MyDigitalFootprint.ORG:
Young People and the Proprietary Ecology of Everyday Data

by

Gregory T. Donovan

A dissertation submitted to the Graduate Faculty in Psychology in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2013

© 2013

Gregory T. Donovan

Some Rights Reserved
(See: Appendix A)

This manuscript has been read and accepted for the
Graduate Faculty in Psychology in satisfaction of the
dissertation requirement for the degree of Doctor of Philosophy.

Cindi Katz, PhD

Date — *Chair of Examining Committee*

Maureen O'Connor, PhD

Date — *Executive Officer*

Michelle Fine, PhD

Joseph Glick, PhD

Joan Greenbaum, PhD

Torin Monahan, PhD

Anders Albrechtslund, PhD

Supervisory Committee

The City University of New York

To my parents,

Joanne C. Donovan & Martin Leo Donovan

Abstract

MyDigitalFootprint.ORG:
Young People and the Proprietary Ecology of Everyday Data

by

Gregory T. Donovan

Advisor: Professor Cindi Katz

Young people are the canaries in our contemporary data mine. They are at the forefront of complex negotiations over privacy, property, and security in environments saturated with information systems. The productive and entertaining promises of proprietary media have led to widespread adoption among youth whose daily activities now generate troves of data that are mined for governance and profit. As they text, email, network, and search within these proprietary ecologies, young people's identity configurations link up with modes of capitalist production. The MyDigitalFootprint.ORG Project was thus initiated to unpack and engage young people's material social relations with/in proprietary ecologies through participatory action design research. The project began by interviewing New Yorkers ages 14-19. Five of these interviewees then participated as co-researchers in a Youth Design and Research Collective (YDRC) to analyze interview findings through the collaborative design of an open source social network. In taking a medium as our method, co-researchers took on the role of social network producers and gained new perspectives otherwise mystified to consumers. Considering my work with the YDRC I argue that involving youth in designing information ecologies fosters critical capacities for participating in acts of research and knowledge production. More critical participation in these ecologies, even proprietary ones, is necessary for opening opaque aspects of our environment and orienting data circulation toward more equitable and just ends.

Acknowledgments

The time and space necessary for developing this project was afforded by friends and family, mentors and colleagues, institutions and collectives. Developing a dissertation can be a socially isolating journey but the following people engaged me in situations that opened my mind, fed my soul, and shaped my scholarship along the way:

The CUNY Graduate Center, who gave me a radical community and a public education. Bill Kelly, Louise Lennihan, Sharon Lerner, Elise Perram, and Matthew Schoengood, who gave me meaningful opportunities to participate in university governance. Setha Low and the Public Space Research Group, who taught me how to do critical ethnographic research and to consider how privatization operates in public. Susan Saegert and the Housing Environments Research Group, who taught me to consider how privatization operates at home. Jared Becker, Hillary Caldwell, David Chapin, Roger Hart, Yvonne Hung, Judith Kubran, Einat Manoff, John Seley, and the Environmental Psychology Program, who taught me that everyday life is a field of study. Neil Smith, who passionately led a yearlong seminar at the Center for Place, Culture and Politics on Geopolitics and (In)Security while I was developing the proposal for this project. That year at the CPCP entailed an international and interdisciplinary dialogue with Bruce Braun, Patricia Clough, Ervin Costa, Deb Cowan, Tina Harris, David Harvey, Elizabeth Johnson, John Morrissey, Charlotte Recoquillon, and Ros Petchesky that gave a new relevance to my research.

Desiree Fields and Kim Libman, who kept me fed, informed, and thoroughly entertained while I wrote this dissertation. Kiersten Greene and Collette Sosnowy, who have been a steady source of support and a constant reminder of how lucky I am to have *you* as colleagues. Jen Jack Gieseking, my companion in this academic journey, who live-tweeted my defense, brought me to Berlin, and taught me to queer life. Aga Skorupka, who radiates strength and who showed interest in my research when I could not. Over coffee in Oslo, Aga brought me to the finish line. Lisa Brundage, Joseph Ugoretz, and the Macaulay Instructional Technology Fellows, who made me a more knowledgeable teacher and helped me think through the pedagogical and technological aspects of my research. Maggie Galvan, and my fellow participants in the OpenCUNY Academic Medium, who have helped me imagine what an open and participatory information ecology might look like. Maria Tore, Caitlin Cahill, and my fellow researchers at the Public Science Project, who provided me with a methodological home and an epistemological stance.

Joana Amaral, Molly Boyle, and Jessica Warren, teachers who believed in me and encouraged me to leave MA for an adventure in NYC. For my high school graduation they gave me Bartlett's *Roget's Thesaurus*, Jung's *Undiscovered Self*, and a sketch pad. They gave me tools for life that have served me well. Jennifer Kotler Clarke, David Cohen, and everyone at Sesame Workshop, who showed me the educational potential of media. Jennifer was the first to encourage me to pursue a doctorate, in fact she was adamant about it, and she has been a cherished friend ever since. Linda Solomon and the Psychology Department at Marymount Manhattan College, who gave me opportunities to learn, teach, and grow as a scholar. Wolfgang Kleinwächter, who

brought me to an East German monastery for two weeks to learn about internet governance from the likes of Milton Mueller, Avri Doria, Olga Cavalli, and Christopher Buckridge.

Matthew Cline, Jason Gardner, Sarah Kiernan, Tracy Motz, Meryl Schienman Van Meter, and Becca Woodrich Zohar who made a family for me in New York, who kept me sane, and who reminded me to have fun. That you responded to so many irrational texts, calls, and emails during the most stressful moments of this project is a testament to our undying friendship -- and your tolerance. Jennifer Oriola Collins, Katie Duggan Fierimonte, Jessica Redman Johnson, Harry Nedley, and Jeffrey Porrier, friends from youth who supported me through challenging times and continue to be a loving and creative presence in my life. The Donovan and Gioioso families, who taught me how to love, support, and debate those you disagree with. My grandmothers, Alice Donovan and Libera Maria Gioioso, who taught me the meaning of sacrifice, the value of work, the horrors of war, and the need for social justice. My parents, who taught me to apply myself, to be honorable, to challenge norms, and to be patient with the slow but inevitable acceptance of progress. My sister, Elyse, who kept me grounded and keeps me laughing. My goddaughter, McKenna, who fills my heart with the joys of youth.

My dissertation committee, each of who represents the kind of critical scholar I aspire to be: Anders Albrechtslund, who got me to rethink my metaphors and reconsider the power dynamics of social networks. Joe Glick, who greatly expanded my reading list. Meetings with Joe entailed exciting discussions of social theory, personal histories, politics, and cultural psychology that always left me asking new questions and ordering more books. Torin Monahan, who brought me to Nashville and encouraged me to consider surveillance as a potentially empowering practice. Torin engaged me with the field of surveillance studies and I am grateful for his generosity of time and knowledge. Michelle Fine, who gave me a hunger for more democratic approaches to knowledge production. Michelle was instrumental in helping me develop the methodology for this project and has been an indispensable mentor. The incredible speed, depth, and purpose at which Michelle operates have been an inspiration to witness. Joan Greenbaum, who got me to think about the role of technology in labor relations and the need to agitate, educate, and organize. Joan has been a mentor, a teacher, a co-researcher, a friend, and a fellow dreamer for a more just society. Joan's dedication to her students is an example of education at its finest.

My advisor and mentor, Cindi Katz, who guided this project from its inception and who talked me off a ledge more than once. Cindi taught me about the problems and possibilities of social reproduction, the power of play, the significance of the banal, and the fun of studying young people's geographies. Cindi has opened her mind, her heart, and -- literally -- her home to give me the time and space to find my voice. No words can properly convey my gratitude. It has been an honor to be her student. Thank you, Cindi.

Finally - I wish to acknowledge Asmaou, Kaitlin, Rose, Saif, and Yvonne, who shared their knowledge with me and made me excited for the future. To state the obvious: this project was only possible because of their interest and participation. Thank you.

Table of Contents

List of Figures

Chapter One
Canaries in the Data Mine

When canaries in a coal mine stop singing it's an early indicator of a toxic environment. It is thus sound ecology to closely consider the interests and concerns of canaries, and foster an environment that keeps them singing. The explosive growth of data generation, consumption, and circulation in advanced capitalist nations has given way to the popularization of a new term often cited in IT circles without the slightest connection to its 'big brother' and 'big government' surveillant connotations: 'big data.' This term refers to the massive and complex data sets being generated about seemingly everything and everyone at all times through the ubiquity of information communication technologies (ICTs). The aim of corporations and governments alike is to figure out how to meaningfully mine and aggregate big data to produce actionable intelligence, and thus economic value. This entails the development of new markets, presupposed by capitalist regimes of property ownership, that enclose data and thus 'monetize' access to the information and knowledge produced from it.[1] In this mad dash to mine, with little debate around people's representation in and access to such data generation, consumption, and circulation, young people are sent foremost into the depths of this data mine.

'The internet' was a phrase the young people I interviewed often used to describe the ICTs in their everyday environments. After 16-year-old Felicia expressed her displeasure with

---

[1] I consider the terms 'data,' 'information,' and 'knowledge' as interdependent phenomena that can be distinguished from each other based on their roles in capitalist production. 'Data' is generally presented as objective and discrete facts, 'information' as the intentional aggregation and circulation of certain data, and 'knowledge' as the application of this information towards personal and collective understandings. This hierarchical production process of generating data for aggregation and circulation in information systems that provide knowledge about people, places, and things is the core of both data mining and broader informational development.

'the internet using a friend's picture in a Facebook ad,' I asked her who or what she thought 'the internet' was.[2] Felicia, a young black woman from the Bronx, referred to an anonymous character from the television drama *Gossip Girl* in her response. The so-called 'Gossip Girl' collects the secrets of young socialites at an elite Manhattan prep school, and reveals them to the public anonymously through *his* personal blog.[3] Gossip Girl's disclosures incite drama each episode as a mostly white cast struggles with the unwanted attention their much-wanted popularity has brought them. This plot line resonated with Felicia's own experience and helped her articulate how she saw the internet as an entity produced through human activity with virtues and vices reflective of its producers:

> [The internet] is us. It's like a Gossip Girl because everything—we created the internet. And so, everything on the internet, we made, we put up there. We decided to use it. We made it accessible.

Most young people I spoke with similarly described the internet as a collective expression of social and material culture. For most, the sense that they could no longer draw a clear boundary between the internet and their daily routines -- or between an 'online' experience and 'offline' experience -- undergirded broader concerns. As Felicia elaborates:

> We made it so big that everyone wanted to use it. And so, it's like—it's just like a Gossip Girl, like we started it and then, we just keep making it better and making it worse and just adding more stuff to it, as if it was a box. And eventually, it's going to explode and

---

[2] Facebook reserves the right to use the names and pictures of its U.S. users in advertisements unless they opt-out of this practice. Felicia described an advertisement on Facebook featuring her friend recommending a product she knew her friend did not 'like' and would not recommend. Felicia expressed surprise that Facebook could do this and worried how her own name and image may have been used in advertisements, yet she also expressed guilt that this was somehow her own fault for not knowing to opt-out of such practices.

[3] Although the "Gossip Girl" anonymously narrated each episode with a female voice, it was revealed in the final episode to be one of the show's leading male characters.

> everything's going to come out, but it just hasn't happened yet. But it's happening, it's spilling over, trust me.

Concern about the ways the internet was "spilling over" into all aspects of life was common and speaks to the bigness of big data. Although the Gossip Girl uses a blog to publish and publicize private information, his communicative presence in the everyday environments of his peers extends well beyond the moments when they deliberately go online and visit his blog. Unlike gossip that takes place in the school yard through word of mouth, this mediated gossip can be stored and combined with other gossip overtime and is generated and accessed from multiple locations. When Gossip Girl publishes a new post, mobile "alerts" are sent out to the phones of his blog's subscribers. Conversely, the gossip disclosed is received as "tips" submitted by peers who email and text him the private details of others. The aggregation and circulation of gossip happening online thus 'spills over' into common routines from math class to dinner with the family.

Four other young women made similar references to *Gossip Girl* in discussing how matters such as cyberbullying and identity theft were a result of people's own actions and desires. Just as Gossip Girl derives information and influence from peers who submit "tips" and subscribe to "alerts," the internet was discussed as something they and their peers were "feeding into" or "addicted to." Their everyday experiences with the internet revealed an intimate, if partial, knowledge of the ways people, place, and media are shaping one another. Through a critical participatory and ecological approach, my aim in this dissertation is to unpack the 'box' that Felicia describes as the internet to understand its role in young people's negotiations of

property, privacy, and security amidst the routine surveillance and mining of their mediated experiences.

Akin to industrial coal mining, contemporary data mining typically entails the enclosure and subsequent regulation of access to public resources for the purposes of private capital accumulation. With people's mediated experiences the new coal mine, and data the new coal, this form of accumulation brings regimes of property ownership into contact with personal and collective understandings of privacy and security. A person's engagements with proprietary social networks such as Facebook generate a range of data including, but not limited to, geographic location, public and interpersonal communications, as well as consumption patterns. This personal data then becomes mined and monetize by corporations with minimal government regulation. Who can and cannot access a person's data, what control a person has in how this data represents them in information ecologies, as well as when and where knowledge derived from these ecologies is made use of ultimately shape what sense of privacy and security people feel they have. In the context of youth, personal and collective understandings of property, privacy, and security can prevent, modulate, or accelerate social acceptance of such data mining as well as the broader socioeconomic development with which it is associated. Minding the interests and concerns of young people, such as Felicia, helps mind this gap between large scale data mining and situated experience; and thus foster understandings of privacy, property, and security that linkup with and support broader movements around socioeconomic and geographic justice.

The expansion of ICTs in the early 21st century has afforded an information ecology that infuses routine behaviors with market interests and unsettles industrial understandings of privacy,

property, and security. Castells (2000, 2003, 2007a) theorizes the material infrastructure of such ICTs as an informational mode of capitalist development characterized by recombinant abilities, expanding processing capacities, and flexible distribution. Castells (2003) discusses this "informationalism" as a technological paradigm currently restructuring industrial capitalism and providing the material conditions for a new social structure he calls "the network society" (p. 10). While I wish to hold onto Castells' formulation of informationalism as a restructuring technological paradigm, I also wish to acknowledge the shortcomings of his theorization of a network society because it obscures the productive forces and relations of capitalism. As Fuchs (2009) argues:

> [The network society] is an ideology that obscures domination because phenomena such as structural unemployment, rising poverty, social exclusion, the deregulation of the welfare state and of labor rights, and the lowering of wages in order to maximize profits can easily be legitimized in a society where networks are seen as natural organization patterns (p. 392).

As Felicia and other young people I spoke with were keenly aware, the internet and its associated ICTs are not natural phenomena. Information ecologies are dynamic entities that are at once materially and socially produced through human activity. While I find utility in Castells' formulation of capitalist restructuring amidst a new technological paradigm, and here take up the use of 'informational,' his formulation of the material as distinct from the social plays into a false binary of nature and technology, and falls short of fully explaining the concerns of young people like Felicia who sense a naturalization of the internet. This binary is most notable in how he seemingly distinguishes both innovation and technological change from capitalist production. Castells (2003) discusses the uneven geography of informational development and argues an "understanding of how certain institutional environments are conducive to innovation and to

advanced technological change, while others are not, is essential for identifying the sources of wealth, power, and well-being in the world" (p. 20). Yet, such an understanding naturalizes both innovation and technological change by presenting them as a given that certain people and places simply respond to. This fosters an understanding of human-environment interactions that leaves little conceptual room for considering how certain people and places produce innovation and technological change. This can be seen in Castells' (1989) theorization of a "space of flows" as a new industrial space that supersedes a historical "space of places" and is "not dependent on the characteristics of any specific locale" (p. 348) to fulfill its productive goals. The distinction of this space of flows from that 'of places' obscures the architectural, legal, social, and built ways that historical notions of place shape the production of this 'new' space. The characteristics of a specific locale such as California, where the International Corporation for Assigned Names and Numbers (ICANN) is organized as a nonprofit corporation, certainly has significant influence over transnational data flows.[4] As Felicia previously noted "the internet is us" and thus cannot be divorced from our historical geography or humanity.

I consider informationalism more critically in the context of young people's environments as a social material process rooted in a neoliberal history of accumulation by dispossession. Harvey (2010) sees privatization as a primary mode of such accumulation in the contemporary neoliberal state, serving to enclose the public commons and consolidate class power. Harvey notes that this process is different, but not detached, from accumulation through the exploitation of labor, as accumulation by dispossession produces capital through the

[4] The International Corporation for Assigned Names and Numbers (ICANN) is organized as a tax-exempt 501(c)(3) in California, and oversees the global management and assignment of domain names and IP addresses.

privatization of public resources and subsequent regulation of access to such resources. Things like personalities, interpersonal communication, and social networks all become privatized resources that people must increasingly pay to access.[5] Fuchs (2009) helps us see how dispossession plays out in an informational context:

> If capitalism is indeed organized as a global network economy, then one has to stress that the spatial geography of this economy is devised in such a way that there is a class of central hubs (corporations, countries, cities, city zones, regions, occupational groups, classes, individuals) that controls the flows of property, money, and goods in the network, hence creates an asymmetrical, divided, exclusive economic space where the majority of people are marginalized and kept outside the network and a divided geography is created (p. 395).

Such a formulation accounts for the material social processes behind informationalism in noting that the economy is intentionally "devised" with "a class of central hubs." If one is kept outside the network, then access to data and information becomes more difficult as does their ability to develop the knowledge necessary to empower themselves within the network or through the creation of other networks. This does not imply infallible domination but it speaks to the ways class power is consolidated by the intentional structuring of flows within a fragmented geography interconnected through information ecologies.

Contemporary information flows are spatially produced and governed in ways largely consistent with a neoliberal doctrine of private property ownership and increasingly private governance models. This can be seen most overtly in such phenomena as the 'semantic web.' The world wide web (WWW) was developed primarily by Tim Burners-Lee in the early 1990s as

---

[5] In some cases this 'pay' is monetary, such as how one typically pays a monthly fee for internet access. In other cases, access to these privatized resources are 'no-fee' such as how one pays no money to use Google's email service yet still 'pay' by viewing advertisements and giving up personal data.

a series of protocols that afford the linking and accessing of hypertext through the internet. The semantic web can be understood broadly as a sustained indexing of the WWW, whereby data is semantically coded to produce information that can then be processed and interpreted through automated analysis. In other words, the semantic web occludes the decisions and judgments of web surfing to search for and deliver information to users. This 'automation' is a notable feature of the semantic web as it suggests information processing between computers without human intervention, thus implying an objective and predictive organization of data into various information systems. An example of this automation can be found in the ways Google tracks a person's online behavior and location to predict the search results a person wants to find based on their search query. Thus, two different people may enter the same search query into Google, but receive two different search results. While this can prove exceptionally useful in quickly delivering the information people might be looking for, it also encloses people in what Pariser (2011) has described as a "filter bubble" or a personally customized ecosystem of information that reinforces a person's existing behaviors and opinions while occluding different viewpoints. In Berners-Lee (1999) discussion of the semantic web he notes that while such automation is necessary so that people can better navigate the massive amounts of online data, he emphasizes that the algorithms and methodologies behind these processes must be transparent and accessible to everyday people so that they may consider the ways their information consumption is mediated. Yet, such algorithms and methodologies are the secret sauce of Google's business model that gives them an edge over their competitors and thus made proprietary.

To semantically code and then circulate data, it must first be sorted and categorically conformed. The semantic web constitutes new ontologies, such as the Web Ontology Language

(OWL), that make information more locative, circulatory and integrable.[6] In doing so, this semantic shift lubricates informational navigation but also erodes the architectural qualities of the internet that afforded higher degrees of privacy and anonymity through highly diffused and decentralized data circulation and storage (cf. Lessig, 2006). Personal data left on different severs by visiting different websites was literally *left there*. Now, this data is continuously fused and aggregated across multiple servers in broader information ecologies. Semantic ontologies, such as OWL, incentivized greater levels of data aggregation and mining by cheaply and quickly networking disparate data. As a set of organizing principles, the semantic web *itself* does not represent dispossession or privatization, yet information businesses such as Google or Facebook accumulate capital in relation to the semantic web by enclosing everyday data and controlling not just access to it, but the information and knowledge production associated with it. I consider this privatization of everyday data as dispossession because everyday people become increasingly dependent on private corporations to make sense of their own data and the data generated in and by their social networks. This form of accumulation by dispossession calls for a steadily increasing flow of data as well as the production of spaces to capture, store, mine, and control access to such data. Young people's experiences amidst this process make them canaries in the contemporary data mine.

In the context of young people's development this situation calls for a more critical consideration of how participation in privatized information ecologies -- what I refer to as 'proprietary ecologies' -- produces and reinforces historical geographies of domination. Proprietary ecologies afford a multidimensional ecosystem of proprietary data flows within

[6] For more detailed information on the Wed Ontology Language (OWL), see the World Wide Web Consortium's summary at http://www.w3.org/TR/owl-features/

which everyday human-environment interactions take place and are thus mediated by the interests of any number of proprietors. Through the material social constitution of proprietary ecologies, capitalist actors like Facebook, Google, and the US Government can develop platforms and practices that privatize and control access to phenomena such as personalities, reputations, communications, and social networks. I theorize this as an 'ecology' because the concept bridges an IT discourse of information systems that interact at various scales (i.e., information ecologies) with a spatial understanding of the relations of production and reproduction (i.e., political ecology).

Proprietary ecologies are thus the medium and the method of accumulation by dispossession in an informational context. Although informational empowerment is possible, even within such ecologies, it remains a material social process like informational domination and thus calls for a dissolving of dualisms and an embrace of the dialectic to realize its potential. This means considering how proprietary media such as Google or Facebook can afford empowerment, domination, or both depending on the situated human practices that create and make use of them in different contexts.

As young bodies bond with increasingly mobile and ever shrinking hardware, their minds mesh with increasingly connective and ever-diffused software. In both cases, the software and hardware is typically produced and owned by a corporate entity. The result is a real-time and reciprocal loop of information production and consumption that expands the field of mediation in everyday human-environment interactions. The reciprocity of this loop tightly couples human development with a transnational informational development that commonly manifests in such everyday forms as intellectual property and data mining practices. This hybrid development

means a generation of young people embodying Donna Haraway's metaphorical cyborg through their psychosocial configuration in a proprietary ecology. Their situated understandings, as well as broader social norms around matters of privacy, property, and security are thus developed in hybridity.

I draw the term 'human-environment interactions' from the field of environmental psychology to account for a person's interactions with their surroundings; theorized as a gestalt construction of people, places, and things (Proshansky, Fabian, & Kaminoff, 1983). This approach comports with the ideas associated with Actor Network Theory (ANT) in media, information, and technology studies. ANT holds that any matter of concern is an assemblage of human and non-human actors, the multidirectional power relations of which are often the object of inquiry (Latour, 2005). However, in emphasizing the relations between humans and their environment rather than humans and non-humans, I emphasize the contextualized and situated ways assembled networks of social relations play out ecologically in individual and collective experience.

It is thus the mutual shaping of young people's development and informational development within everyday environments that is my object of inquiry. I look at the restructuring of young people's environments to understand how informationalism is socially and materially produced and reproduced in situated locations. In an informational context, this means looking at how our increasing dependence on debit cards, mobile technologies, social media, data mining, and ever expanding and securitized intellectual property regimes shape particular understandings of privacy, property, and security. This perspective also calls for looking at how such understandings in turn shape informational development.

The scope of privatization in everyday information ecologies can make it daunting and dystopian to consider, leading more than just Felicia to feel Pandora's box is ready to burst. So much of the media we routinely engage with is proprietary that it is generally only brought into focus through contradiction in discussions of free software, 'software libre,' 'copylefts,' or open source.[7] Propriety has become a default setting in the culture, practices, and architecture of most information ecologies, yet it remains an important focus of analysis even when the aim is to foster a more free and open information ecology. While daunting, this privatization is not a monological process. Human-environment interactions are reciprocal and emergent phenomena, meaning that human activities such as privatization are not only part of our environment but also our selves; at once material and social. Harvey (1973) notes that "human activity creates the needs for specific spatial concepts" (p. 14) that can be absolute, relative, and/or relational. Proprietary ecologies thus exist as a result of human activity; specifically, capitalist relations of production. In taking the "property relationship" as an example, Harvey argues that it "creates absolute spaces in which monopoly control can operate" (p.14). The desire of corporations and governments to enclose and regulate data flows into absolute spaces that produce profit and control thus creates a need for proprietary ecologies. These ecologies are also sustained by people who continue to participate in them for a variety of reasons. I wish to emphasize that people, particularly young people, can rework and even resist their privatized surroundings

[7] Each of these forms still embraces a capitalist approach to private property ownership, yet they seek to invert this process by owning property in order to then make it publicly accessible. A notable example can be found in Linux, the most popular free and open source operating system. Linux is licensed under a copyright that makes its development and distribution open to the public and thus prevents another entity from copyrighting it for profit in the way Microsoft and Apple have done with their respective proprietary operating systems.

through material social practices that produce historical geographies more representative of their own interests and concerns. Their activities also create a need for specific spatial concepts.

Young people are a highly sought after consumer demographic in the US economy. According to Harris Interactive (2010), US youth ages 8-24 have a collective annual spending power of $239 billion that continues to increase despite decreases among other demographics as a result of rising unemployment and reduced wages. As adults spend less on themselves, they continue to spend more on their children and the children of others. This social positioning makes youth a significant object of market interest, which in turn aims to embed them in proprietary ecologies to influence and take advantage of their consumption patterns. This strategic embedding also places them in an environment fraught with phenomena such as cyberbullying, sexting, intellectual property disputes, data mining, and national cybersecurity. This positioning does not make them more endangered or empowered than any other age group, but it does put them at the fore of socioeconomic restructuring.

These dynamic interactions of acceptance, resistance, and reworking in proprietary ecologies constitute an individual's or group's situated knowledge, the unpacking of which can help us understand how the proprietary remains a default setting in contemporary life. As Haraway (1991) and Katz (2001) argue, understanding the objects of transnational domination and their situated lives, offers new perspectives that often question and re-imagine broader modes of production and reproduction in society. In other words, the objects of domination know it well, and it is precisely this epistemology that warrants attention.

With this in mind, I interviewed New Yorkers ages 14-19 as part of the MyDigitalFootprint.ORG Project to better understand their routine interactions with proprietary

media as well as the interests and concerns they associated with such interactions. During the first interviews I brought a list of the most common search engines, cell phones, gaming consoles, social networks, web browsers, and media libraries. I anticipated going through this list towards the end of each interview to assess participants' familiarity with, and feelings towards, each. By the third interview it became obvious there was no need for prompts. While the esoteric distinction of 'proprietary' was never made, the identification of corporately owned media such as Google, Apple, Microsoft, and Facebook permeated their descriptions of everyday routines.

This personal-proprietary coupling represents a dialectic of empowerment and domination. Although this coupling implicates society at large, I argue that young people are the canaries in this data mine because their ecological sensitivity attunes them to subtle environmental change. As young people develop in proprietary ecologies riddled with privacy, property and security disputes, their situated interests and concerns are negotiated in relation to those of governments and corporations. Their interests in and negotiations of these conditions may serve as early indicators for broader material social change. Through an analysis of the MyDigitalFootprint.ORG Project, I take a critical ecological approach to understanding the mutual shaping of people, place, and media through the situated experiences of young people coming of age in proprietary environments. I began this project with a series of 15 interviews to compare and contrast young people's privacy, property, and security concerns within such environments.

