to change relationships or one's environment.

Privacy, then, is rhetorical in four inter-related ways: 1) The term is used, in conjunction with its counterpart *public* (which is either implicitly or explicitly evoked) to frame discussions in different, sometimes conflicting, conceptions of the public/private distinction. These competing understandings of the public/private distinction allow rhetors to frame debates or issues in ways that may hide or make invisible how certain aspects of a situation could be cast differently as public or private. 2) *Privacy* serves as *doxa*, or a commonplace that people think with rather than about, to argue about the common good. Privacy is utilitarian: Rather than being an *a priori* right, it is contextual and practiced differently in different contexts for social well-being. *Privacy* can be used as a term to perpetuate historical injustices related to differences, particularly gendered power differences. 3) Privacy is a rhetorical practice, in that people use objects and discourses in order to engage with their environments in ways that manage visibility and accessibility to the self or to information. 4) Finally, technologies and environments encourage (but do not determine) certain practices related to privacy, making certain practices more possible or likely to occur, and other practices harder to imagine.

Privacy is wrought with a number of different meanings, and when it is evoked, it is often done so in contrast (either explicitly or implicitly) to its counterpart *public*. The use of the term

privacy is often used to frame a situation or debate, which can serve to make other aspects of a situation invisible. That "privacy" frames debates means that, as a rhetorical tool, "privacy" does not simply describe, but helps to create or constitute a rhetorical situation. For example, something that is private in one sense or from one perspective (say, domestic violence as being of concern only to the private family) becomes harder to argue as something of common or public concern. Nancy Fraser makes this point when she explains the rhetorical nature of the public/private distinction for making arguments about behaviors, policies, and values: Something described as private in economic terms is excluded from public debate and politics and placed in the hands of private corporations or companies; something described as domestically private is out of the purview of the state (88). In "The Theory and Politics of the Public/Private Distinction," Jeff Weintraub unpacks the "complex family" of oppositions between private and public, arguing that when someone uses one term, they are often also referring to the definition of the other term. Weintraub offers a useful categorization of the normative and descriptive ways the dichotomy is deployed: 1) in a liberal-economic sense, where the public is state administration and the private is the market economy; 2) in a republican-virtue sense, where the public is the political community and citizenship and the private is the personal sphere; 3) in the sense used by Philippe Ariés, where public is sociality and the private is the individual; and 4) in the sense some feminists critique for the distinction in their critiques of patriarchy, where the private is understood as the family or domestic sphere and the public is the larger economic and political arenas (7). Weintraub's categorization is useful, for as Fraser notes, rhetorics of privacy "exclude some issues and interests from public debate" by economizing them or personalizing or familiarizing them (88). While most senses of private and privacy have a corresponding sense of the public, Michael Warner does note three "senses of private that have no corresponding sense of public": 1) experiences of inwardness and incommunicability; 2) respectfulness, impudence, and propriety; and 3) "genital or sexual" (*Publics and Counterpublics* 30). Generally, though, the

terms *private* and *privacy* are used in a variety of ways, sometimes meaning several things at once, and sometimes blending the sorts of meanings that Weintraub and Warner outline.

Thus, the ways that something is private or public depends on perspective. Susan Gal calls this the indexical nature of the public/private distinction. Something may be viewed as public from one perspective, but private from another perspective, and material or rhetorical actions can help to change perspectives. A public sidewalk in front of a store, for example, is a publicly-owned and traversed space, open to all, but in the moment that a store manager, who is responsible for keeping it clean, sweeps it, the space is seen as private. These "indexical gestures," whether material practices or rhetorical actions, help to shape or frame situations so that they are seen as either public or private from various perspectives (Gal 82). Framing a situation as either public or private, then, serves to exclude perspectives that might see it as public or private in a different way.

For example, common discourses about Facebook, blogs, and Twitter emphasize how they are sites for "oversharing," implying that users should be more reticent in public spaces and are sharing too much private information so freely (private in the sense of personal or propriety). However, what these claims of oversharing obscure is the potential for shared affective work in public. That is, the so-called "oversharing" on blogs can help to create publics where people can work through emotions, such as trauma. Steven Johnson makes this point in his article "In Praise of Oversharing" in *Time* magazine: Sometimes oversharing can be cathartic or lead toward affective work with a public, as in the case of his friend Jeff Jarvis, who blogged about his prostate cancer diagnosis and journey through his cancer treatment and recovery, including such private moments as the removal of his prostate, his experiences with a catheter, his incontinence, and his erectile dysfunction. Topics that are generally taboo in public—dying, illness, sex—might

be seen as private in one sense, but could be viewed as public, and good for the public, in another sense (Johnson; Jarvis 34-35).[2]

Because privacy can be understood differently and practiced differently in different contexts, it is also rhetorical in that it can be argued about. Instead of a stable concept, what is private is defined by and for the common good. Privacy serves as a public good that allows individuals and groups to develop identities away from the surveillance of others, including authority figures or dominant culture; allows individuals to decide what to share and who has access to them so that they can build intimate relationships; and helps the public to discern what issues or problems are up for debate.[3] But while it is true that privacy is a public good, privacy is not an *a priori* right. We do not have to be concerned if it is "true" that we have an ontological "right to privacy," for example. Rather, as Thomas Nagel argues, we need to understand claims about privacy to be moral arguments, which are not about what is true, but about what is better, that is, what is more likely because it helps to make a better world (39).

Lloyd Weinreb also argues that privacy is not an *a priori* right, but is something contingent upon and within communities and on circumstances. To Weinreb, privacy is utilitarian: It is defined and determined by what will most help the common good (42). That we

---

[2] Jarvis's experiences of having cancer and writing about it serves as an example of the value of publicness online in his book *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*. While there's value in much of his discussion, his concepts of *public* and *private* are under-theorized, often conflating various conceptions of *public* and not adequately theorizing how privacy is still managed online. For instance, while he went public with his prostate cancer, he does not adequately dwell on how he managed his publicness and privacy. He didn't immediately "come out" as having prostate cancer, for example; instead he managed the information, at first telling only those in his private sphere—his wife and children. Even that management failed him, as his co-worker was in his network on the website Delicious, where he had bookmarked sites about prostate cancer (35, 40). While Jarvis claims that "Even in intimate details of my life, I now default to public" (35), he doesn't fully explore the complexities of private and public experiences, even in his primary example of the virtues of his publicness. For an excellent extended critique of Jarvis's exploration of the public/private distinction, see David Parry's blog post, "Privacy is a Public Value or Why I Am Not Boarding the Jarvis Bus."

[3] On privacy's value for identity development and construction, see Moore; Nagel (9, 15); Murphy (35-36; 52).

understand privacy as contingent, argued about, and defended means that those who attempt to defend privacy need to understand that they need to argue for privacy in terms of a common good—an argument that includes why their version of privacy is better than other alternatives offered in its place (Weinreb 44; Frey 60). Thus, privacy is squarely in the realm of rhetoric, aligning with the goals of rhetoric to imagine possible futures. Nancy Welch advances this notion of privacy as rhetorical clearly in her exploration of the public/private distinction when she explains that her goal as a writer and teacher is to "make the classifications of public, private, personal, and social *arguable*" ("Ain't Nobody's Business?" 28). Thus, privacy is rhetorical in that it is a term that is descriptive, normative, and constitutive, used not just to describe, but to frame debates.