Following these interviews, I engaged in participatory research and design with a group of five young co-researchers to further investigate the interests and concerns that emerged in the interviews through the development of an open source social network. These five young people,

ages 15-19, made up the Youth Design and Research Collective (YDRC) and worked with me in a series of eight workshops over six months. The workshops began with tutorials on information and network architecture, internet governance, qualitative research, free and open source software, and universal access to enhance the YDRC's consciousness in everyday information environments as well as provide the literacies and shared vocabularies necessary to codevelop our social network. Chapter Three provides a more detailed discussion of the participatory action design research (PADR) approach of the MyDigitalFootprint.ORG Project as well as the various ways participants were recruited and involved in both interviews and workshops. To protect their privacy I use pseudonyms for all participants, and have omitted all personally identifiable information about them here. All interviewees, and their parents if they were under 18, signed consent forms before being interviewed and all consented to the recording of their interviews for transcription purposes.

As the most wired segments of advanced capitalist societies, young people are aware of the spillage taking place as ICTs permeate the everyday. That is, the way data seems no longer containable in discrete spatial-temporalities and thus flows into the most banal routines: browsing YouTube at school, emailing a teacher while sitting down to dinner, or texting with a friend in bed. "The internet" as one interviewee put it "is everything." The young people I interviewed were excited by the possibilities this brings, and they were experienced in the problems it poses. For Felicia, there is a particular concern that the collective 'boxing' and compartmentalizing of everyday mediation is leaving us situationally unaware and thus vulnerable to harming ourselves. When I asked Felicia what she found most concerning about this 'spillage' she raised issues of abduction and authenticity:

> The predator part. Like, everyone that made a chat room so you can have like instant messaging so things could move way faster and way better, but the nasty men now know. Old men are talking to young girls because you can't really see the little pictures, and it's just stuff like that. And then, you can—the whole—it's like the whole internet-fake stuff, it's like everything is fake on the internet—it's not that *everything* is fake, but the whole Wikipedia, you can add your own information to history. You weren't there, how do you add information into history?

Crouched in these concerns of abduction and authenticity is a depiction of "young girls" that don't realize they're chatting with "nasty men" and people who think they're reading encyclopedic information in a dubious Wikipedia. In both cases, Felicia suggests things are not what they seem, and people's failure to fully understand what or who they're interacting with renders them potential victims of "fake" information or worse, "nasty men." Felicia sees vulnerability in failing to understand the boundaries and dynamics of a situation; that almost anyone could gain entry to a chatroom and represent or misrepresent themselves in any number of ways.

Felicia expressed concern in her interview, but not defeat. Like others I spoke with, Felicia saw our collective production of the internet as having the potential to be as helpful as harmful, and she thought young people held much power in influencing this dynamic: "we really control the internet ... the adults may make it, but we control it." Considering the empirical findings of this research I argue that when young people are engaged as producers of information ecologies and participants in social research, rather than as data consumers and research subjects, they develop greater consciousness within informational environments. Such awareness encourages young people to see themselves as self-possessed social actors, while also affording a framework for youth to collaborate meaningfully with researchers, policymakers, designers,

educators, and other social actors to develop more empowering and accessible environments that are sensitive to the interests and concerns of young people.

In this chapter I draw on in-depth interviews with a sample of 15 young people ages 14-19 living in New York City. It's a snapshot in time, in place, and in depth of the experiences of these young New Yorkers during a stage of their development most concerned with articulating identities and roles in social relationships. The period of time in which most interviews occurred saw the national release of *The Social Network*, WikiLeaks erupt as a massive news story with the arrest its founder Julian Assange, the uprisings in Iran, Egypt, and Libya, and the suicide of a freshman at Rutgers University provoked by his dorm mate 'outing' him online. These events took place alongside ongoing realities of a post-9/11 security state, post-No Child Left Behind educational environment, and paranoia around cyberbullying, sexting, file sharing, and child predators on the internet. Each of these phenomena were referred to directly or indirectly by interviewees in articulating their interests and concerns around matters of privacy property and security.

Privacy, property, and security are dynamic matters experienced in situated, relational, and often contradictory fashion; each produced through a complex assemblage of human-environment interactions. Semi-structured interviews offer a way to explore the diverse understandings of these dynamics in-depth, and to compare individual understandings with one another and analyze them in the context of more generalized and popularized understandings of privacy, property and security. As Crouch and McKenzie (2006) argue, such a small sample qualitative approach "is therefore clinical, involving as it does careful history-taking, cross-case comparisons, intuitive judgments and reference to extant theoretical knowledge" and "positively

calls for a collection of respondents' 'states', the size of which can be kept in the researcher's mind as a totality under investigation at all stages of the research" (p. 493). Young people who fiercely guard their privacy were unlikely to travel to midtown Manhattan to discuss their media habits in a 1-to-2-hour long interview with someone they didn't know. Those who did show up, then, were young people who wanted to talk about their interest and concerns about the internet.

In the following sections I outline young people's hybrid development in proprietary ecologies, how this development links up with broader modes of transnational regimes of informational capitalism, and what interests and concerns this connectivity generates among young people around matters of privacy, property, and security. In each instance I draw on my interviews with young people to situate this discussion in a critical consideration of the way these issues play out in the dynamic flow of everyday life. It is important to emphasize that I do not see matters of privacy, property and security as independent phenomena, nor did the young people I interviewed. At the close of each interview I asked participants what the words "privacy," "property," and "security" meant to them. Whitney, 16, offered distinct and elaborate explanations of what each of these three words meant to her but she also saw the interdependence of such matters:

> I think all those words are related to each other too because you have to -- even though you want to still be private, you still want to be secure about the stuff that you're now private with, and you want other people to know that that's your property so don't touch it. Or, you want to be aware of other people's property, so you know not to touch it or violate it in anyway.

I then asked Whitney if she felt this interdependence was complicated or confused at all by the internet:

> Yeah, because I think then you'll be wanting to share stuff because you'll be happy. Or like save it, or you just want -- you want a certain amount of people that you can now reach to everyday to know, but you still can't let them know because you don't know who else is going to know from them knowing -- you don't want everybody to know. So you still want to be private about it.

Like Felicia and the characters of *Gossip Girl*, Whitney struggles with the unwanted attention and situational dysphoria resulting from desired connectivity. As Whitney, Felicia, and other young people negotiate often amorphous and overlapping matters of privacy, property, and security resulting from 'the internet spilling over' into everyday life, governments and corporations are working to negotiate such spillage toward interests of capital accumulation and national security.

Growing Cyborgs

> We are all chimeras, theorized and fabricated hybrids of machine and organism; in short, we are cyborgs. -- Donna Haraway (1991, p. 150)

> So, I just think like as time goes on, I think that the internet is going to become -- like -- everything. -- Orlando, 14

Development in proprietary ecologies begins at the earliest stages of the life course for young Americans like Felicia, Whitney, and others I interviewed. According to the Pew Internet & American Life Project, 77% of US youth ages 12 to 17 have a cell phone (Lenhart, 2012), while 95% have internet access and 80% of those with internet access use social media sites (Lenhart et al., 2011). According to Nielsen Ratings, the monthly data consumed by the average smartphone user grew from 230MB a month in 2010 to 435MB in 2011, an 89% increase (Nielsen Wire, 2011a). A separate Nielsen report measuring all mobile phone users found data

consumption strongest among young people ages 13 to 17 with a monthly average of 320MB in 2011, a 256% increase over 2010 monthly averages (Nielsen Wire, 2011b).[8] The same report found voice calls to have decreased among young people and attributed most of the data growth to an increase in mobile internet, apps, email, texting, and social networking. Texting was the most popular of these activities, with 13 to 17 year olds exchanging an average of 3,417 messages per month.

Most young people I interviewed described such routinized practices of data consumption and production with pleasure, disdain, and indifference. This is not to suggest that some interviewees expressed pleasure while others disdain or indifference, but that these three feelings emerge at some point in every interview as young people discussed these complex and often contradictory practices. At 16, Nicole was like many other interviewees in finding it easier to articulate when and where she doesn't text then when and where she does:

> I don't text while I'm sleeping, so that's -- that would be the only time unless my phone dies, or I'm in a meeting like this, or I'm playing soccer for a while. The times like that where I, I physically can't text, like those would be the only times where I'm just not texting. Which it sounds like a really bad thing, and -- but I, I know that sounds bad.

Texting for Nicole is a routinized and banal practice; the absence of which is more notable than its presence. Nicole derives pleasure from the connectivity texting affords yet she feels its persistent presence in her everyday life "sounds bad." When we consider the totality of data

---

[8] 'Smartphones' -- such as the iPhone, Blackberry, or Android phones -- afford internet access, email, and applications along with the voice and texting features of most mobile phones. The Pew Internet & American Life Project reports that 23% of 12 to 17 year olds indicated having a smartphone, while 54% have a regular mobile phone or are not sure what kind of phone they have (Lenhart, 2012). Twelve of the 15 young people I interviewed had mobile phones, nine of which were smartphones.

flows penetrating and emanating from young people's experiences, we find near constant interactions with and within privately owned property. Nicole, and whomever she is texting, may have temporary personal access to the messages they send and receive but so too do the information companies transmitting them. The post-9/11 US government also claims a right to access such messages for national security purposes through legislation such as the Patriot Act. Further, even if this everyday data is anonymized during or after its initial generation, it often becomes de-anonymized as it circulates in broader information ecologies and fuses with other data.

As Ohm (2009) explains, even anonymized data sets contain partial answers to the questions "who does this data describe?" While a person's name, location, IP address, and birthday might be removed from a particular data set, once that set is combined with one or more other data sets involving that person, the vast behavioral information now attributed to an 'anonymized' individual represents a digital footprint more unique than any name or IP address. While several people might share my name and birthday, no one shares my digital footprint. Thus, simply anonymizing data sets through the removal or personally identifiable information, only keeps those sets anonymous if they are never circulated in broader information ecologies. This fact highlights the technical futility of most personal and local privacy settings and raises questions as to what work such privacy settings do besides providing what seems to be a false sense of control over one's privacy.

Nicole wasn't sure exactly what sounded bad about so much texting. Like many interview participants, she expressed a general sense that there must be an unrealized downside to so much connectivity and that this level of engagement isn't "the best use of [her] time." The

data generated from everyday practices such as texting in proprietary ecologies are routinely circulated and fused into 'big data' sets that are privately controlled by one or more entities; most often corporations and governments. The proprietary quality of this generation, circulation, and fusion frames them as trade and/or state secrets that must be enclosed or policed for purposes of corporate competition and/or national security. In this way proprietary ecologies become opaque assemblages, transparent primarily if not exclusively to their owners. Privatization becomes a method by which medium owners mystify their methods of data generation, circulation, and fusion for the general population. One might sense a downside to their participation in practices such as texting, but rarely can they see or articulate what that downside is. Not knowing how 'the internet' -- or a specific medium such as Facebook or Google -- technically and financially operates was a concern interviewees frequently expressed an interest in addressing.

Proprietary ecologies are constituted by regimes of property ownership that have operated historically to enclose and regulate access to the means of production in capitalist societies. As this production increasingly entails informational modes of development, proprietary ecologies facilitate continuity of transnational capitalist power structures. I wish to address this extension of existing regimes of property ownership to language, concepts, algorithms, social networks, and intimate information as a mitigating factor in the dominating and often empowering aspects of informational development.

The embedding of young people in proprietary ecologies has led to their development as what Donna Haraway termed cyborgs. Like Nicole, these cyborgs are more connected to their peers, mass culture, national security, and transnational economies by circuitous data flows than by integrated silicon chips. Contemporary cyborgs are, as Schuurman (2004) argues, "more than

metal and flesh; they come to life in the presence of data" (p. 1337), and their "peer status is established by common data-collection practices, shared goals, and a similar vocabulary" (p. 1339). I consider young people as growing cyborgs to highlight the ways their psychosocial development, and thus their modes of knowing and becoming, are infused with privatized practices of 'following,' 'friending,' 'liking,' 'updating,' 'checking in,' 'reporting errors,' and 'downloading.' That these practices shape identities, are shaped by identities, and generate data to be mined and monetized, brings to the fore the reciprocal relationship between young people's own development and broader socioeconomic development.

Haraway's (1991) theorization of the cyborg evokes "transgressed boundaries, potent fusions, and dangerous possibilities" (p. 154) that blur distinctions between humans and non-humans, materiality and sociality. Orlando, a 14-year-old young man from Manhattan, speaks to what he feels is the spatiotemporal progression of such blurring in his environment while also echoing Felicia's previously cited concerns that the internet is 'spilling over':

> So, I just think like as time goes on, I think that the internet is going to become -- like -- everything. Everything we've done on the internet now, it's like 'oh, you need help? Go to the internet and log on.' Everything is done on the internet now, nothing is done in person, like most people don't even shop anymore, they just shop online. So, it's like -- I think it's just going to evolve so much that like everything is going to be done on there, even school. People won't even have to go to school anymore, they'll just sit at home and the internet will bring us school.

Understanding how boundaries, fusions, and possibilities relate to modes of becoming and knowing in the situated experiences of growing cyborgs, such as Orlando, helps expose the potentially transgressive, potent, and dangerous aspects of informationalism for those marginalized in the network society.

The young people I interviewed, as well as the members of the YDRC I later worked with, were all engaged in what Erikson (1982) defines as the adolescent stage of development when identity formation begins to "emerge as an evolving configuration" (p. 74). Erikson is eager to note, and I to emphasize, that identity is not *configured* during this stage of the life course, rather it is a *configuration* that evolves throughout life. While the configuration of one's identity begins well before adolescence, it is during this stage when one begins to configure their identity beyond the family and in relation to broader societal norms and expectations. Although Erikson (1982) describes this configuration as a series of "psychosocial crises," I wish to dissociate this from the more common 'youth in crisis' framing that stereotypes young people as helpless victims of cyberbullying, online predators, and even their own sext-ual desires, and/or as hopeless criminals engaged in stealing, hacking, pornography, and bullying. Though any one of them could be, young people are in no more danger or crisis than society at large. Rather, they are engaged in important and complex negotiations regarding their psychosocial identity. As such, the psychosocial crises of adolescents entail as much opportunity as danger.

Adolescence is a formative stage in identity development when young people begin to learn and play out social practices in line with what Erkison (1982) calls "the ethos of production" (p. 75). In 16-year-old Melanie's experience searching for and listening to music through YouTube, we see how social production, evolving identity configurations, and proprietary media intertwine in practice:

> [YouTube] helps you see things that are going around, or music that like people are playing, clicking a lot. Or, music that is kind of like popular, everybody is singing it. So it makes so interesting to -- if it's a nice music and it's like really cool, everybody is clicking it. It kind of like makes you go 'oh, this is so nice, everybody know this music.' So they may kind of like that you're saying it's like cool -- So you know, you kind of like

> listen a lot and you know the lyrics and you might sing it, sing at some places -- you might go to your friend ‘oh, do you know this music? Everybody listen to it.’

Melanie goes on to explain that often she first hears music on TV but then does research using Google, to ultimately find the song or artist on YouTube:

> In T.V., I have this channel MTV, or Trace Music if you have DISH Network. It has like this -- it shows you those kind of new music that comes up, or the old music, and all that. So you know these people that you're going to search for. And, you search them. Sometimes you don't get their name, so you put the one sentence of the -- like this music that would say ‘you're cooler than me,’ right? -- So you put ‘you're cooler than me,’ and then they'll show you the name of the song -- and, you know, you click. It just, you know, tells you. And that's how I find music [on YouTube] that I don't -- didn't know the name but I know the music.

How Melanie comes to know and like music situates how corporate platforms like Google, YouTube’s parent company, facilitate familiar forms of identity configuration in relation to social norms with a proprietary twist. What content Google allows on their servers as well as what forms of research and participation they afford through their interface is oriented by Google’s interest in generating profit. What ‘everybody is clicking’ on YouTube and what Melanie sings the lyrics to when out with her friends is shaped as much by her peers as Google, MTV, and Trace Music -- if you have DISH Network. For growing cyborgs, both people and media function as peers in shaping their tastes and thus identity development.

Melanie helps situate how everyday human-environment interactions generate exchange value for Google and foster particular practices that sustain broader informational development. This bolsters Erikson’s (1982) association of adolescent development with an ethos of production while also suggesting our ‘canaries’ are particularly sensitive to, and early indicators of, evolving work roles:

> A certain hierarchy of *work roles* has already entered the playing and learning child's imagination by way of ideal examples, real or mythical, that now present themselves in the persons of instructing adults, and in the heroes of legend, history, and fiction (p. 75).[9]

What it means to be a Gossip Girl, hacker, pirate, student, gamer, daughter, bully, social media sensation, or Silicon Valley mogul enters the informational imagination of growing cyborgs, and influences the identities they affiliate with or repudiate. Likewise, the repudiations and affiliations of youth in turn shape what modes of development are materially and socially sustained in everyday environments.

Wilson (2009) offers a rereading of the cyborg metaphor's operation in the field of geography to draw attention to the ways it has been taken up to describe an "ontological hybridity" that is "about contingent beings and about forms of becoming that challenge dualist narratives, like human/machine, nature/society and the virtual/real" (p. 499). Along with this ontological hybridity, Wilson calls for more attention to the epistemology of cyborg geographies by researching both "boundaries and boundary-makings" (p. 500), and thus both ways of becoming and knowing in hybrid configurations of people, place, and media. It is precisely these boundary-makings that the analytical pairing of development and development helps bring into focus (cf. Katz 2004); yet boundaries and boundary-makings are also what become so difficult to ascertain in opaque and seemingly amorphous proprietary ecologies. If, as Erikson (1982) argues, negotiating the boundaries between an "inner space" and a "social space" is central to configuring one's identity, then demystifying the boundaries and boundary-makings in and around these spaces is central to understanding the development of adolescents--whether we consider them growing cyborgs or not--in relation to informational development.

---

[9] Emphasis on *work roles* is made by Erikson (1982).

Lewin (1997) argues that people must be understood as operating within a "life space" defined by the sum of all psychological factors experienced at a given time; most notably factors such as "needs, motivation, mood, goals, anxiety, and ideals" (p. 210). Lewin discusses the life space as relationally defined through an evolving "boundary zone" that mediates a person's interactions with a "multitude of processes in the physical and social world" (p. 210). Thus, the scope of a person's situated experience at a given time -- what people, places, and things they do and don't interact with at some level -- shapes the boundaries of their life space and thus the form of their becoming. This boundary-making, as Wilson (2009) reminds us, is an epistemological act in cyborg geographies and, as Erikson (1982) reminds us, a psychosocial act of identity configuration. Thus, I argue these boundary-makings are acts of both knowledge production and identity configuration, which evolve around matters of privacy, property, and security within the life space of young people coming of age. In the lifeworlds of these young people as 'growing cyborgs,' these material social practices develop in relation to the privatized ontology and epistemology of proprietary ecologies.[10]

Engaging Information

As of December 2012, the five most popular websites in the US were Google, Facebook, YouTube, Yahoo! and Amazon.com.[11] Each of these sites represent a proprietary medium that engages millions of people, young and not, with interfaces that allow them to intuitively and

---

[10] See Chapter 2 for a more thorough discussion of how proprietary ecologies operate to aggregate, rationalize, and objectify everyday data.

[11] Alexa Internet is a provider of web traffic statistics. The data presented here was retrieved on 03 December 2012 from http://www.alexa.com/topsites/countries/US.

simultaneously produce, consume, organize, and circulate various kinds of data. Ron, 17, articulates the affective pull of Gmail's interface compared to Yahoo!'s:

> Yahoo is kind of messy, they're putting too much in the web site, like all this and that. And when you go to Google, all it is mail, Gmail, I feel like it's clean and I feel just looking at Google, I go like 'aaaah.'

Although none of the young people I spoke with rhapsodized about Facebook's interface design, it nonetheless has the most youthful data mine of the top five. Pew Internet & American Life Project indicates 93% of social media users ages 12 to 17 have an account with the social network company (Lenhart et al., 2011). Facebook encourages young people to develop presentations of themselves as a social profile. Visualized through a taxonomic survey-like process, social profiles encourage individuals to code themselves with rationalized categories offered by the medium's interface. Age, gender, level of education, sexuality, location, religious affiliation, and political views are all common categories that young people are asked to fill in. These are also categories they observe others fill in.

The affective pull of Facebook's interface, and its associated psychosocial practices, led many interviewees to frame their participation as less voluntary and more of an addiction; something they were, or could become, too dependent upon. Megan, a 15 year old from Brooklyn, described having to negotiate a perceived addiction to computer games:

> I used to be very big on computer games until I realized I was possibly addicted to them. Like the download, the free downloads, so after that, I kind of stopped with the computer games. Same thing with Facebook games, like I used to be the Greatest DJ like my parties would be the best, but I was addicted to the game.

19-year-old Tim, from Brooklyn, discussed his attempts to avoid ever becoming addicted to computer games by keeping his gaming from becoming an "everyday" practice:

> When I'm on Facebook, I check things that my friends updated and stuff, and I play the games of course. I have like 5 or 6 different games I play on there, but I don't do it everyday because you can get addicted to those games for real.

Whitney did not see her relationship with media as an addiction, yet she felt pressure from her mother to 'prove' she wasn't addicted:

> She'll let me be on the computer really for the whole day, but then the next day, I'll go to get on the computer and she'd be like 'using the computer all day yesterday?' And she don't even have to say 'don't get on', she'll just make me feel so bad that I don't even want to get on the computer anymore. Now, I don't want to get on the computer for three days, so I'm not going to do it. ... Because she used to really say 'you're addicted, you're addicted, you're addicted.' So now I have to -- I feel like I have to prove to my mom I'm not addicted. I could go from Saturday until now and not go on the computer.

Orlando explicitly discussed the common perception of Facebook as a drug among his peers, and how he negotiates his own 'addiction' to this drug while noting how this dependence is 'smart' business for Facebook:

> Well, I feel like [Facebook's] like a drug. Like I know people have made that joke — like there's some way to make a syringe through letters and they make a syringe and then in the middle they write like Facebook, and it's like 'Facebook the drug,' and then put it as their status. And it's like true. I mean, obviously it's not a physical drug, I've gone off of Facebook, but it's hard because you want to know who posted on your wall or what notifications you got, so it's like—like they're smart. They know what to do.

Orlando, like others who had "gone off of Facebook" by deactivating their account, learned that deactivating was not the same as deleting. Facebook would continue to periodically update them on their friends' activities as well as personal messages received -- both of which required reactivating the account to view. That this is good business for Facebook highlights how accumulation by dispossession operates in proprietary ecologies by enclosing one's social network and regulating access to it.

Andrejevic (2005) poses that the "participatory injunction of the interactive revolution" (p. 494) has led to a proliferation of peer-to-peer monitoring tools. He theorizes this process as "lateral surveillance" through which everyday people can increasingly spy on each other. In his theorization, hierarchical power structures are ironically reproduced and sustained through covert horizontal surveillance practices such as running online background checks on a peer. These background checks can entail the ways a college or employer might 'google' a potential student or employee to gain more personal information than was volunteered in an application, or how an individual might use an for-pay service like PeopleSmart.com to see if a babysitter or love interest has a criminal record. In the sense that Facebook generates semipublic records on its users through the form of social profiles and personal timelines, Lateral surveillance helps us consider how young people interact with hierarchical power structures through their *use* of such proprietary media. Young people like Megan, Tim, Whitney, and Orlando are engaged in lateral surveillance while observing peers and peer interactions through the *use* of Facebook. An emphasis on *use* is necessary to distinguish such practices from the various forms of participation that may also be possible with and within Facebook. Whatever one might do or achieve through their participation in Facebook, happens alongside their use of a product that is intentionally designed by a corporation for surveillance.

What peer monitoring is possible through Facebook largely depends on the design and governance of its interface. While users of Facebook can negotiate what personal information they choose to share with other users, many of the young people I interviewed didn't feel like they could negotiate their relationship with Facebook so easily. As Anne, 18, explained when I asked her who she felt her Facebook profile belonged to:

> I would like to think it belongs to me, but in a way it doesn't. As soon as I make that profile and submit it, it doesn't belong to me.

Anne went on to connect this directly with an earlier discussion of how people browse each other's photos on Facebook and block certain photos so parents and teachers can't see them:

> You know something like Facebook will tell you how you can choose who will look at your pictures or not, and blah, blah? But that's only like for the older people that use the Facebook.

When Anne says "only like for the older people" she means configuring her privacy settings so that only her 'older friends' -- such as a parent, teacher, or family friend -- cannot see them.

> But who the profile belongs to? To the system. It doesn't really belong to you, it belongs to somebody that pay for it now, so in a way it belongs to you, but when you think about it very deep, it doesn't belong to you.

Anne begins to link privacy with property and implies that because her profile doesn't belong to her, but to "the system," then there's nothing that could be kept private from the system once it's been 'submitted.' Facebook informs its users about some of what they and their peers are doing or have done within the medium. Facebook also consults with its users by continuously monitoring their every interaction with and within the medium to design a 'user experience' or 'UX' that encourages more sharing of personal information. UX can be understood as the way an interface is designed to encourage a particular experience or range of experiences for a user or group of users. Matters of human-computer interaction, information architecture, marketing, and strategic communications are typically considered to inform UX design. What distinguishes UX from participatory design (PD), is the epistemological stance of each process. For UX, it is a focus on understanding user experience to achieve a producer's aims through an informed design

process. For PD, it is a focus on understanding user experience to achieve a user's aims through a collaborative design process. In the former a user is a considered consumer of the interface. In the latter, a user is a participant in the interface's production and purpose.

Using Facebook can be understood as what Arnstein (1969) discusses as "token participation" in that users can only "hear and be heard" without the "power to insure that their views will be heeded by the powerful." Lateral surveillance in Facebook is token participation in the reproduction and reinforcing of hierarchical power structures. This does not mean Facebook users are dupes of its design. It means that whatever ends a user may or may not achieve with and within Facebook, their ability to participate in the design and governance of the space facilitating those ends is hierarchically constrained and policed. As Occupy Wall Street has shown through their occupation of Zuccotti Park during the fall of 2011, attempts to participate in the design and governance of a privatized space is seen by corporations and governments as a violation of its 'terms of use' and grounds for eviction.[12]

Albrechslundt (2008) notes that focusing on lateral surveillance can obscure the truly participatory and potentially empowering aspects of peer monitoring in social network sites. Although *using* a proprietary medium is token and characterized by lateral surveillance, there are other participatory possibilities with particular media; proprietary or otherwise. Albrechslundt (2008) theorizes "participatory surveillance" to account for the ways people draw on social network sites to facilitate individual and collective empowerment through the development of

---

[12] Zuccotti Park in Lower Manhattan is a privately owned public space managed by Brookfield Properties. While Zuccotti is owned by Brookfield Properties, in exchange for tax breaks, it must be kept open to the public 24 hours a day. Yet, Brookfield Properties are allowed to establish a terms of use for the space that is enforced by the New York City Police Department.

mutual subjectivities. From this perspective, despite or in defiance of what little power a person may be afforded in the design and governance of a particular medium or space, participation towards certain ends can afford empowering or simply unpredictable outcomes. Such experiences are exemplified by the Arab Spring, a translocal social movement that has drawn heavily on proprietary media such as Facebook and Twitter to occupy certain historical geographies and reach others who share their interests and concerns.

Taking the tagging of people's faces in photos on Facebook as an example, we can see how a common human-environment interaction in proprietary ecologies simultaneously affords both dominating and empowering outcomes in everyday life depending on its participatory orientation. Tagging encourages elementary participation in a structured and playful mode of biometrics, which eases the social adoption of controversial security technologies such as automated face recognition (Ellerbrok, 2011). At the same time, tagging produces a folksonomic, creative, and potentially empowering organization of visual identities.[13] My project maintains this distinction between lateral surveillance as *use* of a particular social medium and participatory surveillance as potentially empowering practices with social media, while also accounting for their simultaneity in propriety ecologies. Chapter 3 explains how my collaborative research and design with members of the YDRC worked to involve them in the production of a particular medium to juxtapose and investigate these two modes of participation in our environments, the results of which are discussed in Chapter 4.

[13] Folksonomic refers to the collaborative development of categories for organizing content, and stands in contrast to more common topdown taxonomic categorizations.

Peer monitoring was positively discussed by many interviewees as a common and enjoyable practice of "stalking," but also a practice that can foster stress and disorientation when operating at a token level in a proprietary surveillance medium. Elena, a 19-year-old woman from Queens, articulates this disorientation:

> And [Facebook] also makes—you know, you start stalking people, I'm not even going to lie. And it just gives you complete access to what they're doing at like nearly all points in time.

She describes how frequent participation in Facebook led to an inaccurate perception of a relationship with a guy she was dating:

> And what's crazy is, I was dating this guy and he has a Facebook page, but he doesn't really use it. And then, because I use it so much, relating to somebody who doesn't gets you a little paranoid.

Elena describes a complex boundary-making by negotiating her desire to 'compulsively click' and 'stalk' a peer in relation to perceived social norms. All of which takes place in a life space infused with proprietary ecologies that are designed to foster such compulsive clicking and stalking. In this context Elena questions her social perception:

> Because you're like wait, they didn't accept my friend request in two weeks and then it's just like 'oh, they must not like me.' And then, it's like 'wait, they probably did not go on the internet for two weeks.' And it's as simple as that. And then, it's just like compulsive clicking on their name, seeing their friend count changes, I'm so—like I can't believe I'm admitting this.

While in one sense, Elena's participation could be considered all embracing as she can 'stalk' her friend constantly and even compulsively, yet it is also token in that she's left to guess just how much a peer is participating in the same medium; her vision in this environment is restricted. This isn't to suggest that Elena should be able to see everything that Facebook sees, but to show

that Facebook sees and knows more than Elena and thus designs a hierarchical structure of who can see what within the medium. That Elena's position in this hierarchy makes her question her social perception suggests she does not see her own use of Facebook as all embracing participation.

The information architecture of a medium such as Facebook, is designed to encourage a UX of personal sharing and social stalking; both producing exchange value for Facebook by exclusively monitoring and mining this 'shared' data as well as allowing users token participation in certain modes of this monitoring to foster greater use value. In this way, Facebook functions as a social vending machine allowing its owners to organize and display certain data-commodities with different values. This practice is not limited to Facebook or even just social network sites, but applies broadly to all information businesses. One example of this can be found in the 2009 publication of 'price lists' created by corporations such as Yahoo!, Cox Communications, Cingular (now AT&T), and Nextel. These 'lists,' published by Cryptome.com, were created for the US Government to outline the various data and surveillance services that could be made available to law enforcement agencies for a specified price.

This vending is not only oriented towards governments, but also other corporations and consumers alike. Facebook encourages users to easily browse and evaluate some of these data-commodities by allowing to them to navigate their social networks via location, group affiliations, likes and dislikes, music and movie interests, and profile pictures. As Rebecca, 15, explains:

> Facebook is easy to surf, you know. You don't need to have anything in mind when you're surfing. 'Oh, there's an attractive guy. Let me go see who he is' -- you know? You can just do that. Or, 'oh, she's pretty, let me go see who he/she is even though she's a

> friend, of a friend, of a friend.' And that's easy to do even though you might not have it in mind -- 'I'm going to stalk this person right now.' It just happens.

While the fact that Rebecca still considers this practice 'stalking' suggests she also finds it problematic at some level as well, stalking remains something normal that 'just happens.' In contrast Elena expresses a sense of guilt for performing such surveillance practices by notably 'not lying' and 'admitting' that she stalks. Yet both, like other interviewees, discussed their surveillance practices with a sense of joy and satisfaction even if some expressed guilt about it. Shoppers on Amazon and 'stalkers' on Facebook now locate and select books and humans in remarkably similar ways, both depend on a navigational taxonomy configured for purposes of commodification and control. This object-oriented organization of proprietary ecologies helps fulfill many needs, desires, ideals, and anxieties emphasizing the empowering potential of connectivity. Yet when submitting to the Terms of Service of a particular proprietary medium, our growing cyborgs begin to rent access to part of themselves -- their everyday data -- from a medium's proprietor(s). Using a proprietary medium such as Facebook entails placing aspects of oneself within the vending machine.

This process enables Facebook to profit from their users' online reputations as well as to build lucrative databases which link up the consumption behaviors of a particular user with detailed taxonomic information from their profile. Such databases help structure the flow of capital within proprietary ecologies by simultaneously creating refined target markets within a youth demographic as well as the means for directly targeting these markets. Increased categorization and codification is thus promoted by medium owners for the sake of efficiency and flow, and thus, profit and control. Facebook argues that their users 'own their own content,'

but what data -- or replications of that data -- is left on their servers *is* their business. Ownership of a medium means you don't necessarily have to own the content within it since you own both the access to it as well as the consuming of it regardless. It is in this way that proprietary ecologies emerge as practices of ownership that enclose everyday data rather than own it outright. Access to such data also often becomes government business as well as the business of joint ventures with other corporations. Further, what limited ability a proprietary medium allows for exporting one's data typically removes its most meaningful and empowering qualities: its circulation and visualization. Seemingly without irony, Google has assembled its own "Data Liberation Front" (DLF) that implicitly admits a user's data is anything but liberated under normal circumstances at Google. While the "liberation front" in the name implies a political organization of some kind, such as the Palestinian Liberation Front, the DLF is more a working group of Google employees whose mission statement reads "Users should be able to control the data they store in any of Google's products. Our team's goal is to make it easier to move data in and out."[14] DLF is potentially liberating in that they've developed programs that allow users to export their content from a few Google services in a format other programs can read. However, the seven services the DLF currently supports and the limited kind of data one can export from them barely scratches the surface of the everyday data Google aggregates on its users.

For the young people I interviewed, the construction of personas through taxonomic categories encouraged the use of stereotypes both for self-expression and for locating and communicating with others; something many of them wrestled with. Lippmann (1922) connects the use of stereotypes in communication to the roots of mass media, as psychosocial

[14] The mission statement was taken from the official website of Google's Data Liberation Front on 15 January 2013 and can be found at http://www.dataliberation.org

constructions for conveying complex matters. In a similar way, proprietary ecologies encourage stereotypes through semantic codification for purposes of commodification. Such structures, as Elena helps articulate, do not always work out so well when engaged in an evolving configuration of your identity and boundary-making in your life space. OK Cupid is a popular dating site that epitomizes this structure by asking its participants to fill out a social profile, demographic information, and behavioral as well as opinion-focused surveys to quantify and visualize how much of a "Match," "Friend," or "Enemy" two people are likely to be. Although participating in this particular medium, Elena felt it created a static identity that couldn't accommodate her evolving behaviors and opinions, and found OK Cupid's "percentages" and "logistics" to be inaccurate.

Elena more positively discussed her interactions with Craigslist, a proprietary medium offering classified advertisements. Elena describes having used Craigslist to find jobs, do research, or buy things before she "found" their personals section; what she called the "fun stuff section":

> And then, I clicked on the personals and it was just like all these people, and they're so anonymous, and they can say absolutely anything they want. And I totally got dragged in it. [...] So, I just posted an ad, and I was like oh, I'm not going to tell anybody. I'm not going to tell anybody because this makes me look bad. Because people do have the connotation that it's pejorative, like, whatever.

It is notable that Elena feels society judges her anonymous participation in a medium such as Craigslist but does not judge her heavily 'identified' participation in media such as OKCupid or Facebook. The former is a frequent subject of media scrutiny for the anonymity it affords, tacitly implying that more identification in a medium entails more safety. Yet, for Elena, this anonymity and absence of taxonomic navigation afforded a more fulfilling and empowering experience:

> So, posted an ad, got some responses, they were really interesting because I love talking to people. And initially, when people respond to you, they don't know who you are, so they're responding to whatever you wrote. And sometimes you write something and you don't—you have an idea of what you think you're writing, but when somebody else reads it, that's not what they're reading.

Anonymity helps Elena break out of stereotyping herself and others, offering a departure from routine peer monitoring. The unpredictable social interactions this anonymous monitoring affords is precisely what Elena enjoys so much about Craigslist:

> So, it's like communication over the internet is harder than communication over phone or face-to-face. So, it's really interesting, a lot of varied responses from varied people, and you end up talking to like 40-year- old men from New Jersey whose like—this is a true story—whose like daughters are like my age, right? And I'm just talking to him about like life and I've done drugs in the past, whatever. And it's interesting because he's like oh, I want to try LSD. And it's just like, wait, this is like my father I'm talking to. And it just breaks you into this world of wow, everybody is simply a human being, like that's actually when it really hit me. And I started like really loving Craigslist, but there's just a tension, that this is what I realized that OkCupid, Facebook, Craigslist, everything, like all those websites where you get to share, you—well, I rather, really started noticing that I fiend for attention. And so do other people. And you can't assume that that's their means of posting whatever they're posting, but like there really is this underlying basis—underlying basis of wanting attention. And when it comes to something like Craigslist and OkCupid, being female gets you that attention.

Craigslist helps reframe the familiar as strange for Elena, reconfiguring social roles, and leading to new understandings of oneself and society. Although very different from her interactions with and within Facebook and OKCupid, Elena sees an "underlying basis" of "attention-wanting" to such media that produces a "tension." This attention-wanting may be gendered, as Elena suggests, yet it was commonly expressed by both the young men and women I interviewed, and brings us full circle back to Felicia's evocation of *Gossip Girl*. That this attention-wanting is both an integral part of adolescent development as well as a fostered UX for proprietary ecologies

also brings us back to the ways such ecologies can afford both lateral and participatory practices of peer monitoring.

Conclusion

Data flows in the everyday environments of youth. How these flows are organized to constitute various information systems for subsequent knowledge production is integral to understanding how young people negotiate matters of privacy, property, and security. Despite recent labor statistics showing the number of employed US youth ages 16-24 at an all time low of 50.2% (Bureau of Labor Statistics, 2012), youth labor remains a significant element of the informational workforce. While forms of paid piece work or 'microwork' have cropped up, such as Samasource and Amazon.com's Mechanical Turk, the bulk of young people's digital labor in the US remains unpaid.[15] These include the more direct forms of unpaid labor that produce data for commodification during routine engagements with and within proprietary media. They also include more overt forms of unpaid work that increase the productive value of proprietary media through BETA testing software, reporting errors when a software program crashes, indexing and ranking websites for search engines, and a plethora of other strategies often labeled 'crowdsourcing.' That this labor is unpaid makes it no less productive.

Whether this labor is a form of exploitation, some form of equitable and potentially empowering tradeoff, or just a pleasurable engagement with particular media, it is essential to the

---

[15] Samasource (http://samasource.org) describes itself as a "nonprofit social business" that offers "dignified digital work for women, youth, and refugees living in poverty" while Amazon's Mechanical Turk (http://mturk.com) describes itself as offering "businesses and developers access to an on-demand, scalable workforce."

means of production that sustain information corporations from Google and Facebook to News Corp and AT&T. Of course, just as informational capitalism is predicated on the production and reproduction of an information economy in concert with an information society, the significance of youth in this process extends as much to their play as it does their work. Indeed, scholars such as Kücklich (2005) have argued that play can function as a form of unpaid content production, or "playbour," while others have shown how certain forms of play in technological environments are being restructured as vocational practices with the aim of training youth for future informational work (cf. Sandvig, 2006; Donovan & Katz, 2009). In both cases, government and corporate interests in control and profit infuse young people's identity configuration by influencing their daily negotiations of what does and does not constitute a matter of personal privacy, property, and security.

The distinction between paid and unpaid labor, or 'playbour' as it may be, is largely an economic one. Yet, as Dewey (1916) argued during industrial restructuring "it is important not to confuse the psychological distinction between play and work with the economic distinction" (p. 205). While the economic distinction frames play as aimless amusement and work as constrained labor, work and play in a psychosocial context are both intrinsically and extrinsically motivated activities that shape and are shaped by economic conditions. Psychologists such as Vygotsky (1978, p.102), Piaget (1951, p. 147), and Lewin (1935, p. 105) -- despite notable differences -- all discuss play as a practice that breaches the boundary between imagination and reality, and affords an empowering assimilation between the two. In considering the ways young people, as canaries in our contemporary data mine, work and play in proprietary ecologies we consider the ways in which society at large will soon be working and playing. From an economic perspective,

one might consider young people's playful activities in social networks to be unproductive yet this obscures both the economic value these practices produce for corporations as well as the social value these practices provide through their imagining of new realities.

As the material and social are interdependent, changes in one provoke a corresponding change in the other. If technological paradigms such as informationalism provoke a cultural adjustment of beliefs, customs, philosophies, and laws regarding matters of privacy, property and security, then such adjustments also expose, articulate, and call for material social adjustments. Such change must not be monologically accepted, but consciously participated in to realize empowerment. While influenced constantly by a social history of cultural norms and conceptions, young people themselves have no embodied experiences of privacy, property, security, or even identity that does not entail the internet. Individual and collective understandings of such matters are negotiated among youth in real time within proprietary ecologies in relation to informational development.

Young people are thus part and parcel of an environment transiting from industrial to informational, yet they bear no personal history of industrialism with which to wrestle. Often, this makes the more critical perspectives that come with age and accumulated experience something that must be deliberately fostered. For example, having a sense of what privacy was like before ICTs reached their present ubiquitous state, allows today's adult to draw critical comparisons between the way things are in their environment to the way they used to be.

As proprietary media proliferate within young people's environments, so too does an informational mode of development. This spatialized and embodied privatized mediation

warrants a critical and ecological consideration to understand young people's development in relation to current modes of socioeconomic development. Dewey (1916) states:

> Since the young at a given time will at some later date compose the society of that period, the latter's nature will largely turn upon the direction children's activities were given at an earlier period. This cumulative movement of acton toward the later result is what is meant by growth (p. 41).

In short, the future is being built in the life spaces of our growing cyborgs. In facilitating the MyDigitalFootprint.ORG Project, I involved young people in collaborative research and design to understand and engage their growth in proprietary ecologies and thus foster a more critical consideration of their psychosocial development within broader socioeconomic development. Such understandings of, and engagements in, the mutual shaping of people, place and media are necessary to reorient the means of production towards young people's situated interests and concerns, and thus realize a more just society.

Chapter Two
Proprietary Ecologies

When interviewing 15-year-old Megan, I asked her if she thought the internet belonged to anyone.[16] Megan's response is reflective of those given by other interviewees and raises questions of ownership, access, and power in proprietary ecologies:

> I will say the people, but I think by now it's no longer -- the internet owns the people because like there's a lot of people they just don't, they can't, go one day without the internet. It's something--that eventually they'll end up having to use the internet, maybe not because they wanted to, but because something involved, like directions, where they needed to go on the internet. They couldn't find the old-fashioned map, so they had to go on the internet.

Megan draws first from an ideal, "I will say the people," and then from her lived experience when concluding "the internet owns the people." Megan's insight that we may be owned by the internet because of the useful and convenient things it lets us do brings attention to the often mundane ways transnational regimes of informational domination operate in the everyday (cf. Jessop, 2004; Fuchs, 2009). Yet her ideal touches on the more empowering aspects of society's dialectical relationship with media where everyday people own the internet. Castells (1989, 2001) argues that capitalism is being globally restructured according to an information-based mode of development that values the accumulation of knowledge as a dominant source of power. This can be seen most overtly in the use of proprietary trading algorithms to dominate transnational financial markets and the global security practices employed by governments to

[16] As discussed in Chapter 1, the names of interviewees have been changed to protect their privacy.

ensure this distribution of power.[17] This restructuring can also be seen in the intimacy, sociality, and materiality of everyday life. As people move through life drawing on a proprietary map for directions, for instance, their trajectories can be surveilled, rationalized, objectified, and ultimately oriented by the map's proprietors. This possibility calls for critical engagement to understand how human-environment interactions in proprietary ecologies link up with broader modes of development in advanced capitalist societies.

Born one year before the launch of MapQuest, Megan and other young people around her age have long negotiated the boundaries of their life space and the configuration of their identity in relation to proprietary maps.[18] This does not render them passive subjects to proprietary interests. Rather, it entails constant and often commonplace negotiations between acceptance, resistance, and reworking. As Ron, 17, explained when I asked who he thought owned Facebook:

> So it's like in Facebook and stuff like that, we're the ones who's owning the Facebook because we're the ones that are keeping up with the new stuff. We give and put in new ideas, we're the ones who's saying something funny in order to make somebody laugh. Or we're the ones who's inviting other people to come. It's like advertising in TV, let's come use Facebook because Facebook is the best, so we're the ones who's saying it. I feel like it's us, we own it.

---

[17] An illustrative example can be found in the FBI's 2009 involvement in detaining Sergey Aleynikov, an ex-Goldman Sachs programmer. Aleynikov was charged with uploading the proprietary code Goldman uses to facilitate automated stocks and commodities trading to a server based in Germany. The concern around this alleged theft was not that this 'loose' code could be used to manipulate the markets -- as that's precisely what it was designed to do -- but that Goldman might lose their dominance in manipulating financial markets to a competing and potentially foreign entity. Here we see state intervention, through a public security apparatus, to police and protect privately owned intellectual property that ensures national dominance in the global financial markets. The charges brought against Aleynikov can be found at: http://static.reuters.com/resources/media/editorial/20090706/Complaint%20--%20Aleynikov.pdf

[18] MapQuest launched in 1996 as one of the first major online mapping services.

Ron feels ‘we own facebook’ and recognizes Facebook’s dependence on an engaged audience to maintain its existence. Yet, Ron also negotiates the influence Facebook has over his daily routines and discusses how he deactivates and reactivates his Facebook account at times:

> When I started working, and I barely had time to go online, that's when I just deactivated it. But sometimes I feel bad because everybody talk about Facebook, like ‘oh my God, tonight in Facebook I'll be posting this video, you better watch it.’ And then I'll go ‘I wish I had the Facebook on.’ And I feel lazy to go back and activate the Facebook.

He then goes on to explain how he’d prefer his relationship with Facebook to work:

> Say like whenever you feel like you should be on you can just activate it, and deactivate it whenever you feel like you don't need to be on that web site. Or you don't want a web site where you can’t stop whenever, but you don't want to be on a web site where you're going to be vanished forever.

Ron accepts the connectivity and socialization Facebook affords, he resists letting his relationship with Facebook occupy too much of his time, and he’s at least considered how this relationship could be reworked. Such embodied experiences of negotiating proprietary ecologies are part and parcel of Ron and Megan’s situated knowledge and provide an under explored perspective of how informationalism plays out at an intimate scale. Haraway (1991, 2000) theorizes “situated knowledges” as a means of getting beyond a binary epistemology that considers knowledge to be either objectively or subjectively produced. Situated knowledges represent a dialectic of impartiality and partiality where all knowledge is embodied, local, and limited. This means that knowledge becomes objective through its resonance across subjective locations. What situated knowledges young people like Megan and Ron have regarding informationalism, comes from the common ways this socioeconomic paradigm plays out and finds meaning in their respective embodied experiences.

Through a critical understanding of the situated knowledges of youth, as well as their dialectical production and reproduction, more open ecologies oriented toward the situated interests and concerns of young people like Megan and Ron become possible. Since informationalism and its associated proprietary ecologies are not objective *or* subjective phenomena but *both*, the only meaningful way to understand and engage them is through the situations where they are given meaning. It is with this in mind that I interviewed and then conducted participatory research and design with young people to critically consider proprietary ecologies within the situations of their everyday lives and to encourage more diverse and empowering trajectories throughout the life course.

In this chapter, I outline a critical ecological framework for understanding how informationalism is socially reproduced in everyday environments. Latour (1998) argues that to "ecologize" a question, object, and/or datum "means creating the procedures that make it possible to follow a network of quasi-objects whose relations of subordination remain uncertain and which thus require a new form of political activity adapted to following them" (p. 240). I theorize a 'proprietary ecology' to bring into focus the privatized relations of production and reproduction in interactions between people, place, and media, and to reveal participatory and potentially empowering alternatives. Proprietary ecologies are not distinct from the human environment, but a result of procedures designed by governments and corporations to structure the flows of data and capital within everyday environments. In particular, these ecologies work to insert a proprietary interface between people, place, and media so as to privatize not only interactions, but also the various forms of data and information produced from these interactions. When I speak of 'information ecologies' it is to refer to the circulation of data in information

systems within the broader material social environment. Thus, when I speak of 'proprietary ecologies' it is a consideration of property relationships operating within information ecologies.

If accumulation by dispossession operates through regimes of private ownership to enclose and regulate access to public resources, then what form of empowerment might be achieved through participatory ownership? How might this sort of access to the means of production shape public debates around matters of privacy, property, and security that have until now focused almost exclusively on protecting the interests of government and corporate proprietors? This imbalance can be found in legislation such as the 1998 Digital Millennium Copyright Act that protects the intellectual property of corporations, or the 2001 Patriot Act that gives the US government the authority to surveil the digital communications of its citizens for national security purposes. Both acts have been extended since passage and stand in stark contrast to how existing legislation concerned with the personal privacy, security, or property of citizens, such as the 1986 Electronic Communications Privacy Act, that has not been updated to address contemporary forms of communication and information sharing. One might consider the 1998 Children's Online Privacy Protection Act the lone exception, yet its requirement that corporations obtain parental consent if they aggregate data on people under the age of 14 has been shown to be easily circumvented and with little to no penalty (Cai et al., 2003). A critical investigation of proprietary ecologies should help articulate and address such questions of ownership, access, and power in mediated human-environment interactions.

Young people are significant actors in the production and reproduction of an informationalism because of the biological generation they embody as well as the broader continuity and discontinuity they represent in terms of social norms, desires, practices, and

ideologies. Katz (2004) has pointed to the situated experiences of youth as significant factors in the reproduction of global industrial capitalism in places as different as rural Sudan and New York City. Ewen (1976) theorized the significance of youth as an "industrial ideal" that provided an idiom for the social norms, desires, practices, and ideologies necessary to reproduce industrial capitalism within the US at the turn of the 20th century. Not only were young bodies necessary to perform the physically taxing labor carried out in early industrial factories, but the image of youth was drawn on in advertising to sell a range of new commodities such as cosmetics. Presupposed by its industrial manifestation, informational capitalism operates in the embodied and situated experiences of young people as well as through disembodied and idealized cultural stereotypes of youth. 'Youth' emerges a cultural ideal in advertisements and legislation as well as parenting and pedagogical practices that encourages a society to give up 'old' notions of privacy, property, and security, and to adopt 'new' notions that facilitate an informational mode of development. Cultural stereotypes of eager young consumers unconcerned about privacy, young prey stalked by cyberbullies and online predators, or young criminals stealing intellectual property help maintain and reproduce certain modes of production and consumption in the life space of youth; not to mention their parents and educators. In the following sections I outline the circuitous surveillance, rationalization, and objectification operating through proprietary ecologies, and provide an example of how the everyday data generated from these processes become commodified. As young people's environments blend with proprietary media, everyday data around their routines is continuously produced, mined, and privatized. The proprietary media that help them keep pace and place in the historical geographies of informationalism also embed them further in systems of dispossession.

People, Place, and the Proprietary Interface

Everyday data is generated and aggregated in and through a privatized interface between people and their environment. As people live their mediated lives this privatized interface generates data on their everyday activities; from grocery shopping with a Bank of America debit card, to texting with an iPhone, to watching movies on Netflix. This everyday data then circulates in a distributed transnational architecture of cable and telecommunication infrastructures (van Schewick, 2012). Much of this information ends up in corporate databases for targeted marketing purposes (Turow, 2006) and/or in government fusion centers where information from public and private databases is merged and mined according to dubious security rationales (Monahan, 2011; Monahan & Palmer, 2009).[19] Throughout this process the give and take data flow is shaped by software code (Lessig, 2006). In the case of routine text, email, chat, voice, and video interactions, Conti (2009) explains how the data from our "communications tell the online companies who we interact with, what we look like, what we sound like, who we are linked to socially and professionally, as well as the actual contents of [our] messages themselves, both mundane and extremely sensitive" (p. 167). I hasten to add that this engagement with the material circuitry of proprietary ecologies is encouraged, challenged, and/or renegotiated at every level with social practices, needs, desires, and experiences.

---

[19] Examples of such dubious rationales can be found in the establishment of a fusion center to monitor protests during the 2004 Republican National Convention in New York City. While the rational provided was to prevent terrorism, Monahan and Palmer (2009) note that no such fusion center was established for the 2004 Democratic National Convention in Boston. Further, Monahan (2011) explains the ways fusion centers rationalize bypassing a "reasonable suspicion" requirement for "collecting" and "maintaining" criminal intelligence by instead searching and accessing information stored elsewhere through networked computing.

According to Katz (2004), social reproduction "encompasses that broad range of practices and social relations that maintain and reproduce particular relations of production along with the material social grounds in which they take place" (p. X). Such an understanding of social reproduction provides a constructive framework for ecologically investigating the structural continuity and discontinuity of transnational informational capitalism by accounting for the reciprocal relationships of production and social reproduction that sustain it. While social reproduction has often been separated from production, as a phenomenon distinct from and secondary to the economic realm and the paid labor it constitutes, such conceptual distinctions obfuscate the productive yet unpaid labor often carried out by women and youth, among other *others* (cf. Mitchell, Marston, & Katz, 2003). While such a clearly defined conceptual distinction was never functional, its dysfunction is emphasized in the context of proprietary ecologies where the continuous circulation of data generated through human-environment interactions is increasingly rationalized, objectified, and commodified. In a context where social networks *are* corporations, and personal information *is* a commodity; production and social reproduction are overtly and dialectically bound.

Dodge and Kitchin (2005) argue that the technicity of software and hardware code shape the production of space through transduction. They define technicity as the “productive power of technology to make things happen” while transduction is defined as the “constant making anew of a domain in reiterative and transformative practices” (p. 162). If human activity creates the needs for certain conceptions of space, as Harvey (1973) argues, then transduction helps explain how such conceptions play out in practice. The technicity of proprietary ecologies for corporations and governments rest in their ability to produce absolute spaces conducive to

control and capital accumulation in an informational context. Further, while the technicity of proprietary media such as Google Maps help people easily and quickly navigate their environment it also involves them in a range of social practices and relations that orient their surroundings according to particular modes of informational development. Through transduction, proprietary ecologies are constantly, relationally, and socially produced by corporations and governments as well as consumers and citizens.