That *privacy* is argued about leads to the next way in which privacy is rhetorical: It is a commonplace used in public and personal discourses in order to make claims about the common good. As a commonplace, *privacy* is often not coherently defined, but instead has force in discourses in order to support claims. Dana Anderson's exploration of the term *identity* as a commonplace, or *endoxa*, is helpful here. He understands *endoxa* as "beliefs that are widely held, yet open to disputation" and "those ideas we think *with* rather than *about*" (8). Privacy too functions as *endoxa*: a concept deployed in order to make arguments, one thought with rather than about. The term is deployed in order to make normative claims about how we should relate to each other or to understand new communication or social problems.

As a commonplace, *privacy* can thus be deployed in ways that carry with it social and historical baggage that can privilege certain people over others in relation to historical issues of power and identity that continue with us today. That is, terms carry with them their historical uses, often without our explicit awareness. An ecological model of discourse can help us to see how we understand certain discursive actions as public or private based on prior theories of the public and private. Sid Dobrin explains that discourse is not *a priori* public or private, but is

instead understood as public or private through prior theories of discourse. Each communicative moment draws on prior communications that theorize separate realms of private and public, and "is at once dependent upon and moderated by both 'private' and 'public' prior theories" ("Going Public" 216). Dobrin understands all discourse as public, since discourse is only known and interpreted through social interactions and thus is socially constructed (220). He explains, "before a discourse can be made private (the privatization of discourse?), it must first be experienced publicly. Certainly, then, we can say there is a distinction between public and private discourse, but only as a matter of convenience and codification" (221). In this way, all discourse begins as publicly mediated, and then is labeled private according to convention or necessity (221). While Dobrin's goal is to do away with the public/private distinction in regards to discourse and view each communicative action as unique (because the distinction limits possibilities for discourses) (217)—a view I can't entirely agree with because of the values of privacy and the strong hold the public/private distinction has on our imaginations of reality—his schema is helpful in understanding that when we describe or understand something as private we are informed by theories of discourse that have in the past understood similar communicative events as public or private.

In this way, privacy can carry with it sociohistorical inequalities in power when the term is used as *endoxa*. Western culture has historically afforded different understandings of privacy based one's social situation and identity. Particularly, women, people of color, and sexual minorities have not been afforded the same rights of privacy as heterosexual white men. While it has been tempting for some, like Catherine MacKinnon, to conclude that "for women there is no private, either normatively or empirically" (191), the concept is fluid enough that it can still benefit women. Jean Cohen explains that while privacy developed in relation to private property, the freedom to make private contracts, and "entity" privacy, or familial privacy that in many ways served to protect men's property, personal privacy has become conceptually separated from these

other notions of privacy, meaning that the concept can be useful for women in developing autonomy (139). Privacy's application to sodomy laws can serve as an example of the flexible and changing nature of privacy as it has been applied to marginalized groups. When the Supreme Court upheld homosexual sodomy laws in their 1986 decision on *Bowers v. Hardwick*, they applied the question of privacy too narrowly, making it about homosexuals and privacy instead of privacy itself (DeCew 122). However, the Court returned to the decision in the 2003 case *Lawrence v. Texas*, overturning *Bowers v. Hardwick* and extending personal privacy rights to all people for sex in private.

Although conceptions, laws, and practices related to privacy have changed to be more inclusive and just, *privacy* carries with it those historical injustices that still play out today. Fraser provides an example of this holdover in her analysis of the Clarence Thomas trials, where Anita Hill was not afforded the right to privacy in discussing her sexual harassment charges against Thomas. However, Thomas was able to call upon his privacy rights in order to avoid discussing his private life. Fraser argues that disclosing one's private life in public means to be feminized (107). Thomas's appeal to privacy works only because he was able to deploy the term *private* as *doxa*, as a commonplace that others understand—intuitively and through a history of privacy norms—as something that protects a man's private life from public humiliation.

In addition to a way to frame debates and serving as a commonplace, privacy is also rhetorical in that it relates to rhetorical practice with objects in environments: We use objects in order to change our environment, build relationships with others, and build up physical and emotional private spheres. Sociologist Christena Nippert-Eng helps make apparent the use of objects to manage privacy in her study of how people understand and practice privacy. In her observations on a beach, she witnessed beach-goers using umbrellas, strollers, and towers to change the environment around them and create private areas (11-14). The use of objects to affect our environments and negotiate private space is an everyday activity for most of us: We adjust

chairs in meetings so as to not be too close to someone else, we select certain tables at restaurants that are more secluded, we take phone calls into other rooms, we wear headphones in public spaces, we close doors when changing clothes or going to the bathroom. Objects, then, are used to interact with and shape our environments, making privacy an embodied material and rhetorical practice. In the examples I draw on in Chapter 2, users of mobile digital devices use these devices to manage and interact with their spaces as well, and contrary to claims that these users lack a sense of place, their work is embodied and very aware of place.

A fourth rhetorical dimension of privacy is that environments affect privacy practices, encouraging or discouraging certain practices related to privacy and publicity. The environment of a typical classroom, with desks facing forward, encourages certain practices of privacy and understandings of education: The private educational experience of the student listening to and talking to the teacher, rather than a more open, semi-public experience of working together. It also affords the opportunity for private conversations in the back of the classroom. A classroom where chairs are arranged in a circle, however, encourages a less private experience because of the change in the environment. This is not to say that these responses are determined beforehand and that arranging chairs in a circle is a magical way to get students to engage each other. Rather, practices in these classrooms depend on a whole host of factors that help to shape the ecology of the classroom.

Early iterations of Facebook's interfaced encouraged certain attitudes toward privacy. Because the site was initially much more exclusive and less open, and because it requires a real, authentic identity (users agree to use their real name and not impersonate others or create fake profiles, though there are a number of users who violate this agreement), it encouraged the sharing of private information. Initially only open to Harvard students when Facebook began in 2003, and then expanding to other colleges and universities, Facebook's use of "networks" encouraged viewing it as a private space where users were only likely to encounter and interact

with friends and acquaintances. The separation of the site into individual profile pages, before the development of the Newsfeed in 2006, also lent the site a feeling of privacy, making posting on a friend's profile page feel much more private. This understanding of Facebook as a private space was encouraged by the fact that when a user logged in, they were welcomed by their own profile page and links were provided to view "My Friends," "My Groups," "My Messages," and so forth.

Various changes in the ecology of the site, including opening it up to high school students in 2005, opening the site to anyone over the age of 13 in 2006, and the introduction of the Newsfeed in 2006, changed the environment and thus how users responded to the site and practiced visibility and privacy. In fact, the ecology for each user can be drastically different, and even change on a situational basis. For instance, for some users, Facebook can become a completely different space after their parents add them as friends. The environment of Facebook now constantly shifts, providing new and different content and interactions on the Newsfeed when a user logs in—a quite social space that encourages situational actions that have varying degrees of privacy and publicity, depending on the context.

To say that an environment encourages certain behaviors regarding privacy and publicity is not to say that it determines them. A number of factors influence behaviors on a site. Among those influences are the idioms of practice and media ideologies that users bring with them and develop during use that affect how they interact with the interface (thus the importance of Brooke's concept of looking *from*). Thus, while environments are rhetorical in that they encourage certain behaviors and attitudes of privacy and publicity, they are also not deterministic. Instead, users interact with their environments from their perspectives, changing them through rhetorical and material practices. I understand these rhetorical practices with interfaces as a highly literate set of activities for managing privacy, as I'll explain in the next section.