In the context of US youth, the technicity of proprietary ecologies operate in their material social experiences at all scales from the intimate to the translocal long before they enter the workforce as paid labor. The productive and entertaining promises of proprietary education, communication, and play media have led to widespread adoption that ties young people and their environments ever closer to an informational mode of development as they learn, talk with friends, and play, among many other mediated activities. The privatization that permeates this mediated transduction is presupposed by and intertwined with privatization happening elsewhere in our environment; from the enclosure and gentrification of our urban spaces (Low, 2006; Katz, 2006, 1998; Smith, 1996; Harvey, 2005), to the neoliberalization of our education systems (Fine & Ruglis, 2009; Monahan, 2006; Hursh, 2007), to the governance and financialization of our homes (Saegert, Fields & Libman, 2009; Low, Donovan & Gieseking, 2012), and the commodification of our biology (Parry & Gere, 2006; Calvert, 2008). While a number of scholars have theorized an ecological approach to the study of media (cf. Meyrowitz, 1994; Postman, 2000; Capurro 1990; Klaebe, Adkins, Foth & Hearn, 2009), I specifically theorize proprietary ecologies as a way of focusing this approach on the myriad and historical ways privatization plays out in the situated interactions of people, places, and media.

Mediation and privatization intertwine in the intimate texts, social software, fiber optics materials, and translocal communication architectures of our environment. The privatization of our cities, education, homes, bodies, and communication calls for a critical and integrated ecological understanding of the proprietary interface between people, place, and media. Through the study of propriety ecologies I thus consider the mutual shaping of informational development and young people's development within an environment of circuitous surveillance, rationalization, and objectification.

Circuitous Surveillance

Fine and Ruglis (2009) develop a critical inquiry into the systematic miseducation and diploma denial among Black, Latino, immigrant, and/or poor students in the US by focusing on "circuits of dispossession" in order to "queer the question of intent and turn instead to racialized consequences of state policy" (p. 20). This queer yet pragmatic focus on circuitry is important in understanding the consequences of proprietary ecologies because of the material social circuits necessary for informational dispossession, as well as the circuitous presence of surveillance these ecologies produce through transduction. This presence extends to the neoliberal school system itself, where the passage of No Child Left Behind (NCLB) requires schools receiving federal funds to turn over personal data on their students to the Department of Defense.[20] This data is then merged with a range of proprietary marketing data at the Department of Defense's Joint

[20] A discussion of the NCLB Act's provisions requiring schools receiving federal funds to provide certain student data to the Department of Defense is outlined in a Congressional Research Service report titled "Military Recruitment Provisions Under the No Child Left Behind Act: A Legal Analysis." The report was retrieved on 19 October 2012 from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA494158

Advertising Market Research & Studies (JAMRS) program where elaborate recruitment campaigns are developed to target those young people most likely to enlist.[21] That those most likely to enlist are largely Black, Latino, immigrant, and/or poor students helps us see how miseducation and diploma denial in our public schools link up with modes of state surveillance and military recruitment as well as marketing databases.

Proprietary ecologies draw on a multitude of social and material circuitries to facilitate a surveillant assemblage that monitors everyday behaviors. As Haggerty and Ericson (2000) describe it "this assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows" that are then "reassembled into distinct 'data doubles' that can be scrutinized and targeted for intervention" (p. 606).[22] The complexity and magnitude of this assemblage encourages what Latour (1987) discusses as a "black box;" where its operations are perceived as too cumbersome to comprehend so that it becomes easier to focus solely on the technicity associated with the input and output of this now 'boxed' assemblage. This black boxing was pronounced in my interviews with young people. While most could describe in detail and with sophistication how a particular proprietary medium, such as Facebook, helped them do all sorts of things, they had little vocabulary to explain what it is Facebook does. The diffused and circuitous design of this proprietary surveillant assemblage is

---

[21] JAMRS describes itself as "an official Department of Defense program responsible for joint marketing communications and market research and studies" whose objective is to "explore the perceptions, beliefs, and attitudes of American youth as they relate to joining the Military." Retrieved 4 November 2012 from http://www.jamrs.org/

[22] Haggerty and Erikson (2000) theorize the 'data doubles' as additional selves and note that "while such doubles ostensibly refer back to particular individuals, they transcend a purely representational idiom" (p. 614). It is in this sense, that they see the surveillant assemblage as productive of "a new type of individual, one comprised of pure information."

precisely what makes it so difficult to see in everyday environments; its complexity is black boxed leaving a banal presence that fades in one's environmental consciousness if it ever enters it.

The black or white box shaped iPhone is a fitting example of how proprietary ecologies operate in the background through an assemblage of surveillant circuitry to aggregate everyday data. In 2011, two researchers, Alasdair Allan and Pete Warden, discovered that the iPhone was locally storing a hidden file containing data on all the places the device--and thus presumably its owner---had been.[23] Allen and Warden then developed a software application called iPhone Tracker that allowed iPhone owners to access the data from the file on their device and visualize it over time using open source mapping data from OpenStreetMap. For a moment the black box around the iPhone was partially opened, exposing some of its circuitry and allowing people to visualize some of the data Apple was able to see. To quell the public concerns over privacy that erupted as a result of this exposure, Apple quickly removed this local file in a subsequent update to the iPhone operating system. The surveillance practice was never curtailed; the exposed circuitry was simply black boxed again by removing the ability of iPhone users to easily visualize the locative data their iPhone continued to generate.

[23] 'Local' in this context means that the file was stored on the phone itself rather than remotely on a server located elsewhere.

As Figure 2.1 illustrates with the locative data from my own iPhone, the iPhone Tracker allows us to see some of the ways data is spatially and temporally aggregated at multiple scales. Holidays in Massachusetts, international travel, academic conferences, and routine commutes in New York City become rationalized, objectified, and aggregated into my everyday data in proprietary ecologies. Although the iPhone abstracts me from my territorial setting in producing this data, the abstraction remains locative. This means that while a 'data double' of me is produced, something akin to a 'data double' of my space is also produced. My movements are surveilled along with the spaces I move through, thus generating mapped digital footprints that are distinct to me. Koskela (2000) argues that "surveillance actually makes space a container" in which the "watched objects

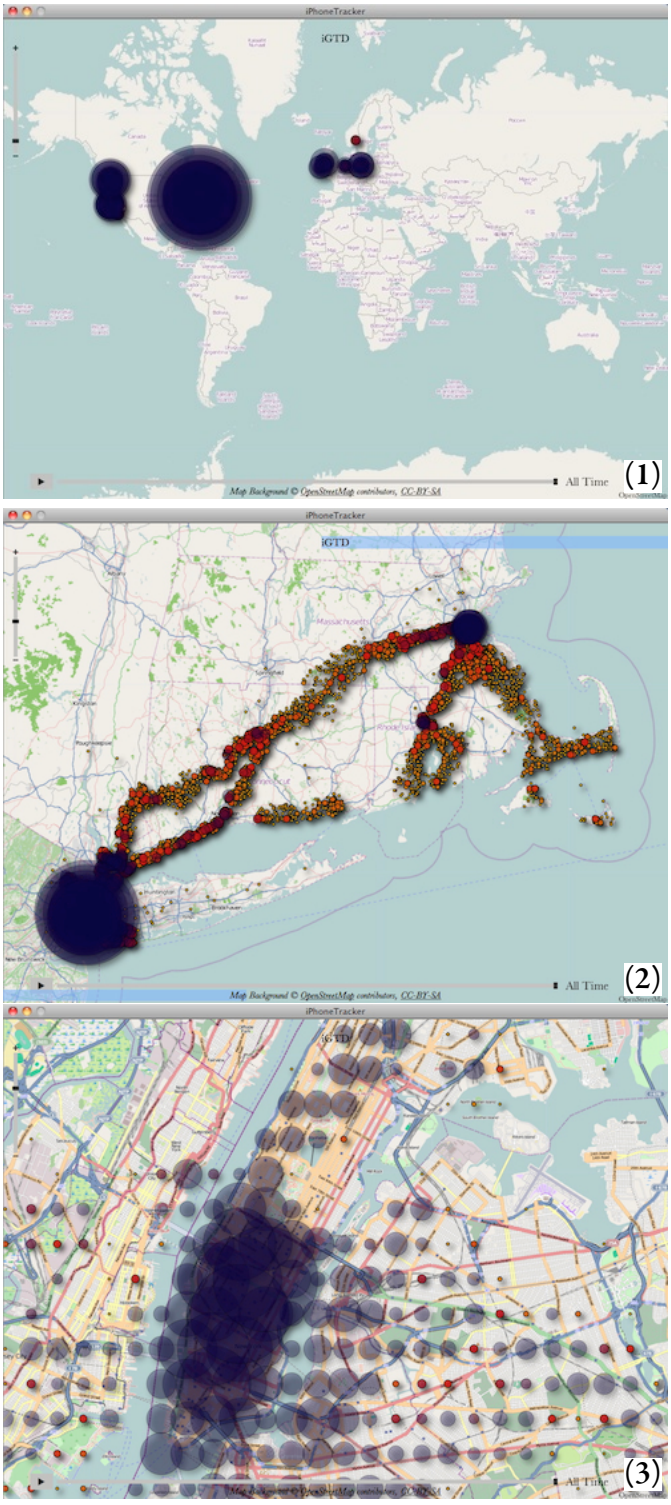

Figure 2.1 iPhone Tracker Screenshots

One year of locative data plotted simultaneously on an OpenStreetMap at the international (1), interstate (2), and local (3) scale.

exist" (p. 248). As a container, the surveilled spatialities of our lives add a valuable layer of locative metadata to our aggregated experience. Regardless of wether my name, age, social security number, or other identifying information is or becomes associated with this data, my distinct movements through space become a valuable indicator of who I am for corporations and governments alike. A report from McKinsey & Company, a large and influential global management consulting firm, helps emphasize the "huge new value" associated with location data:

> Unlike the other domains that we have examined, new pools of personal location data are not confined to a single sector but rather cut across many industries, including telecom, retail, and media. This domain offers the potential for huge new value creation over the next ten years that we estimate at more than $100 billion in revenue to service providers and as much as $700 billion in value to consumer and business end users. Capturing this value will require the right enablers, including sufficient investment in technology, infrastructure, and personnel as well as appropriate government action (Manyika et al., 2011, p. 85).

Black boxes like the iPhone enable the capturing of this potential value of locative data through circuitous surveillance, all the while attempting to conceal its circuitry so as not to provoke concerns of privacy that might problematize this practice or compromise its technicity. Such data could be valuable to the person generating it by allowing them to keep track of the places they've been over time, locating a lost iPhone, or measuring how far they've run in a day. Yet, while increasing Apple's ability to produce value, the black boxing of the iPhone also limits its empowering potential by making it more difficult for people to draw on their own data for their own ends.

Circuitous surveillance, and the situational ignorance it encourages, increases the proprietary value of the data it produces because it is perceived to be more authentic, predictive, and actionable by governments and corporations. This logic can be seen in the devaluing of

social profile data that is deliberately and often thoughtfully entered compared to the data generated through the tracking of online behavior within and across social network sites. This logic has roots in positivist social science research and holds that if the subject is aware they are being researched, then that awareness shapes their behavior and thus contaminates the authenticity of the observational data. Imagery of developmental psychologists observing children playing through a two-way mirror is an appropriate reference point for this research logic. Yet, this encouraging of situational ignorance is about more than just producing seemingly actionable intelligence, it is also about controlling representation and ownership in information ecologies. As the iPhone Tracker illustrates, the circuitry of proprietary ecologies can be visualized, and in doing so it can take on new meanings by allowing people to aggregate their own data according to their own interests and desired representations. Opening and demystifying the black box reveals informational domination to be less totalizing than it otherwise appears and something that can be commandeered by the surveilled.

Rationalization

Proprietary ecologies rationalize data according to the interests and concerns of private owners. In this way, proprietary ecologies are epistemological entities facilitating corporate and government research to produce privatized knowledges that are kept out of the public domain. I use the term ‘rationalize’ to evoke industrial processes of classifying certain workers and work as necessary in the workplace and others as unnecessary and thus warranting of outsourcing and off-shoring in the name of efficiency (cf. Greenbaum, 1979). Not only do proprietary ecologies continue to help facilitate these historical processes of workforce/workplace rationalization, but

they epistemologically reproduce such processes in the amplification and reduction of information through data generation and circulation. With data being an abundant and seemingly exponential resource in contemporary environments, there is little need to maximize its generation through the exploitation of labor. Rather, corporations and governments produce value around certain kinds of data that can then be enclosed and privatized so as to regulate access to it. The information produced from this data through mining and other rationalization practices thus becomes profitable private property. While the exploitation of labor persists, labor is focused on the filtering, mining, processing, and circulation of data. In this way, the exploitation of labor can be understood as part of the broader trend toward enclosing, mining, and regulating access to data, rather than the generation of data.

According to Latour (1999), there is a "dialectic of gain and loss" (p. 70) in the production of data; at each information-producing step of the research process some context is exchanged for greater circulation and visa versa. The owners of a particular proprietary ecology, such as Google, thus decide at what point along this chain of amplification and reduction data should be produced and to what ends the knowledge gained will be put. Zook and Graham (2007) look specifically at GoogleMaps to unpack how the political and economic agenda behind map-generating code lead to the highlighting or obscuring of information regarding different locations in user search results, thereby influencing user perceptions of place. In a similar vein, Introna and Nissenbaum (2000) have looked at how a search engine's politics and technical abilities work together to give prominence to certain sites in their search results, at the expense of others.

Graham (2005) develops the concept of "software-sorting" to describe how code automatically and continually mediates our geography to distinguish between privileged and marginalized people and places. Examples of this software-sorting include "electronic road pricing, 'bypass' immigration based on biometric IDs, 'virtual' and competitive electricity markets, Internet systems where the 'packets' of data are individually prioritised, online geodemographic consumption systems, facial recognition closed circuit television on city streets, and electronic tagging systems for low-level offenders" (p. 565). In linking this with broader neoliberal restructuring in industrialized nations, Graham argues that "software-sorting techniques are diffusing rapidly to mediate the production, consumption and experience of physical and electronic mobility systems and spaces, urban neighbourhoods, a whole plethora of service, finance, and communication systems, and even city streets" (p. 575). The current, and perhaps already past, debate over Net Neutrality standards in the US help consider one example of this sorting: the prioritizing of data packets in information communication.

Until 2003, public access to the internet depended largely on dial-up connections that transmitted data through a telecommunications infrastructure (Zickuhr & Smith, 2012). The phone lines of these services were federally regulated to abide by a 'common carriage' policy that Breitbart (2006) explains prohibited telecommunication services who owned phone lines from prioritizing their customers' calls over those of competitors'. This meant that internet service providers (ISPs) could pay telecommunication companies for access to their phone lines, and that the data transferred by ISP subscribers through the phone lines could not be sorted for purposes of creating a tiered system. Common carriage was problematized as broadband connections, that funnel data through cable services rather than telecommunication services,

increased in popularity. According to the Pew Internet & American Life Project, 62% of US adults over the age of 18 had broadband access at home as of August 2012, while just 3% had dial-up access (Zickuhr & Smith, 2012).

The National Cable and Telecommunications Association (NCTA) argued that cable companies should not be held to the same common carriage standards as telecommunication companies. In 2005, cable broadband was classified as an "information service" rather than "telecommunication service" and thus exempt from adhering to common carriage standards.[24] A subsequent FCC decision, extended this exemption to telecommunication companies.[25] Meinrath and Pickard (2008) argue that these decisions countered a hundred years of telecom policy by removing safeguards against the sorting and prioritizing of data packets in information communication. Early effects of these decisions could be found in two attempts by telecommunications and cable companies to censor data traveling through their networks. In 2006, Time Warner (formerly AOL Time Warner) blocked emails sent through its network from groups such as MoveOn.org and the Christian Coalition who had teamed up in opposition to AOL's proposed tiered email system. In 2007, Verizon blocked text messages sent through its network from NARAL to their supporters. Meanwhile, a 2012 report from the Federal Communication Commission (FCC) indicates that approximately 6% of the US population still lack access to fixed broadband service, with rural and tribal areas disproportionately effected.[26]

---

[24] The syllabus of National Cable & Telecommunications Association et al. v. Brand X Internet Services et al., can be found at: http://en.wikisource.org/wiki/Ashcroft_v._Free_Speech_Coalition?oldid=420606.

[25] More information on the FCC decision can be found at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260433A1.pdf

[26] The FCC's Eight Broadband Access Report was retrieved on 23 September 2012 from http://www.fcc.gov/reports/eighth-broadband-progress-report

Thus highlighting that in addition to the sorting of data within information ecologies, the people and places that get access to these ecologies are also sorted.

In considering some of the ways people, place, and media are rationalized in proprietary ecologies, I wish to show how government and corporate interests draw on modes of surveillance and privatization to suite their own interests. Through rationalization in proprietary ecologies, the interests and concerns of proprietors produce and reproduce historical problems of segregation, stereotyping, and inequality in everyday environments. This not to suggest that society is lurching toward a techno-deterministic dystopia where people and places are controlled through a carefully coded matrix. As Chapter 1 introduces, and Chapter 4 builds upon, the young people I interviewed and worked with were not passive dupes of the big bad machine. Rather, their somewhat unpredictable social actors negotiating historical processes in our environment -- such as territorialization, classism, segregation, sexism, stereotyping, and racism -- that have extended to our information ecologies. As information ecologies expand within everyday environments, considering how these processes work the informational aspects of our environment become increasingly important.

Objectification

Proprietary ecologies work to objectify the data they aggregate and rationalize. This can be for purposes of data circulation, control, and/or commodification, but in either case this objectification is shaped by private interests and concerns. Objectification works to bound and package experiences into discrete objects that can be distinguished from, and connected to, other objects. In so doing, objectification open's up everyday data to commodification through

historical regimes of property ownership. To own ‘something’ or to claim it as property, it must first be defined through a boundary-making process. Having worked previously for an Intellectual Property research firm, I would receive requests from corporations looking to copyright, trademark, or patent a particular brand and/or product. My job was not to facilitate the legal work associated with a copyright, trademark, or patent but to see if such brands or products already existed and thus could be owned by this corporation. This entailed searching both public and private databases to see if any brand or product ‘like‘ the one they were proposing had already been defined elsewhere. If a brand or product, or its likeness, had not already been defined then the corporation would proceed with the legal work to define and own this brand or product themselves. While common customers were software, beverage, and pharmaceutical companies, this process of objectifying information to commodify it extends well beyond these industries and into scientific fields such as biology.

Calvert (2008) analyzes the role of intellectual property in the field of molecular biology to argue that processes of commodification and reductionism are intertwined. The reductionist approach of molecular biology, Calvert argues, epistemologically works to isolate and define biological information in a way that fits readily into existing regimes of property ownership. One can consider the reduction of biology to disentangled DNA structures and paten-able genes as prominent examples of how processes of commodification and reduction intertwine. In both cases objects are clearly defined and separated from other objects, allowing each to be patented similarly to the way a brand might be trademarked. Here we can see how the circuitous surveillance and rationalization of proprietary ecologies help aggregate and mine our experience

for the purposes of objectifying available information deemed ‘important’ or ‘valuable’ to the various proprietors of that ecology.

This objectification can also be found in justifications for the legal constitution of proprietary ecologies themselves. Hunter (2003) and Lemley (2003) have show how a ‘cyberspace as place’ metaphor is increasingly drawn on in the US legal system to justify the mapping of laws regarding physical borders and property onto cyberspace. Hunter (2003) argues that this phenomenon has sparked a “Cyberspace Enclosure Movement” whereby “private interests are reducing the public ownership of, and public access to, ideas and information in the online world” (p. 3). Boyle (2008) discusses the enclosure movement of 19th century English agriculture to highlight the historical continuity of enclosure. Yet, he also points to a historical discontinuity in arguing that in our contemporary legal environment “things that were formerly thought of as either common property or uncommodifiable are being covered with new, or newly extended, property rights” (Boyle, 2008, p. 37). While even this discontinuity can be considered continuous in that it is how capitalism historically operates -- to continuously produce new markets and modes of capital accumulation -- what is ‘new’ are the spaces and objects now being commodified. Just as resources commonly understood as public were enclosed and commodified in the 19th century, resources such as social networks, identities, and data are now also being enclosed and commodified.

When we consider the packaging and package-switching of data entailed in the end-to-end architecture of the internet (van Schewick, 2010), we find a parallel to the reductionist approach of molecular biology. In sorting and privileging certain data packets or biological molecules over others, large swaths of our biological and informational environment become

influenced by commercial interests. The objectification and privatization entailed in the internet's architecture extends to its governance as well. Mueller (2002) has shown how the formation of property rights around internet names (i.e. domain names) and numbers (i.e. internet protocol addresses) facilitated the institutionalization of private governing arrangements around these "resource spaces" (p. 58) through the International Corporation for Assigned Names and Numbers (ICANN).[27] Mitchell (1995, 2003) and Lessig (2004, 2006) have shown how the software and hardware that constitute this architecture and governance also regulate everyday possibilities by encouraging and discouraging various interactions. While the very design and operation of society's vast distributed communication infrastructure format interactions for efficient circulation, they also objectify interactions through this formatting. Once formatted, objectified data fit into existing regimes of property ownership, and in most cases are folded into the current enclosure movement. The following section offers an example from the subways of New York City to illustrate this process.

Everyday Data at Work

I begin in the subways of New York City, with an ad campaign aimed at media buyers and advertisers, to illustrate how proprietary ecologies operate through the intimate, social, material, and translocal dimensions of our human-environment interactions to produce everyday data. According to Flickr, Figure 2.2 was photographed with my Apple iPhone in May 2010.[28] I

[27] ICANN is the U.S. based non-profit corporation that oversees the global management and assignment of domain names and IP addresses associated with the internet. ICANN was established in 1998 to take over these responsibilities from the U.S. government.

[28] Photographed on 7 May 2010 in the First Avenue subway station of New York City's L train.

was exiting the L train at the First Avenue station when this out of place advertisement caught

Figure 2.2 Oxygen Advertisement in NYC Subway

my attention. Figure 2.2 is a trade advertisement for NBC Universal's Oxygen Network. Trade advertisements are targeted towards those working in a specific industry or profession, as opposed to advertisements targeted towards consumers. Figure 2.2 is the kind of advertisement more likely to be found in a trade publication such as *Advertising Weekly* that boasts an audience working in or with the advertising industry. The subway stations of New York City are unusual places for trade advertisements.

However, the western portion of the L line connects the Williamsburg, East Village, Union Square, and Chelsea neighborhoods of New York City. As such, L train commuters constitute an urban population as close to reality as Florida's (2004) much hyped "creative class"

gets. These 'creative commuters' are less members of a romanticized class who produce creative economies in locations they choose to inhabit, and more the everyday commuters who may share a common experience of traveling to work together for Madison Avenue and Silicon Alley industries; media industries that have been socioeconomically stimulated in New York City through deliberate and organized urban development (Indegaard, 2000). If you're a television network looking to speak to media buyers and advertisers or at least those influencing them, then the western portion of the L line is an appropriate location for advertising. The most opportune time to capture the attention of these creative commuters would be during May upfronts; when networks organize media events to showcase their upcoming Fall season and to sell Fall commercial time upfront to media buyers and advertisers. Hence the May appearance of this spatiotemporally targeted trade advertisement for creative commuters in a public space trafficked by common consumers. This ad offers a valuable insight into another dimension of our ecology, one where we are both consumers and commodities that are bought and sold by fellow creative commuters on the L line. The spatial temporality of Figure 2.2 brings into focus its motivations and helps articulate how proprietary ecologies produce value around everyday data, particularly in regard to young women's data.

Figure 2.2 presents creative commuters with Angela, a young white blonde Oxygen fan from Dallas, Texas. Angela "tries new products and is open to new messages," she spends big and "makes the decisions," and most importantly she "indexes high for word of mouth," recommending *[your_commodity_here]* to all of her friends and family. The point is bluntly delivered: Angela, as a charismatic consumer, leaves a digital footprint more valuable than those of other consumers. "In advertising" Oxygen advertises to the creative commuters en route to

buying ad time “all women are not created equal.” To a medium like the Oxygen Network, Angela is a valuable consumer and commodity that brings a competitive edge. In the data mining of everyday experiences, Angela is gold for a cyberprospector.

Figure 2.3 illustrates a more overt form of this trade advertisement that was reserved for trade publications.[29] Absent the gaze of average consumers the “In advertising ... all women are not created equal” byline becomes the glitzy headline. Angela is juxtaposed with the older, poorer, less professional, less educated and shrinking viewership of Lifetime. “If you’re looking for ROI,” Oxygen advertises to the readership of advertising and marketing publications, “meet Ms. Right.”[30] Here we see the objectification of consumer demographics to privilege the market value of certain women at the expense of other women. While this is the historical function of advertising, what I wish to draw attention to are the ways data is increasingly draw on to

Figure 2.3 Oxygen Print Advertisement
© 2010 Oxygen Media

[29] Retrieved from the *Wall Street Journal* on 22 September 2012 from:http://online.wsj.com/article/SB10001424052748704534904575132121037306214.html

[30] ROI stands for return on investment, and refers to the profit gained in relation to the capital invested.

understand, parse, and market various demographics. Previously, only a limited amount of data on consumers was available to markets, and often only when volunteered by a consumer through participation in specific market research projects. Now, a seemingly endless stream of consumer data is available to marketers through proprietary ecologies and at relatively low cost. Angela's embedding in the circuitry of proprietary ecologies and her charismatic consumption makes her an informational ideal in media industries.

Oxygen's parent company NBC Universal is a major player in the proprietary ecosystem with a consumer database of Olympic proportions. A recent article in *The New York Times* discusses the "trove" of behavioral data NBC Universal has mined from their $4 billion purchase of exclusive broadcasting rights for the Olympic Games, from 2012 to 2020 (Chozick, 2012). Exclusive ownership of the broadcasting rights has already given NBC Universal access to everyday data on the 217 million viewers in the US who watched the 2012 London Games. When it comes to the Olympics, NBC Universal is researching who is watching, where they're watching, when they're watching, and what device and platform they're watching it on. Oxygen and the Olympics are both part of NBC Universal's surveillant assemblage and they generate troves of data for mining. While the Olympics derives its value from a broad and diverse cultural appeal, Oxygen's value is derived from its marketing niche with young woman. For NBC Universal, aggregating Angela's everyday data while also selling her attention through the Oxygen medium is lucrative business -- business they believe their competitors in the broader propriety ecosystem should envy. It is, after all, the "#1 youngest most upscale fastest growing women's network." Take that, Lifetime.

Turow (2006) notes in his investigation into marketing discrimination that the marketplace has become "deeply involved in defining an important basis for belonging in society" (p. 3). In a consumer culture defined by interactivity, targeted tracking, and data mining, he argues a sense of "niche envy" speaks to this pervasive market-based approach to societal belonging. Niche envy emerges among both corporations and consumers, in how one corporation might envy a competitor for the perceived value of their customers, as well as the envy one consumer might have toward another who is perceived to have a digital footprint that brings greater market attention. Figure 2.2 and Figure 2.3 evoke envy on both counts. Oxygen's customers should be envied by their competitors, such as Lifetime with its older less affluent demographic. While Angela is receiving attention and appreciation from the market that other consumers should envy. Of course, in the lived experiences of youth this relationship to the market provokes envy, along with disdain, curiosity, and indifference indicating that not everyone strives to be the object of market affection.