Managing Privacy Online as a Highly Literate Set of Practices

Because managing one's privacy in social media environments involves being able to understand, interpret, and put into practice various aspects of an environment, including privacy policies, privacy settings, and interactions with others, managing one's privacy online is a highly literate activity. In fact, as Zizi Papacharissi argues, privacy online is becoming a "luxury commodity" that requires a high degree of literacy that might not be available to most. Managing one's privacy online can require a great deal of time, attention, and digital literacies, and those without the digital literacies to manage their privacy find themselves not as able to manage their privacy online ("Privacy as a Luxury Commodity"). I follow scholars such as Cynthia L. Selfe in understanding digital literacies not as a basic set of neutral, decontextualized skills, but instead, in the words of Selfe, "a complex set of socially and culturally situated values, practices, and skills involved in operating linguistically within the context of electronic environments, including reading, writing, and communicating" (11). Thus, digital literacies involve sets of practices and actions using digital environments that take into account social, cultural, and political values and contexts.

Taking a literacies approach to concerns about privacy in social media environments affords two important insights. First, rather than reject novel actions and practices as frivolous or even harmful, a literacy approach situates those actions and practices in a rhetorical context. This approach means, in part, that users' decisions on Facebook are understood to be informed by media ideologies, shared idioms of practice, and genealogies of practice that lead to conflicting understandings of both social media sites and social behavior (Gershon 3, 6; Sloane). Because many aspects of new media are, in a very real sense, new, there are not widespread understandings of their best uses, and users tend to approach and understand new media in a variety of ways. Ilana Gershon's discussion of how Facebook users delete their Facebook friends

is instructive here: Some of her research subjects see removing Facebook friends as hostile acts, whereas others see friendship on Facebook as not really mattering, and thus they routinely go through bouts of de-friending. These idioms of practice, or shared meaning-making about the uses of technologies, were often developed through shared understandings of Facebook—understandings created through conversations with friends, shared practices, and experimentation (38-42). Because new communication technologies present new situations for users, they often turn to each other in order to understand those new technologies and to develop best practices within their communities. Thus, users are likely to have shared understandings of privacy settings, shared practices and understandings of tagging photos or posting on profiles, and more. In their research, Kevin Lewis, Jason Kaufman, and Nicholas Christakis discovered that users were more likely to have a private Facebook profile if their friends also did.

Conflicting understandings of "proper practices" regarding privacy on these sites is caused, in no small part, because of conflicting media ideologies, or the sets of beliefs about a communication medium that inform users' design, perception, uses, and meaning (Gershon 3). New media are used and understood in a variety ways because there is not necessarily widespread understanding of their uses and purposes. Collin Brooke argues that because of the dynamics of new media (e.g., frequent updates on blogs, continuously changing wikis), there is an "absence of shared experience [that] can become part of the infrastructure of the text" (11). In many ways, there aren't just differing and conflicting understandings of sites like Facebook; instead, because these sites can be put to use in various different ways, there are "*many different Facebooks*" (Wittkower xxiii). Regarding privacy online, these various different Facebooks can lead some to claim that users don't care about privacy, while users themselves can claim to be very invested in privacy online. Broad claims that users do not care about privacy online are informed by media ideologies that privilege more reticence, whereas a closer look at users' attitudes, beliefs, and

practices reveals that users do care about privacy in a myriad of ways and put those concerns into practice in multiple and various ways.

Second, rather than only seeing Facebook as exploiting users for information, a literacies approach helps us to see that users choose to navigate institutions and use literacies as sets of practices and actions for a wide range of purposes. A literacies approach to social media and privacy helps us to think about how users engage in digital environments in order to navigate social situations. Following Jeffrey Grabill, Stuart Selber, Andrew Feenberg, and others, I take a postcritical approach to literacy technologies: A postcritical approach understands that technologies are not neutral tools, but are instead cultural artifacts that influence thoughts and behaviors, but they are also here to stay. Thus a postcritical approach rejects deterministic interpretations of technologies, and takes a critical approach to the use, design, and engagement with technologies (Grabill 34; Selber 8; Feenberg 6).

Put differently, we might be tempted to reject sites like Facebook for exploiting users for their information in order to make money off that information through the selling of advertisements. However, this flat-out rejection ignores the very real social reasons that users turn to sites and are implicit in this exploitation of their information. Users share information on Facebook for a variety of social reasons: to connect with friends, to gain visibility, to develop their identities, to network professionally, to engage in shared interests, to interact in social spaces that might be outside the gaze of other parties, and more. As Bernhard Debatin and his co-authors explain, "the conveniences and gratifications of Facebook as a social tool seem to override privacy concerns" for many users (101). These social reasons have been explored by various ethnographic and survey studies, which show how users maintain relationships and create new relationships, develop social capital (Ellison, Steinfield, and Lampe; Tufekci 21), and use sites like Facebook to interact in social spaces that might be outside the gaze of parents (Livingstone 405). Sociologist Harry Blatterer explains that the need for visibility on these sites is

not caused by the technologies themselves; instead, the desire for visibility is further enabled by these sites. He asked, "why do members of social networking sites voluntarily part with personal data even though that information is potentially retrievable by others who can use that information out of context and against their best interests?" (75). Blatterer argues that there is a human need for visibility that these sites make more possible to act upon, and as users share more, they become "experts not only at self-presentation but also at self-concealment" (79). That is, while users may share much information on these sites, they also make choices about what to share: There is a tension between visibility and privacy that users negotiate, which requires placing practices in context in order to understand how users negotiate this tension and what sorts of information they share, with whom, and why. And as various studies have shown, users *do* care about managing that tension, through using privacy settings, determining what is posted and what is kept off of sites, un-tagging pictures, deleting comments and posts that might seem inappropriate for certain audiences, and other practices (Raynes-Goldies; Boyd and Hargittai; Jones, Johnson-Yale, Millermaier, and Pérez; Lange; Livingstone 405; Tufekci 31-33; Boyd, *Taken Out of Context* 155, 166).

If managing privacy is a set of highly literate skills and practices, as I am arguing here, then it is in the purview of writing teachers and scholars to be concerned about issues and practices related to privacy online. As Anne Frances Wysocki argues, writing teachers and scholars bring an understanding that communication is always contextual and situated to scholarship on new media, which can help to situate practices and assist users in making decisions in new media settings. She explains, "Writing teachers help others consider how the choices we make in producing a text necessarily situate us (or can try to avoid situating us) in the midst of ongoing, concrete, and continually up-for-grabs decisions about the shapes of our lives" ("Opening New Media" 7). Exploring the contextual nature in which users choose to share or not share information and activities online, and understanding how users can do that in ways that

match their desires, is certainly part of digital literacy practices, and thus part of our charge as teachers of writing. Additionally, as writing teachers consider incorporating social networking sites into their classes to explore rhetorical aspects of these sites, including identity construction and technological literacy (Vie; Maranto and Barton), it is increasingly important to explore the difficulties of managing privacy as users (including students and teachers) write and work in these spaces.