We are all participant observers in proprietary ecologies. Angela doesn't just observe Oxygen's content, she participates in the Oxygen medium by consuming its commodities and circulating them through her social network, all the while producing data that's objectified and commodified. The interactions of people, place, and media in proprietary ecologies mean the more a person watches, likes, shares, tweets, retweets, updates, checks in, locates, maps, downloads, emails, searches, and most importantly, buys, the more their everyday data is aggregated, rationalized, and objectified. Indeed, I am not external to this process. I can time this advertisement with May upfronts because my Apple iPhone embedded metadata in the image when it was taken. When I imported the image file from my Apple iPhone to my iPhoto

application on my MacBook Pro I also imported metadata on when, where, and how this piece of visual data was produced. When I uploaded the image file from my Apple iPhoto application to my Flickr Photostream on Yahoo! web servers, the metadata was uploaded with it.[31] My interactions with this proprietary media facilitate my own research process by allowing me to archive and retrieve Figure 2.2, and know that "this photo was taken on May 7, 2010 using an Apple iPhone."[32] These interactions also facilitate research by the staff of Yahoo! and Apple, allowing them too to archive and retrieve Figure 2.2 and know when, where, and how it was taken. Angela and I may not be equal in advertising, but we both participate in proprietary ecologies.

Rose (1998, p. 151) discusses how the pervasiveness of psychology and consumerism in the contemporary neoliberal state co-produce a new entrepreneurial subjectivity. This "entrepreneurial self" encourages a neoliberal politics of personal responsibility and risk taking for profit through constant self-rationalization and measurement. It can be seen in the explosive popularity of "self help" psychology from Eckhart Tolle to Dr. Phil that coincides with, and reinforces, a neoliberal unloading of public problems and government responsibilities onto individual citizens. This entrepreneurship can also be found in the multitude of individuals and small businesses generating mobile apps that aggregate and mine all kinds of data. As of September 2012 Apple's App Store claimed 700,000 of these applications for their iPhones, iTouches, and/or iPads (Etherington, 2012), while the Android Marketplace claimed over

---

[31] Metadata is a set of data about other data. Thus knowing the location of where I buy something adds metadata to my purchasing data.

[32] This image can be found on Flickr at http://www.flickr.com/photos/cyberenvironmentalism/4601945284/in/set-72157620415421058

675,000 as of October 2012 for mobile devices using the Google-owned Android operating system.[33] Each of these apps add a new surveillance circuit to the broader proprietary ecology and encourage rationalization and objectification through their technicity in the everyday. How many followers one has on Twitter, how many people 'like' or share a status update on Facebook, or how many places one has checked into on Foursquare, all become internal measurements of the self, as well as external measurements for corporations, governments, and others to draw on to assess anyone's productive value.

Angela, as a market-base idealization of young women, engages in a range of self-measuring, self-promoting, and convenient human-environment interactions; typically, without the intention of helping any market. We can imagine Angela's iPhone locating her at Target while she buys 'as seen-on-Oxygen' commodities with her Bank of America debit card, and then recommending those commodities to her friends and family via Facebook. Each of these interactions is aggregated, rationalized, and objectified for corporate commodification. The more Angela interacts with people, places, and media through apps like the Oxygen iPhone app -- designed to help Oxygen fans "socialize, interact and react in real time" -- the more NBC Universal can monitor and mine her interactions across multiple platforms, in real time.[34] If inhabiting an entrepreneurial subjectivity through such practices makes a person more conducive to a neoliberal governmentality, as Rose (1998) argues, then it also makes a person more conducive to commodification in an informational mode of development by rationalizing and

---

[33] Retrieved from the Android Marketplace on 5 October 2012: https://play.google.com/about/features/

[34] Retrieved from Apple iTunes on 5 October 2012: https://itunes.apple.com/us/app/oxygenlive/id389178361?mt=8

objectifying their human-environment interactions for circulation and privatization in proprietary ecologies. This of course is just a market-based ideal of young women and not necessarily the lived experience of young women. While Angela is a charismatic consumer that represents the way other people are encouraged to consume, this does not mean that even young women who inhabit such an entrepreneurial subjectivity through their lived experiences do so consciously. This is to say that the ways people, young and old, learn to participate in proprietary ecologies for work, play, and/or convenience is fostered at some level by corporate actors.

Andrejevic (2013) discusses the role of mobile apps, such as Oxygen's, in producing an estranged free labor by contributing to "the misrecognition of one's own participation in the very forces that seem to come from elsewhere" (p. 162). A 2012 report from the Federal Trade Commission (FTC) highlights some of the ways this 'misrecognition' is fostered. The FTC reviewed the privacy disclosures and data aggregation practices of 400 mobile apps that were explicitly marketed for young people (Mohapatra & Hasty, 2012). Of the 400, 59% transmitted personal information on the user to the app's developer or third-parties such as an ad network or web analytics company. However, only 20% of these apps contained any kind of privacy disclosure that explained to the user what was being done with their personal information. Further, many of the apps that did have privacy disclosures often contained incorrect or misleading information, or long highly-technical and jargonistic explanations.

The circuitous surveillance of proprietary ecologies, and the black boxing they encourage, allows one to focus mainly on the technicity of mobile media such as Google Maps (i.e., its usefulness in daily navigation), while tuning out the growing role engagements with this media play in modes of informational development. All of which contributes to the making of

estranged free labor in advanced capitalist societies. Yet, as my interviews with young people like Megan suggest, this labor may not be so estranged. For most of the young people I interviewed, a focus on the technicity of particular media was always primary but a sense that profit-making was undergirding this engagement, and that they had some sort of role in it, was frequently articulated. Whether or not 'Angela' is estranged from the free labor she contributes, Megan suspects this labor might indicate that the media owns us. While this sense of ownership was expressed through a discourse of addiction that was also articulated by other interviewees in Chapter 1, interviewees also regularly noted that they weren't sure how but they were sure companies like Facebook and Google were profiting handsomely off of their participation. Part of this was due to the release of *The Social Network* during the period when the interviews occurred. The story of Mark Zuckerberg starting a social network site and becoming the world's youngest billionaire as a result suggested to interviewees and the YDRC that significant profits were being generated through supposedly 'free' media services like Facebook.

Oxygen's marketing of Angela's human-environment interactions to creative commuters brings to the fore how proprietary ecologies create a privatized interface between people, place, and media to commodify everyday data. Proprietary ecologies assemble knowledge on the neoliberal citizen consumer through the rationalization and objectification of their daily behaviors into privatized objects of data. These knowledges increase corporate profits by helping marketers reach consumers more effectively, sell their consumers to others, and use their consumers to market to their friends and family. Although dominating, this process is not monological. People are dynamic and resilient social actors who are constantly adapting to and crafting a complex life course. They internalize as well as rework, resist, and reproduce the

world around them. It may feel as though the internet owns the people in proprietary ecologies, but the internet is a material social formation of people.

Conclusion

As society increasingly shapes itself and its spaces with proprietary media, we must critically engage this shaping to understand its role in relation to the means of production in advanced capitalist societies. The circuitous surveillance at work in proprietary ecologies mystifies the ways it rationalizes and objectifies the production of everyday data and estranges everyday people from their role in broader modes of informational development. Although appearing totalizing by virtue of its scope, scale, and complexity, this circuitry of dispossession and its consequences can be visualized, understood, and potentially reworked by demystifying informational modes of development. When we consider the role of media in the environments of youth, their experiences not only take place within privately owned property but often the data generated around their experiences become privately owned property and rarely, in either case, are they -- the source of this data -- given any ownership in the process.

The study of proprietary ecologies presents a way of understanding a particular phenomenon in our contemporary neoliberal environment that transcends the distinctions between industrial and informational or offline and online: *privatization*. The intertwining of mediation and privatization in daily life is more pronounced than ever yet it remains an historical process. In Thomas Edison's phonograph and telegraph we find an industrial prototype of our contemporary proprietary ecology that points to longstanding questions of ownership, access,

and power regarding the mutual shaping of people, place, and media. Edison (1878) argued that the development of the phonograph presented the following *faits accomplis*:

1. The captivity of all manner of sound-waves heretofore designated as "fugitive," and their permanent retention.
2. Their reproduction with all their original characteristics at will, without the presence or consent of the original source, and after the lapse of any period of time.
3. The transmission of such captive sounds through the ordinary channel of commercial intercourse and trade in material form, for purposes of communication or merchantable goods.
4. Indefinite multiplication and preservation of such goods, without regard to the existence or non-existence of the original source.
5. The captivation of sounds, with or without the knowledge or consent of the source of their origin. (p. 3)

To Edison, the phonograph worked to capture, reproduce, transmit, multiply, and preserve data (in his case, audio data) with or without the knowledge, consent, or continued existence of the original source. In combining these affordances with those of the telephone, Edison envisioned a "telegraph company of the future" (p. 6) that would transform everyday life, from letter-writing to education to music to advertising. That Edison's language overlaps with McKinsey and Company's call for 'capturing the value' of locative data provides a bridge between the industrial and informational by historically situating circuits of dispossession. What if the original source of everyday data, such as young people, had knowledge of the capturing, reproducing, transmitting, multiplying, and preserving of their data? What if they're consent in processes of surveillance, rationalization, and objectification were required? How might these considerations have shaped the technicity of the phonograph and how might they shape the technicity of the internet? And, how might more meaningful participation in this process shape modes of transduction in everyday environments?

A critical consideration of proprietary ecologies and their consequences provoke historical questions of ownership, access, and power, particularly regarding matters of privacy, property, security, and participation. Yet each of these matters are themselves complex assemblages of human-environment interactions that are experienced relationally and subjectively over the life course and from situated vantage points. We are always situated in multiple proprietary ecologies with differentiated commitments to and engagements with them. Where one stands in a particular proprietary ecology and what consciousness one has of this standing shapes their experiences and understandings of privacy, property, security, and participation. In the following chapter I outline the participatory action design research (PADR) entailed in the MyDigitalFootprint.ORG Project to understand young people's experiences in proprietary ecologies through collective critical inquiry into its circuitry with a team of youth co-researchers. Together, we considered the consequences of our mediated human-environment interactions to imagine more empowering interactions through the design of our own open source social network.

Chapter Three
The Medium is the Method

In this chapter, I unpack both the medium and the methodology behind the MyDigitalFootprint.ORG Project to explain the project's participatory action design research (PADR) approach to knowledge production. In the proprietary ecology of everyday life the media that afford routine human-environment interactions also function to aggregate, format, and privatize those interactions. McLuhan (1964) declares that "the medium is the message" (p. 9) to draw attention to the reciprocity between media, defined as "any extension of ourselves" (p. 10) and messages, defined as "the change of scale or pace or pattern that [a medium] introduces into human affairs." In making the medium the message, McLuhan argues that human experience and technology are locked in a state of reciprocity thus producing an environment of relationships where people and extensions of people mutually shape one another. The methodology of this mutual shaping, particularly within proprietary ecologies, is the focus of this chapter. To understand the methods by which proprietary technologies mediate human-environment interactions is to understand how these interactions shape, and can be shaped by, the scale, pace, and pattern of everyday experiences.

The medium remains the message under transnational informational capitalism, but also emerges as the method. Regardless of whether research is for profit, governance, or social justice, the methods used to rationalize and mine human experience mediate the knowledge produced. Whether this mediation is privatized or participatory influences whether the knowledge produced is proprietary or public. Thus shaping both the aims of the research and the ends to which it can be applied. It is with this in mind that I unpack both the medium and the

methodology behind the MyDigitalFootprint.ORG Project to outline a PADR approach to producing knowledge with young people growing up in proprietary ecologies.

The MyDigitalFootprint.ORG Project took place over a period of thirteen months, the final six of which involved collaborative research and design with five youth co-researchers. Together we investigated how informational capitalism becomes objectified, internalized, reworked, and/or resisted through intimate and translocal interactions with and within our environment. Taking the medium as both our message and method, we organized our work around the production of an open source social network. This helped to demystify our routine behaviors in proprietary ecologies by negotiating new ones in a more open information ecology. Bringing our research medium's design and development into the fold of our participatory methodology allowed youth co-researchers to take on the role of social network producers and thus gain new perspectives otherwise mystified to social network consumers.

Doing Participatory Action Design Research

Proprietary ecologies facilitate young people's interactions while simultaneously privatizing them through a dialectical process of informational accumulation and dispossession. As such, involving young people in the design of their daily information environments is also involving them in practices of research and knowledge production. Collaborative social research and media design are needed to investigate and engage how proprietary ecologies operate to produce and reproduce informationalism through young people's routine engagements with social media. It is with this in mind that I summarize both participatory action research (PAR)

and participatory design (PD) methodologies before outlining the specific practices that produced the MyDigitalFootprint.ORG Project's medium and methodology.

A participatory action research (PAR) approach aims to involve people simultaneously in the collective investigating and improving of problematic situations in their environment. PAR represents an epistemological stance within academic inquiry that "assumes knowledge is rooted in social relations and most powerful when produced collaboratively through action" (Fine et al., 2003, p. 173). I argue that a PAR approach to understanding the proprietary ecology of young people's human-environment interactions means realizing the knowledge rooted in those interactions through youth-based collective research and action. Such an approach helps to understand the environmental experiences of youth as relational, contextual, and constructed at multiple scales throughout the life course (Cahill, 2004; Hopkins & Pain, 2007).

A participatory design (PD) approach aims to involve people in simultaneously designing and improving problematic technological arrangements in their everyday environment. In a digital media context, PD "shares some theories and methods with user-centered design and interaction design, but the main thrust is on democratic and emancipatory practice" (Greenbaum & Loi, 2012, p. 81). PD is primarily concerned with how to involve everyday people in the practice of design (Bannon & Ehn, 2012). Like PAR, a PD approach values the knowledge rooted in the human-environment interactions of the design process, and aims to enhance that knowledge through collective practices.

A participatory action design research (PADR) approach aims to involve people in collaborative research and design simultaneously to investigate and improve problematic human-environment interactions. PADR makes contextual and relational understandings of everyday

experience possible through cyclical processes of collaborative research, design, and reflection. Combining both PAR and PD, a PADR approach can investigate and involve the people, places, and media that afford engagements in proprietary ecologies. Through its research and design politics, a PADR approach offers a counterweight to the everyday pedagogy of proprietary ecologies. Instead of producing new knowledges through proprietary means that are largely mystified to all but their proprietors, a participatory approach counters this production of knowledge by opening up regimes of ownership and involving 'users' in the means of production.

With information systems part and parcel of our urban infrastructure, PADR has been drawn on increasingly in the emerging field of Urban Informatics to understand and engage urban development according to situated interests and concerns (cf. Bilandzic & Venable, 2011; Foth & Adkins, 2006; Foth et al., 2011).[35] In the context of young people, this means taking seriously the knowledge produced through their routine behaviors in proprietary ecologies while also developing a medium and a method through collaborative research and design that values their own situated interests and concerns. Fine et al. (2003) note the ways PAR has increasingly lost its politics overtime to become more a series of techniques. Cognizant of this history, I aimed not to reproduce the specific techniques entailed in previous PAR, PD, or PADR projects. Instead, the focus was on addressing the YDRCs concerns, challenging their knowledge production, and drawing existing methods or developing new ones that served these ends. In

---

[35] According to Foth, Choi, and Satchell (2011), Urban Informatics considers the city as an ecological construction of technological, architectural, and social laters in order to investigate the "processing of information particularly via network technologies, which comprises a wide range of urban constituents from the overall configurations of the city" to "the individual's day-to-day interaction with technologies" (p. 4).

doing so we participated more critically in our own modes of becoming and knowing in proprietary ecologies. The MyDigitalFootprint.ORG Project thus took a PADR approach to involve New York City youth in a collective process of understanding and engaging their human-environment interactions in proprietary ecologies in order to build their capacities for more open information ecologies.

Identifying Matters of Concern

The MyDigitalFootprint.ORG Project developed in two primary phases to involve young people early on in shaping the project's matters of concern. My interest as the project facilitator remained the same: to understand the situated knowledges produced and reproduced around young people's privacy, property and security, and how proprietary ecologies mediate this (re)production. My methodological approach also remained the same: involving young people in collaborative processes of research and reflection through the co-design of an open source social network that addressed their interests and concerns. Key to the project, then, was to involve young people in identifying these situated knowledges, developing methods to investigate and analyze them, and understanding and responding to them through the design of a social network. I was guided by concerns such as what sort of interactions do young people want to amplify and reduce in their own research and design? What skills and literacies are needed to do this research and design, and how can they be fostered? These were the broad questions to be identified in interviews, unpacked in workshops, and acted upon through collective research and design.

The first phase entailed recruiting and interviewing 15 young people ages 14 to 19 living in New York City. Interviews were semi-structured and offered an in-depth focus on

participants' interactions with ICTs and what, if any, interests and concerns emerged through critical discussions of these interactions. The second phase entailed collaborative design and research with a subgroup of five youth co-researchers, the Youth Design and Research Collective (YDRC), to produce a social network that both further investigated and acted in response to the situated interests and concerns that emerged from interviews.

The YDRC and I worked together to demystify their information ecologies through collective research so that we could then collaboratively design an environment that reflected the interests and concerns of the YDRC and other research participants, and at the same time encouraged the kinds of interactions the YDRC valued. We came together for eight workshops at the CUNY Graduate Center over a period of six months: one project orientation workshop, six research and planning workshops, and one project cogitation workshop. Our work continued between these defined meetings with at least 162 emails, 56 forum comments, 31 texts, and nine phone calls exchanged.[36] Through this research and design framework the YDRC participated in investigating and re-orienting their information ecologies. The following sections chronicle the recruitment of interview participants and the assembling of the YDRC as well as the development of the medium and method behind the MyDigitalFootprint.ORG social network.[37]

---

[36] These numbers account only for the emails, texts, and phone calls that I was a party to, and do not account for any of the additional communications that occurred directly among members of the YDRC. The number of comments accounts for all postings and comments made to our internal SNS during our eight workshops.

[37] An interactive timeline of the MyDigitalFootprint.ORG Project can be found at http://mydigitalfootprint.org/timeline

Young People Recruiting

Before I began recruiting research participants for interviews, young people began recruiting me. In spring of 2010 I took part in a Participatory Action Research Methods module at my university. Each week two students presented the PAR projects they were facilitating, or about to facilitate, to other participants in the module. Having just submitted an application for the MyDigitalFootprint.ORG Project to the university's Institutional Review Board (IRB) and awaiting approval before recruiting participants, I was among those 'about to facilitate.'[38] On the day I presented I was paired with another doctoral student who discussed his PAR project on issues faced by immigrant adolescents, documented and undocumented, in New York City. Three of his youth co-researchers attended the module that day to present the findings of their project. Although I had informally discussed the project with students of mine, and young people I worked with in other capacities as an educator and freelance researcher, this was the first time I formally presented my interests and approach to young people. As a result, nothing in my presentation was specifically tailored for a young audience. Although it was a multimedia presentation it had been developed from parts of presentations previously given at academic conferences.

I delivered a twenty minute Keynote presentation summarizing my own interest in, and intended approach to, facilitating the MyDigitalFootprint.ORG Project -- speaking specifically about proprietary ecologies and how I planned to involve research participants in interviews and then youth co-researchers in the design of an open source social network site. When I finished the presentation the three young people in attendance were the first to ask questions. Their

[38] All research conducted at the Graduate Center of the City University of New York must first be evaluated and approved by the university's Institutional Review Board.

questions were pointed and impassioned, and following the module they approached me to ask if they could participate in the project. They expressed an eagerness to better understand how the internet worked, how social networks worked, and how they could build their own social network. Before leaving, each of them gave me their email addresses and asked for mine.

By the next day two of these young people emailed me, unprompted, asking for more information on how they could participate in the project. They asked for the information in a format they could share with their parents to get their permission to participate and with friends to encourage them to participate. I informed them that the project was awaiting IRB approval, but that they would be the first to be interviewed when approval was received. My interaction with these young people shaped the first incarnation of the MyDigitalFootprint.ORG medium, prompting me to combine all necessary project information for both interview participants and youth co-researchers as a recruitment website.

Recruiting Young People

My aim was to recruit interview participants and youth co-researchers who held a variety of interests and concerns. The aim was not to assemble a representative grouping of young people to generate generalized interests and concerns, but to assemble a situated grouping of interests and concerns that were experienced, expressed, and ultimately investigated by young people. To attain such a diverse grouping meant recruiting participants through a variety of social networks; online and offline. While age, location, race, class, and gender were all factors in recruiting participants, they were factors meant to elicit a diversity of interests and concerns. Since most of my participants would be under the age of eighteen, and would thus require signed

parental permission to participate, this recruitment also had to account for the parents of participants. My own education and research networks became the initial springboard for this recruitment as it allowed me to draw on a mix of contacts who could in turn validate my credibility and the authenticity of the project through their own social networks.

Asking a parent to let their teenage child talk to a guy in midtown Manhattan about their relationship with the internet, is asking for a lot of trust. For this reason, communicating that the project had been vetted by my university's Institutional Review Board; providing my academic credentials and those of my advisor's; clearly articulating participants' right to anonymity, confidentiality, and to stop participating at any time without repercussion; and outlining the benefits of participating in the project, all became components of the website. Having worked as an educational media researcher, academic technology consultant, intellectual property researcher, and adjunct professor throughout New York City provided me with a broad network of contacts, each of whom worked with young people in various capacities and could both share and vouch for the project within their networks. Young people interested in participating, or who had participated, were also encouraged to share the website to friends. However, it was made clear that they did not have to circulate the site, that their participation was in no way contingent on sharing the site, and that whether they chose to circulate the site in no way reflected on their level of participation.

Figure 3.1 Participant Recruitment Site

With a basic WordPress installation on leased server space, I designed the site to have three interconnected and sharable sections that could be viewed easily on most computers and mobile devices: Project Description; How to Participate; and, Your Rights as a Participant (Figure 3.1). Each section clearly articulated two levels of participation, as a *Research Participant* and as a *Youth Co-Researcher*. The levels were defined on the website as follows:

> Research Participants take part in a 90 minute semi-structured interview that revolves around their everyday experiences with privacy, security, and property in digital environments. Interviews take place at the Graduate Center of the City University of New York in midtown Manhattan.
>
> Youth Co-Researchers will help MyDigitalFootprint.ORG to develop an open source social network that further investigates the common concerns and interests voiced by

Research Participants, and entails a weekly time commitment of 5 hours for a period of 4-5 weeks.

All participation began with the interviews. Then, if an interviewee was interested in further participating as a youth co-researcher they could make that decision after the interview. Thus, all participants in the MyDigitalFootprint.ORG Project first took part in an in-person interview. Consent forms for participants 18 and over, assent forms for participants under 18 and consent forms for their parents, ways of contacting me, my academic advisor and the IRB administrator directly, as well as recruitment fliers were available through any one of these three sections.

The How to Participate section included a form young people could fill out, providing their contact info and indicating if they wanted to participate in an interview. In the month that the recruitment site was active, it generated 688 unique visits, 53 of which led to the submission of a form.[39] Of those, 22 interviews were scheduled based on the participant's age, location, and availability. Fifteen of the 22 interviews scheduled were conducted. The discrepancy between those interviews scheduled and conducted were due to no shows.

Interviewing Research Participants

Interviews with 15 young people, ages 14 to 19, provided an opportunity to explore individual experiences, interpretations, and concerns regarding key issues and questions. The interview protocol was loosely organized around four areas: how participants interacted with ICTs on a daily basis and what they liked and/or wanted to change about those interactions;

---

[39] Unique visits refer to the number of unique IP addresses, or devices, that access a website. This means that if a visitor checks the website 10 times from their laptop those visits are only counted as one unique visit. However, if a person visits the website from their laptop, a school computer, and their phone, then three unique visits would be counted.

when, where, and how participants accessed online content or participated in mediate communication; what role ICTs had in participants work and play; and, what issues the participants constructed or didn't construct as matters of privacy, property, and security. These semi-structured interviews were audio recorded with consent of the individual and their parent if they were younger than 18 years old. Interviews were coded, compiled, and analyzed for significant ideas and insights into my research topic, and to further form the basis for the group meetings and discussions that were part of the collaborative research and design process that would take place during second phase.

The semi-structured format of the interview was designed to explore the participants' daily routines that involved the internet in some capacity. Then, from this broad entry point, I asked about the participant's interests and concerns associated with those interactions. This approach allowed a more free flowing exchange where participants were able to talk about something they knew well--their everyday routines--and reflect on the interests and concerns they associated with those routines, if any. These routines, in every instance, entailed unprompted references to three or more of the following services: Facebook, Gmail, YouTube, iTunes, Google Search, Chrome, Safari, Yahoo! Mail, Bing, one of the seven mobile wireless providers in New York City, Google Maps, MySpace, Twitter, and Tumblr.[40] It was not difficult to find entry points for discussing their engagements with and within proprietary media.

As the interview progressed, I would begin asking more specific questions around matters of privacy, property, and security that were related to issues discussed by the participant. Questions were never constructed to have answers, but to provoke more discussion. In

[40] The six major mobile wireless providers in New York City are: AT&T, Sprint, Verizon Wireless, Metro PCS, T-Mobile, Cricket, and Qualcomm.

concluding the interview, I would then ask the participant to voice any other interests and concerns they wanted to discuss, including their motivations for coming to the interview. Once the participant felt we were done, the interview was concluded. The length of interviews ranged from 40 minutes, to two hours, with the average being 90 minutes in length. This line of inquiry was designed to develop contextualized, relational, and situated accounts of participants' everyday living in proprietary ecologies that could then be further analyzed in workshops and drawn on to inform my participatory research and design with the YDRC.

During each interview I practiced semantic note taking so that I could quickly distill and organize general themes and notable moments from the interview. This process of semantic note taking was, ironically, infused with proprietary media. A smartpen with a paper-based computing platform was used during interviews so that notes taken on my notebook would be temporally hyperlinked to the interview's audio recording, affording me the ability to begin coding the audio recording in real-time. These semantic notes were then imported to a more advanced audio annotation program that allowed me to expand upon my initial coding process, and begin to draw connections among interviews. At the beginning of each interview, this smartpen and its recording abilities were explained to the participant.

This process not only allowed me to review and refine prompts in between interviews, but also produce a rough summary and analysis for youth co-researchers to work with. While interviews were eventually transcribed in full and coded using both bottom-up and top-down coding structures, the rapid analysis of my semantic notes allowed me to move at a pace that kept research participants interested while also accounting for a variety of perspectives--a primary obstacle in participatory arrangements (cf. Mansbridge, 1973). Taking five months off to

transcribe and code interviews before assembling a research and design collective was not an option.

Assembling a Youth Design and Research Collective

11 of the 15 young people interviewed expressed interest in participating as youth co-researchers. Thanks to a small research grant I could afford to hire eight researchers, and thus only eight of those 11 were offered positions as youth co-researchers. In selecting these eight, I considered their age and level of interest, as well as the interests and concerns they discussed in their interview and how these factors would contribute to a dynamic and diverse grouping.

It was important that these be paid positions not only to compensate the YDRC for their participation but to also to value their expertise monetarily. This is not to argue that participants, and their participation, need to be paid to be valued in participatory research and design. But, in a project on proprietary ecologies, paying participants for their collective research and design afforded reflexive analysis. The YDRC could reflect on the ways their own human-environment interactions were being valued within the project and how this compared with other ways their interactions were or were not being valued in proprietary ecologies.

The Youth Co-Researcher position asked for an initial commitment of five hours a week, over a period of four to five weeks to produce an open source social network that further investigated the common concerns and interests voiced in the interviews. During this initial commitment, youth co-researchers were paid a stipend of $10 an hour that was distributed at the end of each workshop. Co-researchers could stop participating at any time without repercussion but would not receive a stipend for workshops occurring after their departure. These eight

participants were asked to participate in a two hour Project Orientation before committing to the position. To attend the orientation, participants 18 and older had to bring a signed consent form. Those younger than 18 had to bring a signed assent form along with a signed parental consent form.