In the next section, I discuss an example site of literacy (Facebook), exploring how affordances of the site make privacy, especially controlling the access to information, a highly social and distributed activity—other users in one's network, as I explain, exert control over access to a user's information through their privacy settings and practices on Facebook.

Facebook's Governing Documents: Rhetorics of Control

Importantly, the technological developments on sites like Facebook are related to the affordances of digital media that make privacy complicated online: the ability to easily publish, replicate, aggregate, and search for information. These affordances are not discussed in Facebook's Data Use Policy (formerly its privacy policy), leaving a gap in the policy that elides how a user is not always in control of one's information and access to one's activities. Instead, other users are often in more control of access to a user's information and activities because of these affordances.

An important aspect of Facebook is its governing documents: Facebook's Data Use Policy, which outlines what information Facebook collects, how it is collected, and how it is used; its Statement of Rights and Responsibilities, which serves as a terms of service that outlines the relationship between Facebook and users that users agree to; and its Principles, which stand as a sort of philosophy that informs the Rights and Responsibilities of users. Although the majority of users probably do not read these policies, they are still important. As Halbert explains in her

analysis of terms of service documents for online services, including various online games, virtual worlds, and Facebook, "the terms of service (TOS) agreements [. . .] governing virtual worlds have important implications for the political and legal structures under which our virtual selves will function." Even without reading the governing documents, users' experiences on a site are shaped by these sorts of documents, as the TOS serves as a sort of law.

Privacy policies and other governing documents of websites have come under increasing scrutiny from rhetoric, communication, and new media scholars. Justin Grimes, Paul Jaeger, and Kenneth Fleischmann argue in their study of governing documents for virtual worlds such as World of Warcraft and Second Life that these documents govern through "obfuscated code": governing documents contain technical and legal jargon; are housed in various locations, making them hard to access; and are updated frequently without logs of those modifications. Markel adds to our understanding through his analysis of corporations' privacy policies on their Web sites: They often work through misdirection, as they are written in ways that prevent users from understanding them so that companies can exploit users' data.

Exploitation of users' data is key to most of these studies. In their study of privacy statements, Fernback and Papacharissi explained how these statements often "allow companies to profit from consumer data" (715). Though privacy statements prepare

> the user for a guarantee of privacy protection (since they are not 'disclosure statements'), the vocabulary of the statement itself rarely offers explicit privacy protection. [. . .] Privacy statements generally serve two major purposes: to mollify consumers wary of conduction transactions online for fear of privacy violations; and to convince regulators that further legislative initiatives to guarantee consumer privacy are unnecessary, since the industry self-policing efforts sufficiently protect citizen rights. (719)

Fernback and Papacharissi argue that privacy policy statements are in actuality marketing tools: They are meant to give users a sense of comfort about their privacy and sell companies as ethical in the eyes of users and regulators. In effect, "company privacy policies are often invasive rather than protective; they describe how consumer privacy is systematically undermined" (730).

While these analyses focus on how privacy policies use misdirection and mollify consumers in order to exploit information, I am less interested in how Facebook exploits information. That Facebook "exploits" users' information for advertising and financial gain is well known and commonplace. Users choose to share their information and activities with Facebook for a variety of social and personal reasons: to document lives, to share experiences and build relationships with contacts, to gain visibility and acknowledgment, to develop an online (and offline) identity, and more.

Instead, I am interested in placing Facebook's privacy policy in conversation with the site's interface in order to show how other users' privacy settings control access to and the flow of information and activities because of the specific affordances of social media: aggregation, replicability, searchability, and ease of publishing. Put differently, I am interested in placing the policy within the ecology of the specific Web site under investigation in order to explore how information actually flows on the Web site. Indeed, unlike other privacy policies, Facebook's can be fairly clear, though, as Nissenbaum points out, it "is likely to leave one hard-pressed to map accurately and fully the flows of personal information allowed by these policies" (222). Part of the difficulty in determining how information flows on Facebook lies in the fact that Facebook's rhetoric largely ignores that other users' privacy settings actually have great control over your information. It accomplishes this through a rhetoric of protection and control that ignores certain features of the Web site.

Facebook's privacy policy is not an exception to the analyses described above: It is largely a document meant to represent and create a relationship between Facebook and its users.

While most users probably do not read the privacy policy (it is longer than the U.S. Constitution, after all), it serves many of the functions discussed above for those who do read it: It creates a modicum of trust by users, and gives users a sense of control over information. Facebook's privacy policy is organized according to the ways information is received (information users provide, information Facebook collects, and information from third parties), shared (on Facebook or with third parties), and used. Despite relative ease of navigation, the policy's length makes it unlikely that a typical user will read it, given the contexts in which many users sign up for social networking sites.

Facebook uses a rhetoric of safety and protection throughout its privacy policy. Some information is collected "to make Facebook easier to use," "to protect you (and Facebook)," and "to keep Facebook safe and secure" ("Data Use Policy"). This sort of rhetoric of protection and safety makes the sort of privacy violations that concern legal scholars like Solove seem less like violations ("A Taxonomy"). For example, users are given the choice to opt out of, rather than opt into, features like social ads that appropriate one's likeness to benefit advertisers.

Additionally, information about the privacy policy and changes to those policies are spread throughout different documents and spaces on Facebook (the Data Use Policy, the Statement of Rights and Responsibilities, and the Facebook Site Governance Page)—similarly to Grimes, Jaeger, and Fleischmann's charge against other governing documents. Users are notified of changes to the privacy policy on the Facebook Site Governance Page, but users must "Like" that page in order to receive those updates in their Timeline—and even then, those updates might be missed if a user doesn't view their timeline in the right window of time. Facebook's governing policies outline that users have a say in privacy policy changes, but only if enough users comment on a possible change to bring it to a vote ("Statement of Rights and Responsibilities"). Though Facebook suggests a sense of user control and input here, and Facebook is legally safe according to current United States laws, again concerns arise around possible privacy violations: Changes in

privacy policies without proper notification or consent can lead to breach of confidentiality or the disclosure of information a user did not want (see Solove, "A Taxonomy" 526-535).

This rhetoric of safety is supported by a rhetoric of control throughout Facebook's governing documents, which claim that a user "can control how [information] is shared" by using privacy settings and application settings ("Facebook Principles"). Tensions arise, however, in Facebook's verbal rhetoric, which attempts to value both an ethic of visibility and access and an ethic of user control. Facebook's Principles statement advocates "openness and transparency by giving individuals greater power to share and connect" ("Facebook Principles"). This "power to share and connect" marks a tension among Facebook's first three principles, which promote three freedoms for users: "the freedom to share whatever information they want," "the freedom to decide with whom they will share their information," and "the freedom to access all of the information made available to them by others" ("Facebook Principles"). Facebook's principles promote user visibility (share as much as you want with whom you want) and user access (you should have access to everything shared with you), two values that are in tension with the rhetoric of control throughout the site. Because of the aggregation of data, information is able to be moved and manipulated, and thus accessible in new and different ways that can be surprising to users. This increases access, a boon in Facebook's view, but makes the issue of various unintended audiences more acute.

Facebook's rhetoric of control continues throughout its privacy policy. The term "control" occurs frequently, stressing users' ability to control their information and presence on the site. Users can navigate the document to find how to "Control each time you post" and have "Control over your profile." Language elsewhere in the document stresses the ability to control visibility: "When you select an audience for your friend list, you are only controlling who can see it on your profile. We call this a profile visibility control" ("Data Use Policy"). If a user reads through the privacy policy, he or she might feel assured that indeed the control of information is

entrusted in the user, and not elsewhere. After all, the privacy policy explains which privacy settings control what type of information, what the default settings are, and where they can be changed.

However, underneath the headings "Control each time you post" is a caveat, which I find key to understanding how control of access to information occurs on Facebook: "When you comment on or "like" someone else's post, or write on their Wall, that person gets to select the audience" ("Data Use Policy"). Other caveats (now, in the 2011 version of the policy, marked with a light bulb icon) note that information posted on a page or public story will be publicly available. An older version of the privacy policy had only one statement related to how information might be publicly available based on others' settings: "When you post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings." Despite these notices, Facebook's privacy settings (again, like the policy, centrally located with supplemental pages for additional settings) do not mention this at all. Facebook's privacy settings page at first appears simple: Users can choose between making information available to "Public," "Friends," or "Custom."[4] These options simplify a process that was once much more difficult for users to navigate, but once one begins to customize privacy settings, this can become a time consuming and laborious process. Privacy management, as a result, becomes a very labor-intensive process requiring high levels of digital literacy: finding various options, interpreting those options, and putting them in relation to the interface.

Although labor-intensive and possibly overwhelming to use, Facebook's privacy settings interface does give users a sense of control—unless they are confused (and researchers have shown that these settings can be confusing; see Madejski, Johnson, and Bellovin, who found that all the users in their study were either sharing or hiding personal information in ways they had not intended). However, I argue that this is just a *sense* of control. This appearance of control masks

[4] Accessed February 20, 2012, at https://www.facebook.com/settings/?tab=privacy

the social nature of privacy online: Others' privacy settings are as important as your own. Just as the privacy policy is couched in a discourse of control and ignores technological features that give other users control of information, so do the privacy settings. Nowhere in these settings options is there a clear caveat that no matter what settings you choose, others' privacy settings and choices are just as important, or more important, for the protection of your information. Let me provide a few examples to clarify this point.

The News Feed on Facebook provides an example of how the technological functions described above converge, and how control over access to information is distributed throughout one's network on social media sites. When Facebook rolled out the News Feed in 2006, users were upset because now, when I wrote on a friend's wall, it would be available to our mutual friends on their News Feed. Previously, a user had to go directly to a profile to see if someone had written on their wall, whereas now with the News Feed, information that was quickly posted was now aggregated, disseminated, and more easily available for monitoring. Not only has aggregation affected how information is accessible, but also my friend's privacy settings affect who can see this post in their News Feed (his friends, a limited group of his friends, everyone on Facebook, or anyone online).

More recently, the development of the news ticker in the upper right hand corner of Facebook's homepage provides an even more striking example. This news ticker provides real-time updates to your friends' activity, including comments on posts and pictures. Numerous users complain that this development is distracting (and users have developed plugins for their browsers that remove the ticker), but more users complain that now any activity they do on Facebook might show up on their friends' news ticker. An individual user has no control over whether their activity is displayed in this ticker. Instead, it is up to their friend's privacy settings whether it shows up or not. For example, if I comment on a friend's picture, my comment only shows up in the news ticker of other friends if my friend's privacy settings allow for it—if their

picture is made public or is available to friends of friends. These two examples show how publication, aggregation, and monitoring converge on Facebook, and the ticker reveals one of the ways in which other users' privacy settings affect how accessible one's activities are to others.

In addition, it is important as we consider managing privacy online that sites like Facebook are not sealed off from the rest of the Internet. Instead, information is aggregated into larger databases on the Web. Many users may not be aware that by writing on the wall of a public group or event, that users can be found via Google searches, even if they make their profile invisible to searches within Facebook. For instance, I was interested in hiring an intern a few years ago, and decided to search for her on Facebook. When I couldn't find her, I Googled her. One of the top hits led me to a Facebook group: A friend of hers had broken his cell phone and created a public group where friends commented, leaving their cell phone numbers (a frequent activity amongst Facebook users seeking their friends' contact information after losing or breaking a phone). Not only did I now have access to her limited profile (including her AOL instant messenger screen name and her arts and entertainment interests), but I also had her cell phone number. This Facebook user had clearly selected the privacy option to not be found via searches, but this option did not matter because she commented on a group that someone else chose to make publicly available.

These examples show how access to one's information and activities on Facebook are not controlled solely by the individual user and her privacy settings, but instead by others' privacy settings and activities. Because of the affordances of digital environments—easy publication, aggregation of data, replicability, ease of search, and permanence of information—and the convergence of technological functions that allow for the possible violations of privacy, others within one's network have as much control over how a user's information and activities are accessed. None of these features are particularly unique to Facebook. Instead, Facebook is an

ideal site of analysis because these features converge in various and clear ways on one social media site.

Popular Discourses about Privacy: Nostalgia, Antisocial Youth, and Literacy Crises

In this section I turn to popular discourses about privacy, drawing mainly from newspaper and magazine articles, but also some books and blog posts, in order to explore popular understandings of shifting notions and practices of privacy in social networking sites. Facebook in particular has drawn most of the media attention to it regarding privacy, partially because the site is the most popular, but also because privacy settings and policies have changed a number of times since its creation in 2004. Countless articles and editorials share stories of privacy violations, tales about the indiscretions of young users, and outrage at changing privacy policies on Facebook. Additionally, Facebook and its founder Mark Zuckerberg have been the subject of two books, David Kirkpatrick's *The Facebook Effect: The Inside Story of the Company That Is Connecting the World* and Ben Mezrich's *The Accidental Billionaires: The Founding of Facebook, A Tale of Sex, Money, Genius, and Betrayal*, the latter of which became the basis of David Fincher and Aaron Sorkin's popular and academy award winning 2010 drama *The Social Network*. Other treatments of Facebook include the 2010 documentary *Catfish*, about the discovery of an elaborate hoax on Facebook, and various parody videos on sites like YouTube, College Humor, and others that mock Facebook sociability—an archive that warrants its own study for common conceptions about Facebook sociability.

As an increasingly present part of many users' lives, Facebook has received more media attention than is possible to cover here, but a quick sampling is warranted to explore how social media sites are understood in popular discourses. As Altman explains, how we discuss new technologies is important for how we understand them and take them up (16). Marita Sturken and

Douglas Thomas add that rhetorics about new technologies often say more about us and our values than about how the media is actually used. As they explain, "Emergent technologies have been the fuel for social imaginings, both of what society should be and of its potential to go farther off course from some ideal path to betterment" (1). Rhetoric about the Internet, they explain, often relies on this conjunction of utopian and dystopian thinking. Some praise the Internet for making it possible for better, stronger, and more connectivity with the possibility for more equality and a more globalized, democratic world, while other express fears that human connectivity is lost, and that we are becoming more isolated, antisocial, and disconnected (3). But it is not merely that these rhetorics, whether utopian or dystopian, reveal anxieties and hopes about new communication technologies—they are also productive, affecting how new technologies are integrated into the lives of users and how people understand them (3).