Project Orientation

The project orientation was scheduled at the CUNY Graduate Center during a time when everyone agreed they could attend. Six of the invited participants attended the orientation. We discussed their personal motivations for attending and what each person hoped to achieve through their participation. My role as a facilitator and their role as youth co-researchers in a PADR project were discussed as was the IRB's role in evaluating and approving our research. I shared the IRB application that I had submitted before conducting the interviews to give them a sense of this evaluation and approval process. We concluded by reviewing interviewee concerns, and brainstorming ideas for how we might better understand and address such concerns with an open source social network. The reason for asking participants to come to an orientation was to give them a better sense of how the project would operate, to consider their role in it more fully, and to imagine how the project might progress before asking them to commit to anything. Upon leaving the orientation participants were asked to let me know in the following days if they wanted to be youth co-researchers in the MyDigitalFootprint.ORG Project.

The YDRC

Five of the participants from the orientation chose to continue on as youth co-researchers for the MyDigitalFootprint.ORG Project, with one declining citing a demanding extracurricular schedule. I wish to note that the 15 people interviewed for the project were considerably more diverse in terms of race than those that ultimately participated in the YDRC. Further, the two participants who were invited to the orientation but chose not to attend or participate further, and the one participant who attended the orientation but chose not to participate further in the project were all white. This left an entirely nonwhite group of young people that made up the YDRC. Two parents called me following the orientation to further discuss the youth co-researcher position before giving their consent. In both cases, the parent consented and their children participated in the YDRC. Together, the YDRC and I scheduled six "Research and Planning Workshops" at the CUNY Graduate Center so that we could begin our process of collaborative research and design.

Although developed at the end of our work together and initiated during our cogitation workshop, the following bios serve as appropriate and 'official' introductions to each youth co-researcher. These bios are public statements written by each youth co-researcher to describe themselves and to summarize their own motivations for participating in the project as well as what they personally gained from their participation. These are the members of the YDRC as described by themselves, with the age at which they began the project added next to their self-chosen names:

> MY NAME IS ASMAOU [16] and I am from Togo. I will be studying biology at SUNY New Paltz in the fall, and I love to listen to music. I wanted to participate in this research because it sounded interesting. It was research about youth and the internet. So, being a young person that uses the internet pretty much every day, I was so curious to know more

beyond just a computer and my invisible internet. I thought it was going to be interesting, and there was a lot to learn from this research. I learned about how the internet works, I also learned that whatever is being put in the internet is never fully deleted and some websites, such as Facebook, use our info to make money. *– Asmaou 7/9/11*

I AM KAITLIN [15], 16 years young and elated to be a part of this project. Like most, I enjoy socializing, in person and online. I have become so involved in the Internet over the years that sometimes I lose count of my interactions with it. As the Internet evolves, I find new reasons and sites that I convince myself that I need, whether it's a blog site for my poetry or a social networking site that allows me to be the Kaitlin few rarely see. The Internet, to me is attractive and addictive. Oftentimes, it seems as though I can't function properly without it. So when I was offered an opportunity to work with the Internet and possibly find an answer to why I'm so in love with it, I took the chance and ran away with it. *— Kaitlin 5/20/11*

HI, MY NAME IS ROSE [18]. I am from Haiti and I am graduating high school this year. I want to go to college to become a pediatric nurse. What I like to do on the Internet is go on Facebook, spend time chatting with my friends, shopping for clothes, communicating with others from other countries, and playing games. I also use the Internet to search for information that I need. What I don't like about the Internet is the pornography, the insults, and the advertisements that give your computer viruses when you click on them. I wanted to participate in this project because I wanted to learn more about what's behind the Internet. Also, I wanted to learn if my privacy was safe on the Internet. *– Rose 7/12/11*

I AM SAIF [17] and I was born in Bangladesh. I moved to the USA at the age of 11. Just like all other people who migrate, I had a tough time with adjusting to a new culture and living a new life. I've always been inspired by people around me to try new things, such as making film, music, and acting. I have worked on short films, and recently on a music album, which will be released in my home country and worldwide on iTunes in September 2011. I've always wanted to learn more about the Internet and its role on our daily life. When I was offered the opportunity to work with a group of students to explore the concept of Internet, I was really excited. After working on this research project I now know the Internet is the biggest part of my generation. *– Saif 8/10/11*

MY NAME IS YVONNE [19], I am a 12 grader at Brooklyn International High School. I love poetry and Jamaican reggae. My father is from Senegal, my mom is from Barbados, and I was born in the U.S. I lived in Senegal for 10 years and I also lived in Barbados, but now I just go on vacation there. The internet plays a big role in my life because I have friends in these countries that I can't see all the time, so the internet helps me communicate with them on Facebook, Gmail, etc. I also use the Internet to entertain myself. For example, I go on YouTube and look for Jamaican reggae because I love their music. I also like to play games on Facebook. I spend more time on the internet than I

> spend with my dad, therefore I decided to participate in this research so I can learn more about the internet and how to protect myself online. — *Yvonne 5/21/11*

As is evident from their own descriptions, the YDRC ranged in age from 15 to 19, consisted mostly of young women, immigrants or children of immigrants, and were all people of color. After months of recruiting, these were the five young people most interested and motivated to participate in the MyDigitalFootprint.ORG Project. I did not recruit a particular subsample of my original group of participants, but rather these were the young people who most eagerly wanted to continue participating in the project. Their motivations generally concerned wanting to know more about "how the internet works," and to learn something about their relationship with it. Their interests in media were diverse, ranging from listening to Jamaican reggae on YouTube to leveraging iTunes for the worldwide release of their music album.

It is important to note that these bios do not represent the full range of motivations, interests, and concerns that were articulated, developed, and explored in both interviews and workshops. Yet these bios are what the YDRC felt comfortable sharing about themselves publicly. As a research and design collective we agreed to attribute all actions and words collectively to the YDRC unless it was made explicitly clear that a participant wanted, or was comfortable with, specific words and actions associated individually to them by name. As I unpack and analyze the motivations, interests, and concerns expressed by interview participants and youth co-researchers, the participants identity will always be concealed unless approval was received from the participant.

Designing MyDigitalFootprint.ORG

Once the design and research collective was assembled, the MyDigitalFootprint.ORG Project moved into its second phase: collaboratively designing a social network that both further investigated and acted in response to the situated interests and concerns voiced in interviews and discussed in the orientation. The transition from interviewing young people to conducting research and design with youth co-researchers signaled not only a methodological shift in the project but also a bureaucratic restructuring. Having initially received approval from my university's IRB to involve young people as "research participants" in the project, it was necessary to file an amendment to my application that added each member of the YDRC as "research personnel" so they could officially conduct and analyze research with me.

This amendment process required that the YDRC be certified in "human subjects research" through the successful completion of seven online research and ethics modules offered by the Collaborative Institutional Training Initiative (CITI) Program.[41] I led 30 minute tutorials before each of the first three research and planning workshops. During each of these tutorials we would collectively read and discuss two modules before taking the online multiple-choice tests that followed each section. Certification required that each module be passed, but participants can retake the modules as many times as necessary. If someone got a question wrong, we would discuss why it was marked wrong so that the member would be better prepared the next time they took the exam on that module. The two members who had previously worked as youth co-

[41] Certification was facilitated by the Collaborative Institutional Training Initiative (CITI) Program. The modules covered can be found online at: http://www.citiprogram.org/citidocuments/forms/Human%20Subjects%20Research%20(HSR)%20Catalog.pdf

researchers on a PAR project had already received this certification.[42] This was critical as they were able to assist me in facilitating the teach-ins while also making clear to the other YDRC members that, yes, this was doable.

Like the stipends, this process afforded more opportunities for reflexive analysis. As researchers and producers, how might we redesign the relations that typically involve us as subjects and consumers? If this is the kind of oversight our academic research was to be subjected to, what sort of oversight is Facebook's research subjected to? In short, having to consider and reflect on our own research ethics provided opportunities and vocabularies for discussing research ethics in proprietary ecologies, shaping new multidimensional understandings of privacy, property and security.

Research and Planning Workshops

The six research and planning workshops took place at the CUNY Graduate Center, either in a small conference room with one computer and a projector, or a computer lab where each of us would have a computer organized in front of a projector. These workshops provided an opportunity to engage the YDRC in investigating and responding to their own situated interests and concerns as well as those that emerged from interviews. To critically investigate the proprietary ecology of human-environment interactions we also had to consider the ecology of the human-environment interactions within our own research. Luttrell (2012) emphasizes this reflexivity as a centerpiece of the qualitative research design and process that "makes visible the central role that research relationships play," arguing that "negotiating and representing research

[42] Since CITI Certification lasts for two years, both of these co-researchers were already had certificates that could be submitted to the IRB.

relationships -- what and how we learn with and about others and ourselves -- is the heart of the research journey" (p. 160). In proprietary information ecologies, human-environment interactions are research relationships, albeit not ones that are generally visible to participants. That our focus was on demystifying how our own behaviors and experiences were being documented, traced, tracked and privatized, meant visualizing and negotiating our own research relationships as they emerged as both a form of reflexive analysis and collective action. By reflexively analyzing and negotiating our own research relationships we were actively producing new relations that countered, paralleled, and reworked those produced through proprietary research. Making visible our own research relationships also helped us to identify the skills and literacies we would need to conduct our research and design plans.

The workshops began with tutorials on information architecture, internet governance, qualitative research, free and open source software, as well as a review of diversity and open access issues to enhance the YDRC's consciousness in information ecologies as well as provide the media and research literacies needed to develop an open source social network. The workshops also provided an orientation to the server and tutorials on both the front-end and back-end of the software we were using to set up our social network. Both WordPress Multisite and BuddyPress platforms were installed on our server and drawn on to build our social network. WordPress Multisite is a free and open source blogging platform that is capable of generating an unlimited number of networked blogs much how proprietary blogging services such as Blogger or WordPress.com operate.[43] BuddyPress is a free and open source platform that adds common

[43] Although WordPress.com is a proprietary blogging service, the WordPress platform itself is open source and freely available to the public to download and install on their own servers. This distinction is reflected in the "WordPress.com" location of their proprietary service and the "WordPress.org" location of their open source platform.

social networking features to WordPress, such as social profiles, forums, activity feeds, and groups.

Throughout this process we drew on Cahill's (2007) "collective praxis" approach, described in her research with the Fed Up Honeys as helping to methodologically establish "a set of rituals that facilitated deep participant involvement and collective ownership over the research process" (p. 304). This practice was important because ownership over the research process is ownership over the means of knowledge production, a primary matter of concern in proprietary ecologies. While the Fed Up Honeys practiced writing as one such ritual, the YDRC primarily practiced design as a ritual that facilitated collective ownership of our research medium, the social network. Designing the social network oriented our experiential continuum (Dewey, 1938) through a set of practices and rituals so that new experiences would draw from what was learned during past experiences.

When designing the profiles in our own social network we had to research how our own social profiles on networks like Facebook were designed. This allowed us to reflect on what questions social profiles ask and why, and how people fill them out and why. Ultimately we decided what questions we wanted to ask and why, and then collaboratively designed our profile accordingly. We could then begin to see how our questions generated 'data' on the back-end of our medium, thus prompting new discussions about, and research into, what Facebook might see on their back-end. This helped us develop shared vocabularies and experiences through the research and design process that facilitated our collaborative work while giving participants greater ownership of our medium. In this way, we followed a participatory design that was both cooperative and pragmatic in its approach to understanding our interactions with technology

(Greenbaum & Kyng, 1991; McCarthy & Wright, 2004). When we encountered a breakdown in our research or design, we focused on the factors contributing to the breakdown and addressed them through collective research before returning to the collaborative design process.

Interview Vlog

One of the main initiatives that developed from these workshops was the production of an Interview Vlog that allowed the YDRC to asynchronously interview various experts in-between workshops.[44] Members of the YDRC frequently lamented how their only formal education around the internet was organized around issues of cyberbullying and illegal file-sharing. So as we began to focus our concerns and identify our aims for producing a social network, we developed ten key questions that we wanted to ask people who had certain kinds of knowledge that we didn't have (Figure 3.2). I then recruited IP lawyers, social media marketers, IT workers, internet governance people, online game developers, academic technologists, digital activists, internet researchers, and

1. What is your job and how does it relate to the internet?
2. How did you "discover" the internet?
3. What role does the internet play in how we think and act?
4. How can the internet be used to promote acceptance and general well being?
5. Who buys and sells our online information, and why?
6. How can we balance what the internet does for us and what we do for the internet?
7. Who produces online content, and why do they do it?
8. How is it that data is never fully deleted on the internet?
9. How does your job change how you use the internet?
10. If you could ask us one question about the internet what would it be?

Figure 3.2 Interview Vlog Questions

[44] A vlog, or video blog, is an online video publishing platform.

online publishers who might inform our questions. Essentially, I drew on my own social network to recruit people with the kinds of knowledge these young people didn't have, and whom they would rarely come across in their environment.

Each youth co-researcher video-recorded two of these ten questions. Each video was embedded on a blog post of our private Interview Vlog. Using the same open source WordPress software we were using to build our social network, we configured a vlog for the YDRCs interview questions. Each video was less than 30 seconds long, and featured one YDRC member asking the research participant one question. Each of the 10 questions had a corresponding video so that the participant could be interviewed, asynchronously, by the YDRC. Each youth co-researcher asked two questions a piece. Our participants were then given accounts to the Interview Vlog and asked to log in and comment on each question. In the comment box under each video, the participant was able to leave a text-based response and/or upload their own video or audio response. Nine people participated, five of whom uploaded videos of themselves answering each question and four left a text-based response to each question. When participants responded to a video, their response was visible only to me and the YDRC. Participants were not able to see the responses left by other Interview Vlog participants. As the experts responded to our questions we would watch (or read) and collectively analyze them during our workshops. The initiative expanded the knowledge base of the YDRC while also giving us an opportunity to try out our research medium and methods.

Project Cogitation

A Project Cogitation was conducted, two months after our last research and planning workshop to give the YDRC a chance to reflect on and evaluate the collaborative research, group discussions, group analysis, and design process. This cogitation was also used to identify what, if any, aspect of our social network should be made available to the public. Together, we discussed what parts of the social network should be made public, and what methods we should use for contextualizing and anonymizing this public content. The cogitation followed a focus group structure where areas of agreement as well as disagreement on issues and statements were explored to analyze the frameworks of thinking underlying the opinions and experiences of the YDRC (cf. Glick, 1999).

Turkle's (2005) notion of an "evocative object" was drawn on in this cogitation to explicitly link ourselves and our own development with that of information ecologies and their development.[45] In building an open source social network that was approved by my university's IRB and that had to operate at each of Berners-Lee's (1999) four layers of the web (i.e., content, software, hardware, and transmission) provided us a series of openings for multidimensional understandings. Content evoked *an intimate dimension*, software evoked *a cultural dimension*, hardware evoked *a local dimension*, and transmission evoked *a translocal dimension*. Although everyday life and everyday media do not break down so neatly into four dimensions with four

[45] Turkle (2005) looked beyond the computer as an "analytical engine" to explore its "second nature" as an "evocative object." As an analytical engine, the computer is a rational and logical machine; yet, as an evocative object, the computer "fascinates, disturbs equanimity, and precipitates thought" (p. 19). My aim is to harness both of these aspects in an informational context by looking at cyberspace as an analytical engine to understand its role as an object that evokes certain understandings of privacy, property, and security in the everyday life of young people.

corresponding layers, this approach helped us see and communicate that there are indeed layers and dimensions to our mediated experiences. 'Dimensions' was intentionally drawn on as a term to evoke this partiality, as 'a dimension' always indicates one aspect of a broader picture. Thus, while software might be considered to primarily evoke a cultural dimension, this would be but one aspect of software alongside intimate, built, and translocal dimensions.

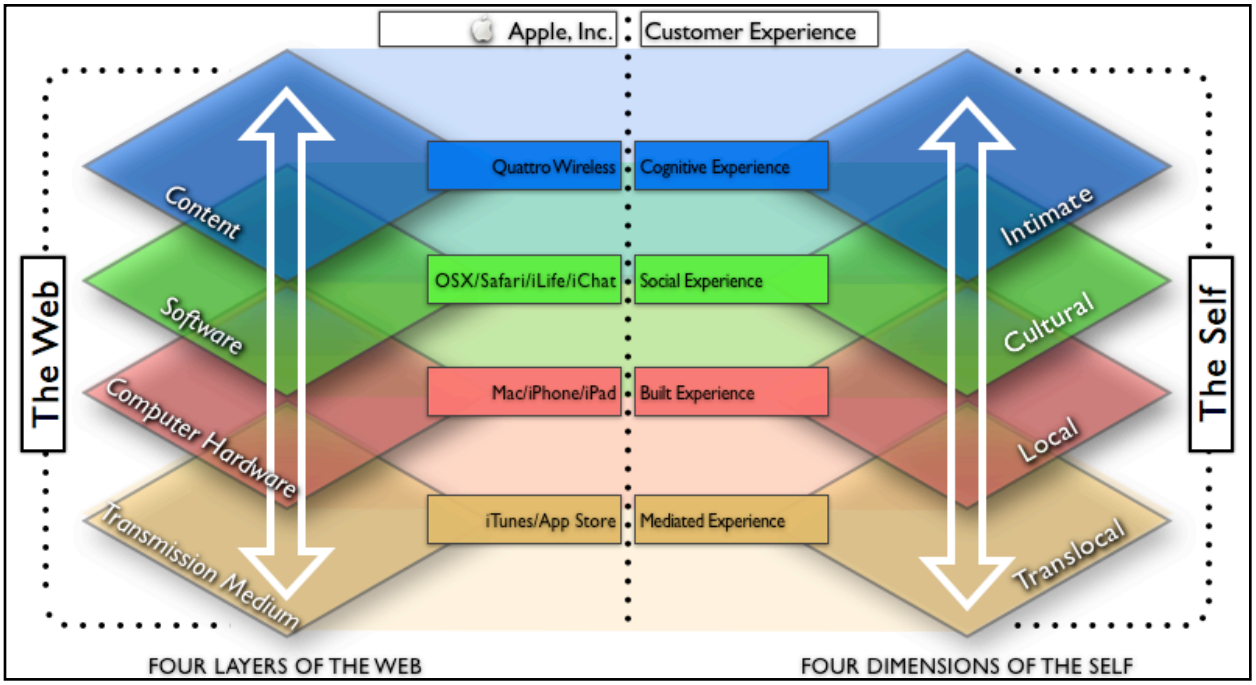

Figure 3.3 Four Dimensions of the Digital Self

Figure 3.3 was projected during our cogitation workshop to help focus this discussion. On the left are the four layers of the web, on the right are four dimensions of the self, while the middle column takes one corporation -- Apple, Inc. -- as an example to specifically consider how their content, software, hardware, and transmission products interact with their consumers experiences at various levels and dimensions. Talking about hardware, software, content, and transmission -- just like talking about intimacy, sociality, locality, and translocality -- were breakthrough moments in understanding proprietary ecologies and the YRDC's interactions with

and within them. The YDRC began to critically question their surroundings as they developed a terms of service for the social network, configured social profiles, instituted a participatory content flagging system, learned to distinguish between server-based software and desktop-based software, and made sense of a Secured Socket Layer (SSL) certificate for our server. Each of these practices created openings to discuss and capacities to analyze how such phenomena does and should operate in the proprietary ecologies of their everyday.

Conclusion

A participatory action design research (PADR) approach helps expose and express the relations and perspectives most neglected by the media and methods that characterize proprietary ecologies. Through their involvement in the MyDigitalFootprint.ORG Project the YDRC transitioned from social research subjects and social network consumers, to social research participants and social network producers. This transition process prompted breakdowns that unsettled previous understandings of privacy, property, and security, and ultimately led to breakthroughs when we were able to design our own social network to address new, more critical, understandings.

Interviewees and the YDRC had broad experience using ICTs to search for, organize, compose and publish, as well as share and discuss various media. Practices such as these were drawn on in my work with the YDRC as a basis from which to develop the literacies and capacities necessary to design and govern an information ecology. In learning how to be productive with information, the YDRC began to develop skills and insights for reorienting information ecologies towards their own situated interests and concerns.

Taking the medium as both our message and method, we organized our work around the production of an open source social network. This helped to demystify our human-environment interactions in proprietary ecologies by producing new ones in a more open ecology. As Cahill (2007) argues "engaging young people in research helps challenge social exclusion, democratize the research process, and build the capacity of young people to analyze and transform their own lives and communities" (p. 298). In the following chapter, I unpack how the participatory research and design process behind the MyDigitalFootprint.ORG social network engaged the YDRC in analyzing and transforming their informational surroundings.

Chapter Four
Learning to be Informational

At the empirical core of my project was my collaborative work with the Youth Design and Research Collective (YDRC), who were asked to reflect critically on their daily experiences as users of social media to design our social network. Their experiences emailing, texting, posting, commenting, 'liking,' browsing, searching, and sharing while configuring their identities guided the design of the MyDigitalFootprint.ORG social network. In this chapter I draw from this experience-oriented design process to discuss how broader modes of informational development were reproduced, reworked, and/or resisted by youth co-researchers. I will continue to draw on my interviews with young people to situate and aerate my analysis as well as to discuss how similar interests and concerns were taken up and negotiated by the YDRC during our six Research and Planning Workshops.[46]

The youth co-researchers' formal school-based education around media was predominately framed in terms of how they should not steal music or internet connections, how they should not access certain sites on school computers or at home, and most importantly how someone is always watching and waiting to catch them if they did something wrong online. This comported with references to "the government," "the police," "a librarian," "mom," "some evil genius," "a predator" and other actors routinely named by interviewees as potential spies monitoring their

---

[46] As discussed in Chapter 3, all youth co-researchers consented to the audio recording of these workshops but collectively decided that any direct quotes used in this analysis were to be attributed simply to 'member(s) of the YDRC,' 'youth co-researcher(s),' or just 'the YDRC.' Asmaou, Kaitlin, Rose, Saif, and Yvonne all felt comfortable publicly identifying themselves as members of the YDRC but they did not want to have to have individual quotes or actions attributed specifically to their name.

mediated engagements. As these statements suggest, formal education is focused largely on protecting and policing youthful engagements with media, typically motivated by parents' and teachers' sincere concern for a child or student's safety. Yet, it provides little in the way of media skills or literacies from which to negotiate a social network in an informed way, let alone design one.

None of the co-researchers had received formal education regarding media production, information architecture, information ethics, internet governance, or other areas of knowledge that would foster greater consciousness and more critical participation in information ecologies. Many of the youth co-researchers explicitly cited an interest to 'know how the internet worked' or to 'learn how to make a social network' as their motivation for participating in the MyDigitalFootprint.ORG Project. As one stated "I always wanted to work with the internet but not, like, entertainment stuff." In most cases, they specifically mentioned how unhelpful they've found their formal education to be in addressing these interests. As Monahan (2006) has argued, such education plays into a broader neoliberal curriculum that frames young people as either "victims or criminals" who must learn to be "protected or controlled." This binary occludes any sense of young people as actors who could be engaged in debates that define what security means and how best to ensure it within one's life space. In this context, desires to either protect or control young people's mediated engagements works against empowering them, and cultivates a public that is both dependent on governments and corporations to filter their information and that must be subjected to consistent policing. Under both conditions, an ontological fear and insecurity is socially reproduced, surveillance is normalized, and political disengagement is promoted.

In contrast to their formal education, the YDRC found value in the informal ways their daily interactions with and within social networks and other social media educated them about information environments. I use 'informal' here to distinguish this mode of education from more formalized school-based modes of education. In this sense, informal education still accounts for the quite formal ways proprietary media, such as Google or Facebook, encourage particular modes of searching and tagging; even if one chooses to reject or rework such encouragement. Further, while this education is rarely part of the structured curriculum most young people experience in school, it is still often entailed in the conducting of homework that was frequently discussed by interviewees and the YDRC as an online activity, and in the occasional request of a teacher to use Google to find information or to setup an email account with Gmail or Yahoo! to submit assignments.

Interviewees as well as the YDRC felt more experienced than their parents or teachers in the affective and fulfilling qualities of social networks as well as the unpleasant and unwanted ones. Youth co-researchers had fun browsing photos of themselves, friends, and even strangers on Facebook. They also expressed concern that someone "creepy" could be looking at their photos or the photos of friends and family members. Concerns were also raised that they could lose control of their online representations by losing control of what photos of themselves get posted where and when. Co-researchers often instructed each other that the present posting of a photo of oneself to Facebook or other social media could come back to haunt them later in life if found by a college or employer.

Although these concerns were felt and often noted, some YDRC members would still take photos of themselves or others during workshops and upload them to Facebook in the blink

of an eye. Even the co-researchers who often lectured others about uploading certain photos would themselves participate in this practice. The youth co-researchers were experienced in the nuanced and often contradictory emotions and practices that come with participating in proprietary social networks. They understood wanting interpersonal engagement and social exposure while simultaneously wanting personal privacy and tight control over their mediated representations. This contradictory life in proprietary ecologies undergirded the informal learning of co-researchers and provided them with a common experience that they felt was not shared with adults. It was frequently noted that parents, teachers, aunts, grandparents, or other adults seemed to lack a common sense that they and their peers shared. This is not to suggest that these adults were internet idiots, but that interviewees and youth co-researchers alike often felt adults were less experienced with the internet and thus more naive than they were.

Many of the interviewees described themselves as more capable of negotiating their privacy, property, and security than their teachers and especially their parents. Disclosures of managing a parent's engagements with the internet to ensure a certain degree of personal privacy were most common, as in this example from 14-year-old Orlando:

> Well, like my mom is kind of annoying how she like— like she's a great person, but how sometimes when she gets on Facebook, she'll just start clicking. So, if she sees anything that I've been tagged in, she'll click on it and she'll go through the whole album.

Not wanting his mother to see every photo of him that gets posted to Facebook, but also not wanting to hurt his mother's feelings by "defriending" her, Orlando configured his mother's Facebook privacy settings to enhance his own privacy:

> So, what I did was I went on her—when she went to the bathroom and she was on Facebook and I went on there and I went into my profile and I said 'hide all posts.' So, I don't think she can see it, but I asked her 'would you be mad if I defriended you' and she'd be like 'yeah!' But it's so obvious if you block someone, it's even just like defriending them.

In changing his mother's privacy settings to "hide all posts" from his personal account, Orlando remains his mother's 'friend' but she can no longer see the photos, comments, and status updates associated with his account. In configuring his mother's account to filter out his account, Orlando achieves a similar result to defriending his mother, except that they technically remain friends and his mother fails to notice the obvious absence of her son's content in her news feed.

Alternatively, 15-year-old Megan was concerned that her mother's online shopping and bill paying practices could result in the theft of her mother's identity:

> I think I'm really concerned about, like, for my mother. Since she uses -- like she uses online to pay her bills and things. So I would say her identity, like, because often I realize that, when I go -- I order on Forever 21 and I was about to enter her credit card number that, you know, how sometimes it's saved already, like it's in the box under it. And so -- but that I wasn't her, that wasn't the card I was about to use, and I was like 'it shouldn't have been saved.' That was something I figured shouldn't have been saved. Things like that.