My analysis here is admittedly limited, but I want to highlight three themes in popular discourses about Facebook and privacy. The first is a nostalgia for an unmediated "real world" past that had more personal privacy and people engaged with each other more face-to-face in contrast to the isolated digital mediation of today. The second theme draws on that nostalgia to promote a moral panic that depicts youth as increasingly anti-social, as isolated and alone, without a sense of privacy and with an increasing inability to connect face-to-face. The third connects this moral panic to the literacy crisis, making narratives about lost privacy interconnected to narratives about decreasing literacy due to digital media. After I overview these three threads, which overlap, I turn to discussion of how these narratives often ignore actual, embodied practices with social media technologies that integrate these technologies into users' everyday lives.

Much of the rhetoric about digital media relies on nostalgia for a past with more face-to-face communication, more reticent privacy practices, and more vibrant public spaces. Of course, we often understand new media through nostalgia, as we interpret new media based on

experiences—imaged or real—with other media. Nostalgia is perhaps inescapable, but, as Johndan Johnson-Eilola explains in his discussion of the rhetorics surrounding hypertext in the 1980s and 1990s, "Nostalgias are ideological—not in the sense of false consciousness, but of necessarily partial and conflictual representations of social reality. In tracing that longing, we find we want not so much the past itself as what our image of the past projected our future to be" (176). Just as nostalgic rhetoric about hypertext marks a longing for "the innocence we sometimes assumed marked human existence prior to print, an impossible Eden of pure knowledge and perfect communication unmarked by the 'complications' of technology" (176), nostalgic rhetoric about privacy online often calls upon a more perfect past, one that helps us to argue about what the social and political present *should* look like.

Nostalgia, as it is deployed in popular rhetoric about Facbook privacy, particularly longs for practices of privacy when they occurred in material, physical spaces and places, and idealizes face-to-face communication, which is viewed as more authentic and more intimate. For instance, when Facebook rolled out their (quickly embarrassing) program Beacon in 2007, it was easy for *The New York Times*' Christopher Caldwell to compare shopping in physical locations in the past to shopping now. Beacon, a short-lived software component that posted shopping information on Facebook profiles when users made purchases on integrated sites, was opt-out, meaning that a user had to intentionally select an option so that purchase information was not posted on their Facebook profile. In a case that garnered much attention, a Massachusetts man bought a diamond ring for his wife, and the activity posted to Facebook, ruining the Christmas surprise. Speculation and outrage about privacy proliferated: What if this ring had not been for his wife? What if he was buying something embarrassing that he didn't want his 720 friends to know about? Caldwell saw this as a perfect moment to lament how creepy behavior is now normal online: "We used to live in a world where if someone secretly followed you from store to store, recording your

purchases, it would be considered impolite and even weird. Today, such an option can be redefined as 'default' behavior."

Face-to-face connections of the past are idealized in the narratives about online activity, creating concerns that we are too tied behind a scene and that new privacy practices are making us creepy and harming our face-to-face sociality. In another example, *Guardian* columnist Tom Hodgkinson also questions Facebook's ability to create connections: "Doesn't it rather disconnect us, since instead of doing something enjoyable such as talking and eating and dancing with my friends, I am merely sending them ungrammatical notes and amusing photos in cyberspace, while chained to my desk?" Concerns abound that with sites like Facebook, users will see less incentive to meet face-to-face. Philosopher Mariam Thalos makes this claim in her contribution to *Facebook and Philosophy*, expressing that Facebook "might make a wide range of face-to-face interactions obsolete" (75). Without face-to-face bonding, Thalos worries that we will become more isolated: "Bonding represents a commitment, and a medium that fosters it also fosters commitment. On the other hand, a medium that inhibits bonding will foster isolation instead. Facebook, over time, will do the latter" (85). For Thalos, face-to-face encounters promote a credible, committed self-presentation. It is not Facebook itself that prevents bonding, she clarifies; it is that self-presentation must be credible, fixed, and enduring in order to facilitate bonding, and because of the nature of online discourse, we can easily change how we present ourselves and to whom (86).

These are just a few examples of writers extolling the virtues of face-to-face communication and expressing concerns that online interactions are moving users away from embodied interactions in physical environments. These concerns are further elaborated in a moral panic that youth don't care about privacy anymore, are indiscriminate about posting information online, and are thus increasingly anti-social as they withdraw from face-to-face encounters and become attached to screens, leading to isolation and a loss of the private self. As a 2007 London

Sunday Times headline reads, "the children of the internet age are ready to bare their bodies and souls in a way their parents never could" (qtd. in Livingstone 395). Headlines and stories focus on oversharing online, blaming both users for their dumb decisions and social media sites for their lack of clarity or ethics in privacy controls. *The New York Times* editorialized in 2006 that "Many young people think nothing of posting intimate material on the Web, whether its daily minutiae, personal poems or snapshots of a fraternity beer pong tournament" ("Online Party Crashers").

And, of course, mass media doesn't shy away from enjoying the repercussions of youth's "oversharing" online. In response to news that potential employers were searching for job applicants' profiles on Facebook, the same *New York Times* editorial almost gloated that youth are finally "getting . . . an education in the virtues of privacy" ("Online Party Crashers"). In a story about responses to Facebook's unveiling of the News Feed in 2006, which aggregated users' updates from their profile pages into a homepage on Facebook, making expressions more accessible, *The New York Times* cast understandings of privacy as a generational split: "If there is a single quality that separates those in their late teens and early 20's from previous generations of young people, it is a willingness bordering on compulsion to broadcast the details of their private lives to the general public" (St. John). Once again, *The New York Times* turns to a wake-up call: Because of the News Feed, young people were getting their comeuppance. Shocked to find their information and activities more accessible to others, users were upset. As one young adult explains, "we didn't realize how much of our personal information we were putting out there. . . . You don't see it until you get it served on a platter" (St. John).

The moral panic about youth's increasing anti-sociality due to digital communication are represented well in three arguments published in 2010: Zadie Smith's *New York Review of Books* review of *The Social Network*, Hilary Stout's *New York Times* column "The Anti-Social Network," and Camille Paglia's evisceration of Lady Gaga in the *London Sunday Times*. All three contend that screens are destroying youth sociality and the Internet is corrupting youth's ability to

connect. The focus on how new technologies are corrupting youth is not new: As many scholars have shown, the corruption of children has been a common trope when new technologies emerge, including claims that automobiles would isolate youth from their families, and that dime novels would teach criminality and other anti-social behavior (see Baym 42).[5] But the corruption brought by digital communication brings a new extremity to describing youth's anti-sociality: They are isolated, alone, have no sense of privacy, and are affectless and unable to be sociable face-to-face. Smith describes what she calls "Generation Facebook" as putting all their private information online, which reduces them to "a set of data" so that "Everything shrinks. Individual character. Friendship. Language. Sensibility." Users transcend their bodies, losing "our messy feelings, our desires, our fears" as they spend all their time on Facebook and other social networking sites. This leads to "superficial relationships" and a loss of a sense of the self as "A private person, a person who is a mystery, to the world and—which is more important—to herself."

Stout argues that youth's digital activities are concerning because their material practices lead to isolation and inhibit their ability to truly connect to each other. In a nostalgic turn to the past, Stout echoes a common claim: Youth today are too attached to their screen and too afraid to actually connect to each other face-to-face, or even through voice contact on phones. Citing statistical data from the Pew Research Center, Stout notes that 54 percept of youth text their friends every day, but only 33 percent actually talk to their friends face-to-face every day. This, she claims, should be our primary concern about digital communication—more so than other overly hyped concerns like texting sexual images or cyberbullying—because it's possible that

[5] I find the connection between automobiles and teen sociality fascinating. Today, teenage automobile ownership of the 1960s is idealized and romanticized despite initial concerns that automobiles would separate youth from their families. Recent trends in youth driving habits show that fewer U.S. teenagers are getting driver's licenses, owning cars, and driving. A BBC report speculates that this is partially because of increased gas prices and congested traffic, but also because teens are choosing to spend their money on cell phones and other technology and are communicating more online (Wheeler).

"the quality of their interactions is being diminished without the intimacy and emotional give and take of regular, extended face-to-face time." She explains:

> Children used to actually talk to their friends. Those hours spent on the family princess phone or hanging out with pals in the neighborhood after school vanished long ago. But now, even chatting on cellphones or via e-mail (through which you can at least converse in paragraphs) is passé. For today's teenagers and preteens, the give and take of friendship seems to be conducted increasingly in the abbreviated snatches of cellphone texts and instant messages, or through the very public forum of Facebook walls and MySpace bulletins. (Stout)

Drawing on a number of psychologists, Stout also expresses concern that youth won't have a "bosom buddy" like prior generations did, and will have trouble developing trust in others and empathy for others. They will have difficulty, she claims, in reading social cues because of these superficial relationships online. (I have to wonder how many teenagers saw their friends face-to-face on a daily basis in the past, before they were using cell phones and social media. Growing up on a farm, I certainly didn't see friends outside of school; many weekends and good parts of summers were often spent in social isolation until I got a job when I was 17.)

As Smith's and Stout's accounts above reveal, much of the public imagination around Facebook and other Internet sites revolve around concerns that youth are constantly connected to their computers rather than in each other's actual presence. However, the fear that teenagers and young adults are on their screens far too much and never interact with each other is a dystopian narrative that often ignores the lived realities of teenagers and young adults. It is also a narrative that gets recounted time and time again with new technologies: When I was growing up in the 1980s, for example, the narrative was that we children were spending too much time in front of the television and not enough time with our families, with our friends, and outside. Much like the moral panic around children glued to televisions for eight hours a day, stories about teenagers in

front of their computers, looking at their cell phone screens, and isolated from each other resonate with a vast amount of Americans, particularly adults who find youth's developing technological practices unsettling and strange.

But these narratives do not carry weight only with older, non-Facebook users. They also carry weight with youth and young adults themselves, even as it contradicts their own lived experiences. As a writing teacher, every term I teach first-year writing, I have students who want to write essays or share in class about how Facebook is "harming relationships" or not "real communication." In one course, my students read Camille Paglia's scathing critique of Lady Gaga in the *London Sunday Times*. In her column, Paglia indicts not only Lady Gaga for her inauthenticity, but also her fans, whose "voices have atrophied: they communicate mutely via a constant stream of atomized, telegraphic text messages. Gaga's flat affect doesn't bother them because they're not attuned to facial expressions. They don't notice her awkwardness because they've abandoned body language in daily interactions." In short, Paglia argues that youth are so often behind screens that they can no longer relate to each other with their bodies. While many students rejected this narrative, a few nevertheless agreed with Paglia. I found this shocking, given their own sociable face-to-face interactions in class, and how the Facebook and Twitter updates I see from these same students are often about face-to-face interactions they recently had or were about to have with their friends. The narratives about youth's declining sociablity because of their physical isolation, private information online, and increasing communication via screens resonates not only with adults, but with the users themselves.

The privacy crisis depicted in popular media is intricately linked to a perceived literacy crisis, the third theme about popular discourses I would like to highlight. This is evident in Smith's account when she contrasts her own social circle to "Generation Facebook": she texts in full sentences, whereas youth use abbreviations; language is being reduced online, and youth don't have the language to express themselves, instead writing in abbreviations with affective

markers unrecognizable to Smith. When she imagines a young Facebook user writing on the wall of a deceased friend ("*Sorry babes! Missin' you!!! Hopin' u iz with the Angles. I remember the jokes we used to have LOL! PEACE XXXXX*"), Smith expresses that "It's only poor education. They feel the same way as anyone would, they just don't have the language to express it." And as we saw in accounts I mentioned above, youth are sending "ungrammatical notes" (Hodgkinson). Privacy and literacy are tied together so strongly that even as early as 1994, it was a concern for Sven Birkerts in *The Gutenberg Elegies*, where he laments declining literacy because of the Internet. The idealized literacy of being alone, privately reading a book in leisure, conflicts with the hectic, interconnected image of reading and writing for the web. Birkerts writes, "When everyone is online, when the circuits are crackling, the impulses speeding every which way like thoughts in a fevered brain, we will have to rethink our definitions of individuality and our time-honored ideals of subjective individualism. And of the privacy that has always pertained thereto" (220). Concerned about "invisible elsewheres," Birkerts argues that there is a decline in literacy because of the Internet and the subsequent lack of depth and duration in our thinking (219). He idealizes books as "a portable enclosure, a place I can repair to to release the private, unsocialized dreaming self. A book is solitude, privacy; it is a way of holding the self apart from the crush of the outer world" (164). Reading print is "essentially private," the communication of private experiences from the sender to the receiver who reads in private (122). As early as 1994, then, we have concerns that the Internet was causing both "contractions in the private sphere" and declining literacy (131).

These three themes in popular discourses about Facebook—nostalgia for face-to-face communication, the moral panic of anti-sociability, especially in youth, and a connected literacy crisis—recur in discourses about social media and other digital technologies and resurface frequently in my analyses throughout this dissertation. For example, in Chapter 2, where I discuss the uses of mobile devices like laptops and cell phones in public spaces, I explore the "discourse

of crisis" (Reynolds, *Geographies* 24) that mourns the loss of public spaces—a discourse animated in part by nostalgia for unmediated public sociality in coffee shops and a certain historically privileged type of public discourse. Nostalgia, moral panics, and literacy crises are three frequent popular responses to changing social and literate practices with new technologies, discourses that in many ways are exigencies for my discussions throughout this dissertation.

Outline of the Dissertation

Thus far I have explained how privacy is a cluster concept, involving informational privacy, spatial and bodily privacy, and expressive privacy, and a set of rhetorical and literate practices and behaviors users draw upon to engage in their environments. Privacy is rhetorical in a number of ways—in that it is used to frame issues, is drawn upon as a commonplace, and is argued about, and in that interfaces encourage certain practices related to privacy and publicity. I have argued that privacy is thoroughly social, providing an example from Facebook that despite its rhetoric of user control, privacy is in fact controlled throughout one's social network on the site by others' practices and privacy settings. The affordances of digital media—permanence, replicability, scalability, searchability, and aggregation—mean that privacy functions differently in social media environments than in physical spaces or in print. But changing practices related to privacy online have been responded to in popular discourses by moral panics that site youth as indiscriminately sharing and not concerned with privacy—a belief that is used to portray youth as anti-social and incapable of face-to-face sociability. This moral crisis is also intricately tied to a literacy crisis—as literacy declines in online environments, according to this narrative, so does our ability to protect our private selves.