After beginning to enter her mother's personal information when buying clothes online, Megan's web browser began to automatically fill-in the information for another one of her mother's credit cards. This 'auto-fill' feature is common among most web browsers and, in this case, the web browser had stored the credit card information that Megan's mother had previously entered when buying something or paying a bill online. Whether the browser's storage of this financial information was intended or unintended by her mother, Megan found this very concerning and

decided to show her mother how to prevent the web browser from saving such information in the future to protect her mother's privacy and financial security.

This is not to say that interviewees or the YDRC felt totally in control within proprietary ecologies. Despite feeling they knew more than others, they also frequently alluded to what they perceived as their own failures by relying too much on "the internet," "Facebook," "Google," or "texting." They expressed guilt for getting too wrapped up in online gossip, stalking, and socializing. This sense of personal failure and guilt was rooted in a belief that they could be doing more productive things on or offline. As described in Chapter 1, the internet was seen by interviewees as a relatively unknown and highly addictive assemblage. The expressed guilt around this felt ignorance and addiction was a tacit awareness that this assemblage was produced and that by understanding its production one could better control their own privacy, property, and security -- or those of others, such as parents. I hasten to add that aspects of this guilt are indeed socially encouraged through the ways Facebook, Google, and other proprietary services overwhelm users with many complicated but weak privacy settings that become easier to avoid, and feel bad about, than actually configure. In this sense, young people are guilted into accepting responsibility for not knowing how to overcome obstacles that are precisely designed to make them not control their privacy. Even as this guilt is encouraged and misplaced, it remains a desire to know more and do better than one currently feels to be the case. In this sense, the guilt expressed by interviewees and youth co-researchers was somewhat aspirational; if they didn't care to know more or feel more in control, then a sense of apathy and not guilt would have been expressed. Despite popular stereotypes of 'apathetic youth,' the young people I talked and worked with through the MyDigitalFootprint.ORG Project were interested and concerned.

In workshops the YDRC regularly alluded to the notion that the internet was not a natural phenomena and thus did not have to be taken as is. In citing "a man" that made the internet, "that guy" who started Facebook, or "a terminal somewhere" that all internet-based communication goes through, the YDRC was often short on vocabulary and vague in their concepts, yet this still conveyed a sense that people, places, and things were involved in the internet's production and maintenance. Co-researchers were not sure how the internet worked, but their experiences indicated there was indeed work involved. More empowering relationships with and within even proprietary ecologies were possible through more critical participation in them, and even this limited consciousness of informational production provided us a framework for such engagement.

Like other young people, the YDRC were informally learning to use search engines to find media; to collaboratively develop coding schemes for organizing media through tagging, ranking, and categorizing practices; to compose and publish their own content on multiple platforms; and to share and discuss various content asynchronously and in real-time. Learned practices such as these were drawn on in my work with the YDRC as a basis from which to develop the skills and literacies necessary to design and govern our social network. In learning how to be productive with information, the YDRC began to develop skills and insights for reorienting informational production towards their own situated interests and concerns.

In this chapter I draw from my work with the YDRC to unpack what I call 'cyberdominance' as a primary mode of informational development and to consider the ways this mode was reproduced, reworked, and/or resisted by the YDRC. I discuss cyberdominance as a boundary-making process whereby access to, and circulation within, proprietary ecologies is

controlled through the production and policing of personal, commercial, and national borders. Cyberdominance does not account for all of informational development, nor is it a discrete phenomenon. It operates at multiple scales and in various contexts to involve governments, corporations, civil institutions, families, and individuals across an uneven historical geography. Cyberdominance came into focus through my work with the YDRC and thus warrants further articulation and analysis here to consider some of the ways informational capitalism plays out in young people's everyday environments.

Informational Youth

At some point in every workshop I would project Figure 4.1 on the wall of our meeting space. This Venn diagram of what I call 'Informational Youth' was meant to help us consider the ways young people's practices shaped and were shaped by cultural expectations for youth. For example, considering how parents, teachers, and others expected them to be a certain kind of student helped us reflect on how their learning practices were negotiated vis-à-vis such expectations. How did cultural expectations for young users, producers, and students matchup with or misrepresent their own routine practices of consumption, production, and education? How did they negotiate these situated experiences in relation to cultural expectations and how did such negotiations shape understandings of privacy, property, and security in different contexts? These questions were important to our research and design as they got at the crux of broader negotiations over social norms and practices in relation to informational development. What a society perceives to be a matter of privacy, property, or security in certain contexts, has significant bearing on what is permissible with governance and commerce in each context.

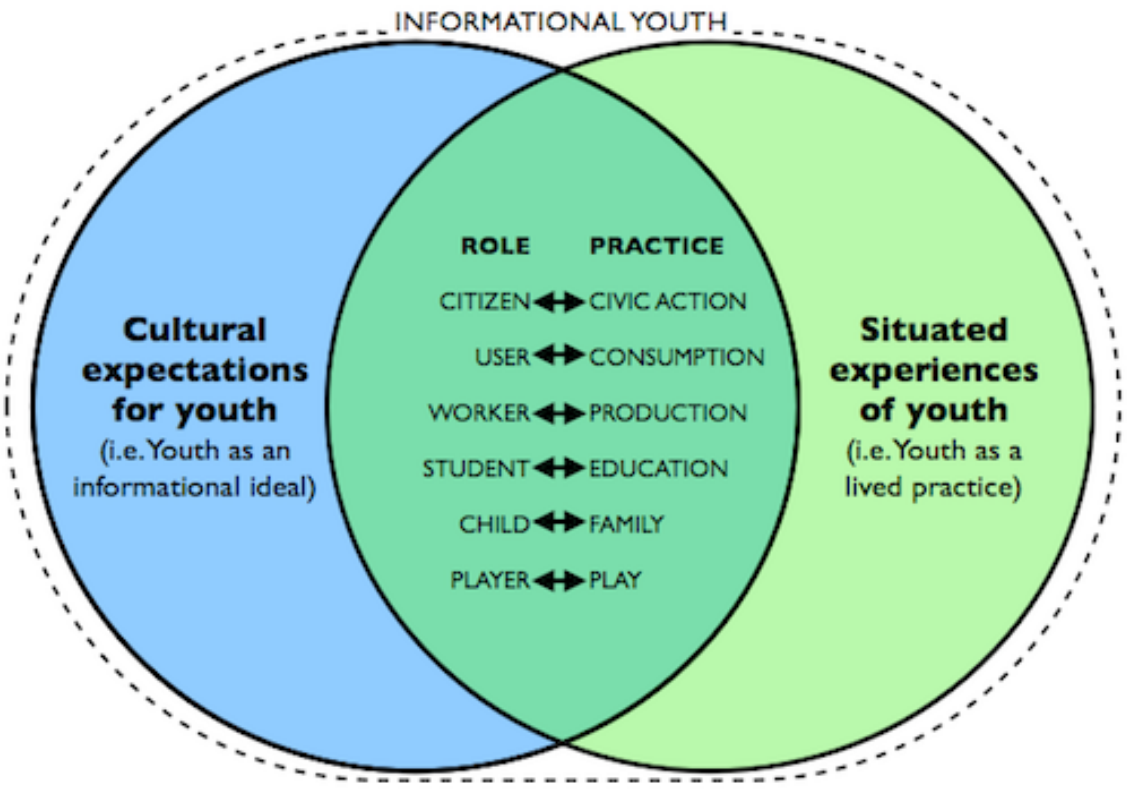

Figure 4.1 Youth as Informational Ideal and Practice

Federal legislation such as the Digital Millennium Copyright Act (DMCA) and corporate lobbying groups such as the Recording Industry Association of America (RIAA) and Motion Picture Association of America (MPAA) consider even small-scale file sharing to be piracy; that is, unauthorized access to or use of private property.[47] In this context a social practice that youth are often encouraged to do in school and most families -- sharing among friends -- is considered a criminal act of piracy that compromises the security of the entertainment industry's intellectual property and thus warrants various forms of private and state-backed policing. That people who are unlikely to participate in file sharing also consider it morally unacceptable while those who find it morally acceptable are likely to file share (LaRose et al., 2005), indicates that wether one

[47] The Digital Millennium Copyright Act (DMCA), passed in 1998, is a U.S. copyright law that largely focuses on digital rights management (DRM) to both criminalize copyright infringement as well as the. Year??circumvention of copyright controls.

considers this practice ‘sharing’ or ‘piracy’ has significant influence over their practice. However, if 46% of all adults in the US, including 70% of those adults 18-29 years old, indicate they have ‘shared’ music, TV shows, or movies (Karaganis, 2011), it suggests that common social practices and norms indicate such policing and its associated justifications have little efficacy in the lived experiences of everyday people. It also indicates that practices such as file sharing extend well beyond the habits of youth, and are as common a social practice as jaywalking.

What this policing does do is encourage an ethos of criminality around a common social practice a broad and diverse public continues to engage in. The issuing of cease and desist orders as a result of the DMCA, the local blocking of file sharing sites by professional and educational institutions, the state-enforced taking down of file sharing sites like the original Napster and Pirate Bay, the monitoring and throttling of a user’s bandwidth by an ISP to minimize one’s ability to file share, and the significant media attention all of this receives clearly communicates a sense that such practices are not condoned by authorities.[48] The recent suicide of Aaron Shwartz after months of bullying by federal agencies for downloading and releasing millions of

[48] The monitoring and throttling of a user’s bandwidth typically occurs when an ISP customer is downloading and/or uploading above-average amounts of data through their technically ‘unlimited’ internet connection. In such cases an ISP might restrict how much bandwidth the user can use, thus slowing down considerably the time it takes to upload and download content.

academic articles, and the media attention this has received, further communicates to the public the consequences of such practices.[49]

Although all of the young people I spoke with were at least somewhat aware of the potential legal and financial consequences that could result from file sharing media considered 'pirated' by authorities, most felt this was highly unlikely to happen to them and were far more concerned about getting a computer virus from file sharing than getting sued or arrested. Thus, while prompting little in terms of concern for the private property of entertainment industries, the ethos of criminality these industries foster around file sharing does provoke personal security concerns. In the case of 19-year-old Elena her concern for getting a computer virus from downloading music through file sharing sites like Kickass, Torrent, and Pirate Bay led her to participate in a private file sharing collective:

> And those are really cool because even though you have to maintain a ratio, like it's really nice because you have to give back to get actually more music. And all the files you're going to download are not virus. They don't have viruses. Like, they're clean files.

In that viruses were Elena's primary concern in file sharing, her solution was to find a smaller more equitable environment that allowed her to download "clean files." Real or imagined, the participation in this environment that required Elena to give as much as she received was equated

---

[49] Aaron Shwartz was an internet activist who assisted in both the development of the RSS web feed format and the social news site Reddit as well as lead successful citizen opposition to the recently proposed anti-piracy laws that would have further extended the DMCA. Prior to his suicide he had been under investigation by federal authorities for hacking and fraud charges as a result of his downloading millions of articles from the JSTOR database and making them publicly available. These articles were already freely available to faculty and students at universities and shortly after this incidence JSTOR made most of these articles freely available to the public. Despite JSTOR choosing not to press charges, federal authorities brought 13 felony charges against Shwartz with the potential of serving up to 50 years in prison.

with a greater degree of security. The clear terms of participation and communal atmosphere made it more knowable to Elena and thus more secure. This information ecology stands in stark contrast with the proprietary ecology of iTunes and the kinds of security it aims to ensure.

With iTunes, Apple was able to convince a recording industry that had just successfully shutdown Napster that it could provide a lucrative mode of content distribution. iTunes offered a proprietary ecosystem of integrated hardware, software, and encrypted data flows that would allow these companies to sell digital reproductions of their content without them then being easily redistributed for free on other platforms. Content could freely circulate from iTunes to the iMac and to the iPod without ever leaving Apple's borders. Buying music on a Compact Disc (CD) or vinyl record makes it the consumer's property, who is then legally entitled to make as many digital reproductions of the album on as many devices as they wish as long as those copies are for personal and non-commercial use. The CD or vinyl records themselves can also be lent or given to a friend or even resold by their owner, as is commonly done on eBay or at used record stores. In contrast, buying an album from iTunes, in most cases, entitles the consumer only to reproduce that content on up to five devices. These restrictions are enforced through digital rights management (DRM) layers that encrypt content sold on iTunes.[50] At no point can these albums be resold by the consumer. Unlike Elena's file sharing site, iTunes helps Apple and the entertainment industry accumulate more capital by controlling when, where, and how content --

[50] As of 2009, iTunes began selling music files without DRM encryption layers at the same time that they began moving to a tiered pricing system. Previously, all song files were 99 cents but most came with DRM restrictions. This can be seen as a shift away from encryption in environments where greater surveillance is possible. Now that Apple, and by extension record companies, can assess what music a user has stored in their local or cloud-based iTunes Library, and wether they purchased this content or not, there is less desire to encrypt these files before distribution.

and reproductions of content -- is accessed and circulated well after its initial consumption.

This extends to content well beyond music and proprietary platforms other than iTunes, as some consumers of Amazon's Kindle learned when they suddenly and ironically found their bought copies of George Orwell's *1984* deleted remotely from their Kindle. A copyright dispute with the publisher of Orwell's content prompted Amazon to remove the author's ebooks from their online store, remotely delete all local copies that had been sold in the US, and credit consumers' accounts for their past purchase. The market value of companies like Apple and Amazon rests partly in their ability to control how intellectual properties circulate or don't in information ecologies long after their initial acquisition. In iTunes, we can see an information ecology enclosed for purposes of capital accumulation by dispossession. In constituting proprietary ecologies, corporations like Apple and Amazon generate profits through the enclosure and controlled access to resources previously considered public or common. While the products themselves were always private and not a public resource, what meaning could be made personally and collectively from these products is at the center of this enclosure. Few would consider the singing of "Happy Birthday to You" to be the ground of an intellectual property dispute. Yet, that is exactly where a German kindergarten found themselves when they were notified that they must pay a fee to Germany's music licensing agency, GEMA, if they wished to print the words to the copyrighted "Happy Birthday to You" for their students to sing. What being enclosed are the social relations and spaces that revolve around commodities, bring them too into the fold of corporate profit and government control. In considering the private file sharing site Elena participates in, we see a different ecology enclosed for purposes of sharing and

personal security. For Elena, it's clear that participation in the former is socially accepted and expected of her while participation in the latter takes on a pejorative social connotation even while it fulfills a personal desire for secured file sharing. We also see an attempt to shield the social relations around these files -- the sharing -- from commodification and policing.

This sort of negotiation between expectations for youth and the actual experiences of youth can also be found in the online surveillance and censorship practices of many educational institutions. The YDRC frequently discussed experiences with their schools blocking access to Facebook, Google Chat, AOL Instant Messenger, ESPN, and other "non-educational" or "fun" media from school computers. That school filters were discussed as easy to circumvent on school computers with proxy sites such as HideMyAss.com, or simply with a smartphone to access the internet while at school, indicates they do little to curb access to such media for young people intent on accessing them. What was communicated by these filters, and expressed by members of the YDRC, was a felt presence of institutional surveillance and censorship that framed certain media as unproductive in and irrelevant to their formal education. When circumventing filters to access sites such as Facebook or ESPN, one did so as a rebel much as one file shares as a pirate.

The pejorative framing of certain places and practices within young people's life space as criminal, non-educational, or unproductive obfuscates their empowering, educational, and productive potential. Such framing also hinders the ways young people distribute personal knowledge through a network of social contacts that are usually accessible. Blocking social media such as Facebook, AOL Instant Messenger, or Google Chat on school computers causes friction in this distribution of knowledge. It hinders a student from accessing the classmate who can help them with a math problem, or the aunt whose grammatical expertise can assist with a

writing assignment, or the friend who can calm them down when they're flustered and unable to concentrate. Young people increasingly distribute and collectively produce knowledge through information ecologies in these ways. Indeed, drawing on one's surroundings to access certain kinds of knowledge is increasingly how most people young and old now produce knowledge in advanced capitalist nations. Such skills are essential to develop in an increasingly crowded and omnipresent information environment where being able to navigate, evaluate, and make sense of a vast array of content may be more practical than memorizing or 'storing' it all internally.

Before there were computers with object-oriented interfaces and distributed cloud networks, individuals were embedding information in the people, places, and things that surrounded them. Then too, these objects were often subjects of various investments and control. One can look to the ways the Roman Catholic Church tried to prevent the popularization of the printing press in the 1500s for fear their social influence would diminish if the public no longer depended on them as an access point to the word of god (Postman, 1992). Further, what books were printed, who could afford to buy them, and who was capable of reading them all regulated who could access the knowledge stored in these objects. Now that the cost of publishing books, particularly ebooks, is minimal and literacy levels are high the accessing and use of books become a new domain for capital accumulation and control. Having spent my high school years working in a record store, interacting with my record collection still connects me with memories and feelings from that past. When I play PJ Harvey's *Is this Desire?* on my record player and hold the record sleeve in my hands I can access information from my junior year of high school that I'd otherwise find difficult to recall. My engagements with this object are more personally valuable than the $19.99 I paid to own it. If, I had bought this commodity in a proprietary digital

format through iTunes or Amazon, my access to it could potentially be revoked or renegotiated like Amazon did with Orwell's *1984*. I own my copy of *Is this Desire?,* but in this later case I would be leasing access to it and thus tying my cognition to its proprietor's inevitable desire for greater profit.

That routine forms of personal and collective knowledge are increasingly privatized and oriented toward capital accumulation through the enclosure of information ecologies is problematic, and presented here as a form of dispossession. I also wish to emphasize that even the marginalizing or divorcing of such problematic proprietary productions of knowledge from formal education does little to empower young people. More critical participation in such knowledge production, not less, is necessary to reorient this accumulation and resist such dispossession. If people only use Facebook in ways they are socially expected to, for example, then they will never imagine or realize alternative applications for such media nor will they come to see their playful use of such media as something worth building upon rather than suppressing it as 'unproductive' behavior. It is here most notably where we see the consequences of divorcing play from work in formal education. Play, as a creative and often demystifying practice, should be critically considered and meaningfully valued in processes of knowledge production (Katz, 2004).

I thus worked with the YDRC to focus on the practices they found playful and/or productive regarding their own informal education and evolving identity configurations. In designing the MyDigitalFootprint.ORG social network we engaged the boundaries and boundary-makings between cultural expectations for youth and the situated experiences of youth. This entailed working with the YDRC to explore how the proprietary orientation of their

everyday environments might be reconsidered in an open source social network. To this end, we built our social network using the publishing platform WordPress because of its open source code. If we desired, and if we had the skills, there was little about this platform's design or operation that we couldn't manipulate. None of WordPress' source code was enclosed by a restrictive Terms of Service or copyright.

This meant we could configure the look and feel of a social profile or registration process in ways that would be impossible using proprietary networks like Facebook. Figure 4.2 shows how, from the backend of our social network's interface, we could easily generate social profile fields that asked our own questions and allowed the YDRC to designate how a participant could or could not fill in these fields. When Facebook only allows users to indicate their "sex" as male or female from a drop down menu, they do so to box people in predefined marketing

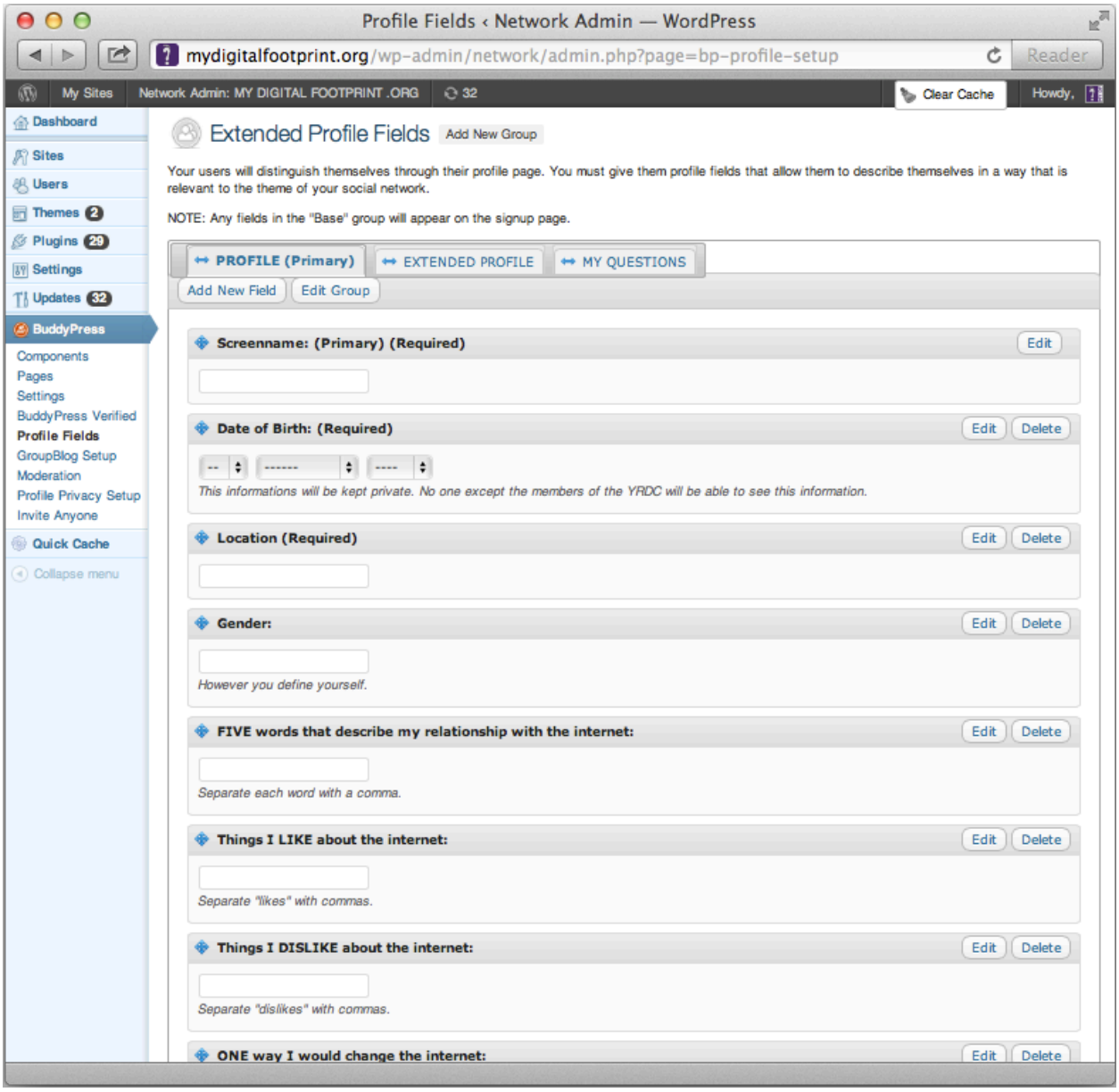

Figure 4.2 Backend View of Social Profile Fields

demographics. This leaves users with only three options: designate your sex as male, female, or leave this field empty. As the YDRC was more interested in knowing how our participants choose to identify their gender, if at all, we decided to make an optional profile field called "Gender" that allowed participants to fill in whatever answer they felt most appropriate and then indicate wether this profile field should be visible to other participants or kept private so that only myself and YDRC could see it.

Practices that the YDRC felt constituted matters of privacy, property, and security were explored in more depth. This was often began with a passing reference to a practice such as deleting emails, alongside an articulated concern such as 'when I delete an email from my Gmail account, Google should delete it from their computer.' I would then work between workshops to compile a range of educational multimedia so as to present a more structured consideration of the matter at the following workshop to foster a more informed discussion that reconsidered the matter in relation to our own social network by asking questions such as 'should we be deleting a social profile from our server if a participant wants it deleted?' In this way we addressed issues such as bullying, peer monitoring, file sharing, identity theft, representation in social media, online surveillance, e-commerce, and media activism. Although interactions that constituted such matters were influenced by cultural expectations, we sought to consider them through our own practices as social network users and now producers.

When the YDRC voiced their displeasure with the way Facebook frequently asked them to submit to a Terms of Service policy that they felt was too long to read and too complicated to understand, we asked ourselves 'how should we do this in our social network?' My university's Institutional Review Board (IRB) required that all participants in our social network agree to an online consent form that briefly explained their rights as participants and the personal data that would be collected on them in easy to understand language. Rather than having a Terms of Service policy, we thus decided to create a Terms of Participation policy that would articulate a short and concise governance policy that satisfied our own ethical concerns as well as those of the IRB. Through this process the YDRC members found themselves asking 'why can't Facebook do it like this?' It wasn't that creating these terms turned out to be easy, it's that it

turned out to be doable. Through design, the YDRC came to see governance policies as complex processes carried out by actual people rather than naturally occurring phenomena that must be accepted and submitted to as is.

Rather than discussing cyberbullying with a social casting of victims and criminals, we had to consider the ways interface design and medium governance do or could shape this social practice. In one workshop we juxtaposed a public statement from Facebook's Marketing Director calling for all individuals to be identified online to keep kids safe from bullying, alongside an email from the IRB asking that participants under 18 years of age be allowed to join our social network anonymously to protect their privacy and safety.[51] These statements stood in total contradiction, with the former emphasizing security through less privacy and the latter emphasizing security through more privacy. As we unpacked this contradiction, property emerged as the key distinction between the two approaches. Is personal information the participant's property to disclose and control access to within a social network, or is it the social network's -- and thus its proprietors' -- property? What changes when a social network conducts for-profit social research as opposed to academic social research, and whose property—and privacy--is being protected in each instance? In negotiating such matters while configuring our

[51] Although the comments of Randi Zuckerberg, Facebook's Marketing Director, were widely reported, the YDRC and I read the *Daily Mail*'s reporting of the comments during a roundtable on cyberbullying hosted by *Marie Claire* magazine. This article also compared Zuckerberg's statement to similar ones made by Google CEO Eric Schmidt. According to the article, Zuckerberg stated, "I think anonymity on the Internet has to go away. People behave a lot better when they have their real names down. … I think people hide behind anonymity and they feel like they can say whatever they want behind closed doors." This article was accessed on 26 February 2011 from http://www.dailymail.co.uk/news/article-2019544/Facebook-director-Randi-Zuckerberg-calls-end-internet-anonymity.html#ixzz2HCxSvfTa

social network and constructing its privacy policy, the YDRC broke out of the stifling victim/ criminal binary.

These negotiations entailed the boundaries and boundary-makings of informationalism in relation to participants' own life space. What does it mean to be the user and the producer, the watched and the watcher, the one who submits to a privacy policy and the one who creates a privacy policy? Technically, these were practical questions to consider when designing our social network. We needed to configure social profile fields, establish privacy and governance policies, set up a registration process, and decide who could have access to the various data generated and in what context. These were technical issues the YDRC encountered for the first time in constructing our social network, but they provoked complex emotional, ethical, and political discussions. Their individual and collective negotiations of these matters were also explored as part of constructing broader identity configurations. Psychosocially, sorting out how our social network would be configured and operated through a collective design process was linked to how the YDRC wanted to configure themselves and operate in information ecologies.

Cyberdominance

To understand cyberdominance it is necessary to revive and unpack a term that was never mentioned by the young people I interviewed yet remains central to informational development: *cyberspace*. When I first asked the YDRC what they thought of the word cyberspace they appeared a little confused and explained that while they were familiar with the word, they felt terms like 'online' or 'the internet' were more common and useful for explaining their mediated interactions. One member declared that it was a "sci-fi geek thing." The others concurred and the

consensus was that cyberspace was a word young people never used. *Wired* magazine has put it more bluntly:

> No body uses the word ‘cyber’ anymore, except people trying to scare you and trying to make the internet seem scary or foreign (Singel, 2010).