In the rest of this dissertation, I continue to explore the rhetorical and social dimensions of privacy in digital environments by exploring four concepts that are intricately related to

privacy: *materiality, identity, intimacy,* and *sociability*. I turn to four studies of significant rhetorical practices—the uses of mobile devices like laptops and cell phones in public spaces, the research and aggregation of identities in online environments, sexting by teenagers and young adults, and Josh Harris's 1990s experiments involving surveillance and privacy, in order to explore these concepts. In each of these analyses, I attend to popular and scholarly discourses, interfaces used, and practices with devices and interfaces in order to build a rhetorical understanding of privacy.

In Chapter 2, I explore the material practices of managing privacy in public spaces through the uses of objects, including mobile phones and laptops. The increased use of mobile phones and laptops in public spaces like coffee shops have prompted a "discourse of crisis" (Reynolds, *Geographies* 24) that public spaces are being privatized by users of these devices—discourses that depend on a nostalgia for an idealized face-to-face sociality of coffee shops. In order to investigate these practices and the discourses surrounding them, I investigate the practices of two graduate students who write in coffee shops and a particular material response to those who "isolate" themselves in public spaces: Snakes & Lattes Board Game Café, a café in Toronto that bans wifi and laptops and encourages sociability through board game playing in public. This chapter argues that people have always used mobile objects—books, magazines, newspapers, board games, cigarettes, cell phones, laptops, and so forth—in order to manage and interact with their environments. Objects serve as a sort of *ethos* that people use to create relationships and to create private spaces. What makes laptops and cell phones different than other mobile objects is the secrecy of what's behind the screen. Drawing on Jason Farman's work on mobile interfaces and Shuhei Hosokawa's theorizing of the Walkman, Sony's mobile audio cassette player, I theorize that mobile devices are particularly disturbing because accesses to virtuals proliferate—but virtuals are secret and not available to others. Nostalgia for face-to-face sociality in coffee shops serves to ignore the nuances of actual practices in public spaces—

particularly how these practices are embodied and have a strong sense of place—and privilege unmediated public discourse while ignoring that even coffee shops have historically been sites of secrecy, discourse mediated through multimodal literacy, and mobility.

In Chapter 3, I investigate issues of privacy and identity by turning to the case of Tyler Clementi, the gay Rutgers undergraduate who committed suicide in 2008 after his roommate, Dharun Ravi, spied on him using a webcam. When reporting on the invasion of privacy and Clementi's suicide, mass media portrayed the situation as a case of recorded sex posted online and made public, and that Ravi's invasion of Clementi's sexual experiences *caused* Clementi's suicide. In actuality, there was no sex, no recorded video, no posting online for public access, and likely no causation. What I find more interesting, then, is the literate and discursive activities before, during, and after the webcam incident. Before meeting Clementi, Ravi spent time researching Clementi online, developing an image of who Clementi was based on his externalized private information left on various sites. Mass media, particularly the website *Gawker*, followed a similar logic regarding Clementi, attempting to discover who exactly he was through his mediated traces left online. During Ravi's trial for invasions of privacy, bias intimidation (New Jersey's term for a hate crime), and tampering with evidence and a witness, digital evidence was again key, used to make arguments about Ravi's character (as a homophobe). I use these examples to argue that identity is increasingly externalized online, left as a series of digital traces that others use to construct one's identity. Rhetorical scholars have typically approached identity online as situated performances, but I argue it is just as necessary to attend to how people construct others' identities through their private information posted in various locations online.

In Chapter 4, I turn to the moral panic surrounding sexting, the sending and receiving of sexually explicit or suggestive images and texts. Sexting has become a particular problem because when teenagers have sent sexualized images of themselves, others in their schools have forwarded these on, resulting in extreme bullying, suicides, and strong legal penalties for

teenagers. The moral panic surrounding bullying has resulted in a "public pedagogy" (Giroux, *The Abandoned Generation* 38) about sexting that teaches young women to protect their privacy and just not sext, rather than explore the ethics of not sharing others' images. I argue that, like other moral panics, this moral panic has targeted the wrong problem: Sexting is not the problem, but rather a sexist cultural logic of privacy that blames young women and girls for making themselves vulnerable disproportionately to how much blame it puts on others—particularly young men who expect to receive such images and forward them on. Privacy, then, is still incredibly gendered, and our culture has not yet extended the sorts of expectations and rights of privacy to women and girls as it extends to men and boys.

Chapter 5 shifts its attention to the film *We Live in Public*, Ondi Timoner's 2009 Sundance-award-winning documentary about the rise and fall of 1990s dot com millionaire Josh Harris and his socio-technological experiments about surveillance and privacy. In his 1999 project Quiet, Harris constructed a capsule hotel where residents lived under constant camera surveillance for nearly a month without leaving, and in 2000, Harris and his girlfriend Tanya Corrin lived in their apartment with dozens of webcams broadcasting their lives on the website weliveinpublic.com. Both experiments resulted in the breakdown of sociality, as participants in Quiet expressed that they were unable to develop intimacy without any privacy and even felt their sense of self deteriorating. Eventually, violence broke out as well. Harris and Corrin's relationship fell apart, in part because they began to perform for the camera rather than to actually discuss issues and problems with each other. Timoner understands her film as a parable for the dangers of sharing too much online on social media, and reviewers of the film followed her lead, expressing that it was a "warning shot" for users of social media. I argue that the film has much to teach about the values of privacy—it is important for developing identities and relationships—but not so much to teach us about sociability on social media sites. The film takes the materiality of Harris's experiments as a precursor to social media, but the architecture of his experiments differs

drastically from social media interfaces. Further, Harris's experiments ignore how bodies are practiced. In order to explore sociability on social media sites, I argue, we need to attend to the particulars of specific interfaces, as well as users' media ideologies, idioms of practice, and "sensuous training" (Wysocki, "Unfitting Beauties" 104), or how our bodies have been trained for affective and aesthetic responses to texts. Grand narratives about the future of sociability online are typically misguided, as they miss the nuances of actual bodily practices with digital media in specific ecologies.

In the conclusion, Chapter 6, I turn to the question, "What might digital literacies of privacy look like?" As I have already argued, managing privacy online is a highly literate set of practices and activities. In the conclusion, I outline a heuristic for understanding the literacies necessary for managing privacy on social media sites, drawing on Selber's distinction between functional, critical, and rhetorical literacies. As Selber explains, these literacies are fundamentally social, even functional literacy, which often gets dismissed as being a "simple nuts-and-bolts matter" and as repressive (32-33). Facebook's privacy settings make the social aspect of functional literacy quite apparent: Understanding and knowing how to use settings on a social media site is inherently social, as these settings are helping to situate how and in what contexts users relate to others in the service. In laying out this heuristic of literate practices related to privacy, I do not mean to emphasize just *protecting* one's privacy online. Instead, I draw on several political and ethical implications of my discussion throughout the conclusion. For example, users of social media sites need to have critical approaches to the historical and current uses of *privacy* that have excluded certain populations—women and girls, particularly, but also racial and sexual minorities—from full civic participation. In a sense, a full rhetorical literacy of privacy helps social media users understand that *privacy* is arguable, up for deliberation, political, and contextual. As social media becomes more and more integrated into many of our everyday lives—and as our students continue to turn to social media services in their social and political

lives, and we ask them to investigate them as rhetorical sites and use them in our classes—it becomes increasingly important to develop a critical literacy of privacy for social media environments.