These insights suggest a reconsideration of cyber terminology. The cyber prefix after all finds its origin in cybernetics; a science organized around remotely controlling technology and humans from a distance. George (1965) traces the development of cybernetics to Norbert Weiner's antiaircraft warfare research conducted during WWII, when Weiner and his associates "noticed various resemblances both in the behavioral characteristics, and sometimes in the structural characteristics, between computer-type systems and the human being" (p. 4). Cybernetics, with its interest in merging digital and biological systems for the sake of communication and control, lies at the center of a dialectical tension emerging from cyberdominance.

Whose communication and whose control dominates and is dominated in various contexts shapes what action is and isn’t possible by various actors. My revival of cyberspace is not to scare, or to reinforce an antiquated dualism between ‘cyberspace and meatspace,’ rather I take up cyberspace to draw attention to the ways individuals, governments, and corporations construct cyberdomains as geopolitical territories that then become the subject of control. This mode plays out at various scales beyond the nation state in local cybersecurity legislation and policies, cybersafety media campaigns, and home computer filters like Cyber Patrol and Cyber Sitter. Whether or not people use the term cyberspace in local vernacular, its use by governments and corporations at all scales gives it presence in the life space. As Chapter 2 discussed, cyberspace remains an important spatial metaphor in legal justifications for applying existing regimes of

property ownership to the constitution of proprietary ecologies. I here consider how cyberspace also functions as a spatial ontology for national, corporate, and even intimate practices that reinforce informational capitalism.

It is understandable that the YDRC thought of cyberspace as a "sci-fi geek thing." William Gibson (1984) popularized cyberspace through his classic science fiction novel *Neuromancer* as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation ... a graphic representation of data abstracted from the banks of every computer in the human system" (p.51). A less poetic and more technically defined cyberspace can be found in the US Department of Defense's *Dictionary of Military and Associated Terms*:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[52]

In Gibson's depiction, cyberspace is more than a technical assemblage of information communication technologies, it is a daily human experience shared with others through social and material practice. In the Department of Defense's depiction, cyberspace is a way of demarcating the production of this shared experience through its physical infrastructures, networks, systems, processors, and controllers. All of which must physically exist somewhere in a global geography of nation-states. In organizing a cyberspace according to this historical geography, existing modes of geopolitical dominance have continued relevance. Since

---

[52] Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms", dated 8 November 2010 and amended through 15 November 2012, and accessed on 23 November 2012 at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

cyberspace is a collective expression of material social practices, these practices too are brought under geopolitical consideration.

When WikiLeaks decided to publish US State Department diplomatic cables on its website in 2010, the physical location of the servers hosting its website became of primary interest to the US government. Hosted at the time by US-based Amazon Web Services (AWS), WikiLeaks was forced to move to Banhof AB servers in Sweden after US Senators lobbied AWS to shut down the site. That WikiLeaks sought international refuge on Banhof AB servers that were located in a former WWII bunker built into the White Mountains of Sweden, provides a quite literal metaphor for the ways an industrial geopolitics continues to play out informationally.[53]

Cyberdominance, at a global scale, ensures that the consensual hallucination Gibson speaks of is not experienced by people in *every* nation; as the people of Egypt and Syria can attest. During the recent uprisings in these countries, the national governments were able to shutdown internet access within their borders through the use of Border Gateway Protocols (BGPs); software that affords the decentralized facilitation of internet-based communication. In the case of Egypt this meant the government ordering all private Internet Service Providers (ISPs) operating within the country to close their gateways and effectively cut off most data flows going in and coming out of Egypt's national borders. In the case of Syria, where the

[53] Banhof AB and the Banhof Bunker where its servers are located can be viewed at http://www.bahnhof.net

government controlled the only ISP available to its citizens, this meant the government itself closing these gateways to cut off connectivity within its borders.[54]

In interviews with young people there was a common view that a government entity was always watching them and others through the internet in an unexplainable way. At times this was expressed as some "conspiracy" other people believed. Other times, this was discussed though specific examples of legislation and court cases that gave them a sense of the government's potential ability to watch. As Orlando specified,

> Well, I know this for a fact that the government can look at all your emails. Like, the amazing Patriot Act, one of the wonderful things that we created. ... Well, I don't like how the government thinks that they can just do anything to like give up our freedom for safety. So, like the Patriot Act, like I'm not for it, I just think it's stupid. Like unless you really suspect someone, why are you going through their stuff and like destroying First Amendment?

Others, such as sixteen year old Felicia, didn't cite a specific policy or piece of legislation but felt the government was always watching and as a result, there was no such thing as privacy:

> Everything can be seen by the government. There's no such thing as privacy anymore. They say you can—any time your phone is on, you can be followed. Like you can be being traced, your phone calls can be listened to and if police wanted to get your text messages, they could get your text messages. Private or not.

Some couldn't explain why they thought the government was watching but, like sixteen year old Whitney, they felt its gaze regardless:

---

[54] For a more detailed description of how BGPs can be used to shutdown connections to the internet within specific borders, see Cloud Flare's recent analysis of how Syria shutdown the internet at http://blog.cloudflare.com/how-syria-turned-off-the-internet

> Like I just know it. And I know that the government could see everything you do in a computer. Like if you're doing like credit card scams and stuff like that, they could trace it back to that computer.

Fifteen year old Rebecca got a sense the government was watching, or could watch, from the prosecutorial practices entailed in the much reported Casey Anthony trial:

> Well, as I was talking about before with like killer cases or, you know. I think there's a girl that was killed by her mother, as awful as it sounds, like a couple of years ago in Florida or someplace. And they, they went on the mom's computer and they looked in her Google search to see what she had been researching, and it was like how to smother somebody or how to like break their neck or something like that. So then they -- so they, they thought it was her, but it wasn't. They weren't sure that it was her, but then these searches kind of made it seem like, well, why are you like looking at that? You know, what were, what were your intentions?[55]

After Megan described her texting habits, I asked her how she thought her texts got from Point A to Point B. In explaining this process she discusses government surveillance but dismisses it as a conspiracy:

> I know they go through some like major, major terminal or something like that, and then they shoot to the person. Like I know it may be like two seconds before they get the text messages, but it went some way at first. And then there's a conspiracy that someone was reading our text messages. I don't know if that's true or not. Like, you know, on TV when there's always -- on a TV show, there's always somebody who has this FBI conspiracy complex and they talk about how they're reading your text messages. They'll listen to your phone calls, and they're listening for key words.

When I asked her if she thought this conspiracy had any truth to it. She said, "it could be true. But I feel like if that's the case, then I would've been in so much trouble by now. So yeah."

---

[55] Casey Anthony was tried in Florida for the premeditated murder of her two year old daughter, Caylee, but was ultimately found innocent by a jury of her peers. Google search records from a computer accessible to Casey were presented as evidence against her during the trial. Among the searches made on Google were "neck breaking" and "how to make chloroform."

Megan, like others I interviewed as well as members of the YDRC, discussed government surveillance as a phenomenon that didn't affect them since they themselves had not been arrested, or sued, or spied on -- at least to their knowledge. Yet, the regular raising of this matter by one or more youth co-researchers in multiple workshops pointed to the banal but important ways such surveillance factors into their identity configurations.

Even when discussing surveillance, or "spying online," as an unethical practice that they did not want to be subjected to, they expressed a certain empathy for the practice. One co-researcher was offended that their mother tried to regulate their home internet access with a content filter. The co-researcher was able to easily circumvent the filter, but took the protective gesture as a sign that their mother "didn't trust I could think for myself." At the same time, this co-researcher stressed that such a filter really was needed for their younger brother, and described the additional measures they took -- such as, checking the web browser's history to see where he'd been surfing -- to monitor his online behaviors because "he doesn't know any better." Another youth co-researcher discussed their concern with racism online and how they felt the internet allowed people "like the KKK" to "pull, like, a digital hood over their faces." This co-researcher felt more online surveillance was necessary to identify and "unmask" people engaged in racist cyberbullying. The co-researcher also felt it was important to censor racist language online. To address this concern, we debated how we might distinguish between what was and was not considered racist content, and considered the problems of having a small group of people evaluate and censor a larger group of people's communications.

While some content may be obviously racist, sexist, homophobic, or just spam, we reasoned that it may not be so easy to decide what was and was not appropriate content. We

decided to implement a content 'flagging' system in our network, as seen in Figure 4.3. Participants would be allowed to post whatever they wanted but small flag icons would be automatically added to it so others could flag the content if they personally felt it was inappropriate. When someone flagged a piece of content, the YDRC and I would be notified by email so we could evaluate the content together and decide if it should remain or be deleted. If more than two participants flagged the content before we were able to evaluate it, the content was temporarily removed from the site until we could evaluate it. This allowed us to monitor potential spam or inappropriate content that other participants were bothered by, allowing us to take into account the judgments and feelings of participants. This also created a temporary system where content that participants found particularly offensive could be removed immediately by them through collective action until we had a chance to consider it and decide if it should be reinstated or not.

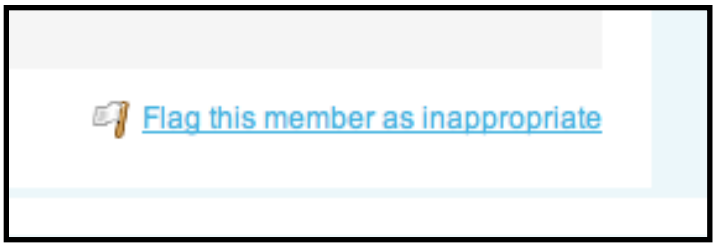

Figure 4.3 Content Flagging System

Interestingly, in discussing how we should organize our own social network and what sort of information we wanted to aggregate from our eventual participants, the YDRC was unanimous in wanting to only aggregate data that was necessary and through modes that were obvious to people. The request for an email address so participants could then manage their own accounts sounded reasonable to the YDRC and necessary so participants could reset their own passwords. It also seemed fair to record the IP addresses of people who logged into the social network so we could both prevent spam and hacked accounts as well as get a general sense of the

geographical location of our participants. The only other modes we agreed to aggregate data through were social profile fields and public comments made on participant profiles through status updates or wall posts as well as on blog posts in our Research Pods. Co-researchers did not want people to upload more than one profile picture, they didn't want to let people 'check in' anywhere, they wanted to make it easy for people to delete their accounts, and they did not want to allow people to send private messages to each other. 'Checking in' or 'tagging' oneself at a certain physical location, a common practice on Facebook, Twitter, and Foursquare, was particularly unappealing to the YDRC. While this practice is often flagged as dangerous by parents and teachers because of the way it potentially lets strangers know where they are physically located in real-time, this was not why the YDRC singled out this specific practice from exclusion from our social network. Their reasoning was twofold: they personally found this practice to be an "annoying" way that people publicly flaunted certain offline behaviors, and they found no value in aggregating this kind of information for our research purposes.

The desire to prohibit private messages between social network participants stemmed from a governance issue. Initially the YDRC assumed we couldn't see the private messages exchanged by participants. I explained that, as network administrators, it would be possible for us to see even these private messages if we wanted to look at them. Thus, ensuring participants that their personal messages within the network were private would be inaccurate; we could only state we wouldn't look at them. That *The Social Network*, a movie about the creation of Facebook, had recently been in theaters made most of the YDRC aware that there were actual people who developed and operated Facebook. They frequently referred to "the guy" that made Facebook. The revelation of what we could see as network administrators, thus led one co-

researcher to reflect on the role Facebook's employees might play in compromising their personal privacy:

> Like, I know [with] Facebook not one person can man it by themselves -- maybe when it first began. So, if you're constantly hiring new workers, that means that what was once secure is no longer secure. Because now multiple people that weren't supposed to know what was in the message now knows what content it held. And once they're fired, they're angry and they share that. So it just keeps going on and on and then in chain emails -- now the whole world knows what that message said.

As this discussion of privacy and security unfolded another YDRC member explained how they choose not to use any of Facebook's privacy controls -- what this co-researcher referred to as 'privatizing' their content -- because they didn't trust the efficacy of such controls:

> I don't privatize it because even so, there's always a way around. I feel like there are hackers out there no matter what. [Privacy] doesn't exist. It's a façade. Like it's something that somebody -- like they want to say, okay, we did this and that to make sure your page is secure just so they couldn't be blamed if something like they were hacked or things like that.

Whether it was a disgruntled former employee of Facebook or "hackers out there," the realization that there were people and practices that could not be stopped through the standard privacy settings caused the YDRC to more critically consider the work such settings do if they don't fully protect their privacy.

Rather than trying to find some way to truly ensure private communication, the YDRC decided the best course of action would be to prevent the notion that a private message could be sent at all. Their ultimate solution was to only design public communications within the network that could be seen by all participants, aside from the most sensitive information that could be used to identify a person. This meant all social network participants could see what the YDRC

and I could see, except for personal IP addresses, email addresses, and passwords. This information was known only to participants, myself, and the YDRC. Email and IP addresses were specifically singled out for special treatment as a result of our engagements with the IRB. The following inquiry was one of the few design features we were asked to further explain by the IRB after submitting our proposed plans for the social network: "We should also know about protection of the children's email addresses and IP addresses from hackers." In responding to this question, we followed CITI guidelines for "Internet Research" to setup a Secure Socket Layer (SSL) connection so that such data was transmitted securely and unlikely to be accessed by unauthorized actors. While I personally handled obtaining, purchasing, and configuring the SSL certificate for our social network, I updated the YDRC at each stage of this process in workshops and by email so that they got a sense of what was being done and how we were securing certain data flows in our network. Suddenly, what sites they used that did or did not offer them an SSL or "https" connection meant something and was now regularly mentioned in workshops. At the time, Facebook had yet to begin offering SSL connections for its users. That we were offering a form of informational security, and thus a certain level of privacy that Facebook wasn't, made the YDRC openly question "why don't they do this?"

The YDRC expressed surprising restraint in a socioeconomic climate where corporations like Google and Facebook try to aggregate as much information as possible so they can mine and potentially monetize it at a future date. Likewise, governments aggregate and store as much information as possible so they can mine it to prevent yet-to-emerge security problems. Despite expressing their own desire to oversee and censor in certain contexts, the YDRC did not want to be data hoarders with participant information. And, they wanted to make it clear to the

participant when they were watching and what they were watching. In this complex and contradictory way the YDRC negotiated what it meant to be the watcher and watched in various contexts before settling on what sort of watching they wanted to do with their own social network. They reproduced common social network features such as social profile fields, status updates, and personal accounts. They reworked regular user access to social network information by only designing public communication between participants that all members of the network could see. Password, email, and IP address information was carefully considered and specially secured. Finally, they resisted the informational ethos of 'aggregate now, ask questions later.' Their banal experiences of surveillance, censorship, government, proprietary social networks, and racism thus shaped their evolving understandings of privacy, property and security, and resulted in nuanced practices of reproducing, reworking, and resisting in our social network design.

Katz (2007) brings our attention to the ways fear and risk have become routinized in a post-9/11 US through constant, if mundane, performances of security. In appropriating Billig's (1995) concept of "banal nationalism," she describes the way security performances produce a "banal terrorism" in everyday environments through a range of discursive and material social practices.[56] Katz and Billig argue for the importance of considering the banal when unpacking how broader phenomena are constituted and sustained with and within routine practices and individual as well as collective identities. In considering how broader phenomena operate in these small ways, we might thus also consider how modes of informational development such as

[56] Billig's (1995) theorization of "banal nationalism" extends broadly to everyday practices of nationalism, such as raising a national flag or singing the national anthem, that foster geopolitical identity configurations where individuals affiliate with certain nations and/or homelands.

cyberdomination permeate the routines of young people and assist the social reproduction of informational capitalism.

Parikka (2005) considers the small ways fear and risk operate in the context of computer viruses and the privatized security performances with which they have become associated. As he argues, the "threats of capitalism are turned into general fears and risks, which in turn are translated into consumer products that aim to control that fear and deliver safety" (para. 29). Even when not using specific antivirus products, the fear of viruses was still often addressed by interviewees and YDRC members through routine security performances that evoked the purpose and practices behind such products. Vague references to anti-viral software that were used to "clean" their computers were often made in interviews. Eighteen year old Jane explains how she "cleans" viruses from her computer by clearing her browser's history and suggests a deeper cleaning is necessary when a "bad virus" is contracted:

> Like say all the website you visit, like if you click anything, it just stays on the hard drive. So, if you go to clear history and then you just click on it, it clear it. But if you get the bad virus stuff, if it go all over everything. I just clean it. Like [viruses] want to see what I type and stuff, but I clean it. But it is not like 'clean, clean, clean.'

The expressive hand gestures Jane made when explaining this process are worth noting. When she says "but I clean it" she wiped her hand laterally over the table as if to wipe a hard drive. When she says "it is not like clean, clean, clean" she made a more traditional sweeping gesture as if cleaning the floor with a broom. For Jane, this viral cleaning is comparable but not the same as sweeping the floor. Unlike dust or dirt, Jane sees computer viruses as strategic actors interested in her personal information. As such, cleaning in this context is about the security of her informational property and thus tied to her sense of privacy.

Few things could be considered more boring and mundane than cleaning, yet Jane was not the only interviewee to evoke this practice as important for securing privacy and property. In the case of Felicia sweeping is discussed alongside securing her Facebook account's password and controlling access to personal photos:

> It's like I have a security sweep so my computer won't get viruses and stuff. And if I had a virus, that thing pops up on my screen. And then, it's just like the whole Facebook thing, like make sure your password is secured, and make sure your photos are blocked only to your friends and stuff like that. You don't want—just security is protection from the outside world to make sure that people that you don't know don't get access to your private life and stuff like that.

Felicia describes securing privacy through cyberdominance. She negotiates her interactions with "the outside world" through security sweeps, censorship, and secured passwords in order to feel a sense of protection. She describes a boundary-making process and the self-policing of these boundaries to negotiate access between what she sees as a public and private life.

In unpacking such practices with the YDRC it became clear what young people define as private in information ecologies is something they have come to understand as their personal property. Their ability to meaningfully negotiate access to this property gives them a sense of security. Tactically, this is not so different from the previous example of Apple developing a lucrative business model with iTunes within a domain that what was previously considered threatening to corporate profits. However, unlike iTunes that practices cyberdominance for capital accumulation, these young people practice cyberdominance for situated and often self-fulfilling purposes. While Parikka (2005) brings our attention to the ways a "viral capitalism" sustains itself through the production of social problems and the selling of commodified solutions, this consideration does not fully account for the ways people also produce spaces

without consumer products to control such generalized fear; as previously highlighted in my discussion of Elena's private file sharing site. Taken together, banal practices in everyday environments can be understood as reproducing but also renegotiating and resisting fear and risk in information ecologies. That feelings of both insecurity and security can function to sustain capitalist modes of production calls for more attention to the configuration of individual and collective identities around matters of securitization.[57]

Situating Cyberspace

There was a consistent trend among the young people I interviewed whereby they could articulate a detailed knowledge of the physical hardware and branded software and services with which they regularly interacted. Yet, little knowledge was articulated regarding the spaces produced through these interactions. While interviewees and the YDRC conveyed an awareness of the internet's physicality -- through references to "wires," "satellites," "databases," "servers," and "a building somewhere" -- there was little conception of cyberspace as a definable domain within their everyday life. The internet and its associated cyberspaces produced through human interaction were thus taken as a magical entity that operated unexplainably in the background. Eager to further explore this trend, I showed the YDRC Figure 4.4 during our first workshop. I created this visual following the interviews to lightheartedly convey this magical aspect of the internet and its associated cyberspace that was routinely expressed by interviewees.

---

[57] I draw the term 'securitization' from international relations literature (cf. Buzan, Wæver & Wilde, 1998) to account for the process of framing a given matter in terms of national, corporate, or personal security. As such, the securitization of cyberspace is the making of cyberspace a matter of security that must then be addressed through surveillance, censorship, policing, and other security practices.

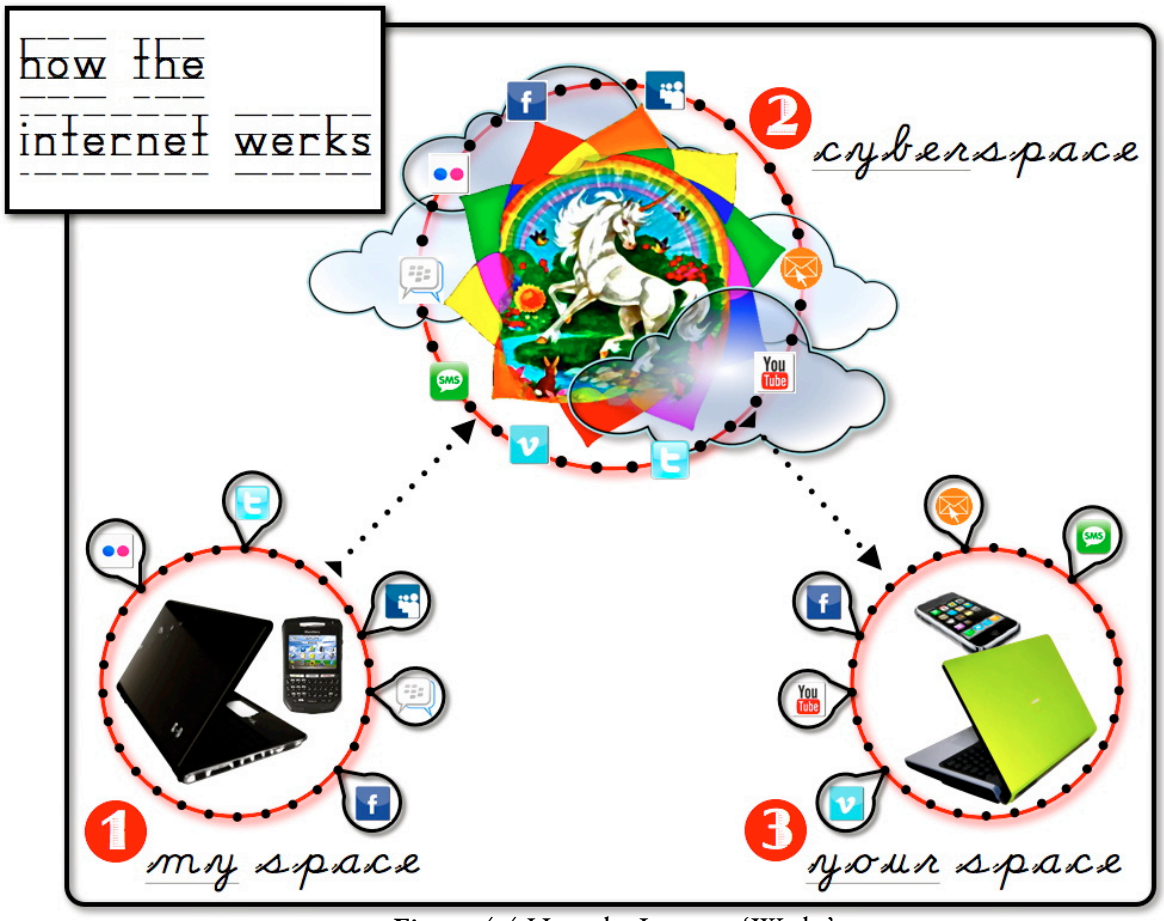

Figure 4.4 How the Internet 'Werks'

With states and corporations focused on defining a cyberspace to enhance their own situational awareness and dominance within it, Figure 4.4 was meant to help the YDRC imagine their cyberspace(s) to enhance their own environmental consciousness. The YDRC laughed when they saw this visual, but they also expressed a sense of 'being had' by having to agree that they had no idea how the internet worked or how they'd describe cyberspace. I made Figure 4.4 lighthearted both to convey a sense of absurdity that something we interact with so regularly could still remain somewhat unknown, and to poke fun at myself. After all, this cloudy monstrosity of unicorns and rainbows was my best attempt to visualize cyberspace. The aim was

to draw attention to a shortcoming in our environmental knowledge without making it feel alarming or too significant to overcome.

To emphasize that this lack of knowledge was not unique to me, them, or even young people more generally, I played a video of former US Senator Ted Stevens. The video featured Stevens, then Chairman of the Senate Commerce Committee, discussing his opposition to a Net Neutrality amendment proposed for the Communications, Consumer's Choice, and Broadband Deployment Act of 2006. Net Neutrality is a concept derived from the end-to-end design of internet-based communication; namely, that all data traveling through networks should be treated equally as they travel from end to end and the privileging of certain data flows over others should thus be prohibited. If proprietary ecologies allow corporations to control the circulation of, and access to, information then being able to charge for certain modes of circulation and degrees of access would accelerate the accumulation of capital. Net Neutrality was meant to work against this by preventing a tiered internet in which people could pay more for better circulation. Stevens strongly opposed Net Neutrality and his opposition became famous for its impassioned and confused description of the internet:

> Ten movies streaming across that, that internet, and what happens to your own personal internet? I just the other day got -- an internet was sent by my staff at ten o'clock in the morning on Friday. I got it yesterday! Why? Because it got tangled up with all these things going on the internet, commercially.[58]

The YDRC laughed more, but also became intrigued how so many people, even powerful senators, could barely explain how the internet worked. This led to new discussions about how

[58] Transcribed from http://www.youtube.com/watch?v=f99PcP0aFNE

few opportunities there were for people to meaningfully participate in the day-to-day development of the internet and in the operation of information ecologies.

Being taught how to stay safe or out of trouble online was now discussed as more than just an annoyance. Such education was considered a distraction from what they wanted to be learning and what they felt would be empowering to learn. Discussions turned to the "tech geeks" in their schools who they felt held much power because they were able to technologically outsmart teachers and administrators. These tech geeks, for example, were discussed as among the first to figure out a way around school filters and to share this knowledge with other students. Their knowledge of the internet gave them a degree of cyberdominance within their schools. The linking of awareness in information ecologies with empowerment through these discussions made the YDRC more eager to build the social network so that they might gain a better understanding as to how information circulated in their environment. The designing of a social network thus became as much of an end itself as whatever additional meaning this social network took on after it was designed.

This led to several tutorials on information architecture as well as internet history and governance. My goal was not to provide a comprehensive understanding for the YDRC of these areas, but to curate a variety of short videos, news articles, visuals, and other engaging but educational media that we could interact with together during workshops and discuss in real time. These discussions helped build new knowledge but also raised new questions for further investigation. These discussions helped focus the questions in our Interview Vlog, as well as the

kinds of experts the YDRC were now interested in talking to through the vlog.[59] This also began to deepen our discussions of international affairs and the ways they touch down in everyday life, providing a shared vocabulary for informational issues.

Towards the beginning of each workshop we would take time for members of the YDRC to raise whatever issue was on their mind, or to share any kind of media they desired. This was typically a website, a video, a song, or just an idea that was related to something we previously discussed or that a co-researcher wanted us to discuss. In our second Research and Planning Workshop one of the youth co-researchers brought up the uprisings in Egypt and Libya that were being reported in American media: "That guy in Egypt -- it keeps happening in different countries. Libya, too." The others quickly joined the discussion to talk about the ways social media was being used, with one youth co-researcher noting how the governments in each nation were "shutting down the internet." Notably, the victims and criminals in this discussion were muddled with one youth co-researcher commenting on Muammar Gaddafi as "a good guy, everything I hear is that he's a good guy" and another on Hosni Mubarak as "a good leader, but he's just been there too long." That the YDRC consisted of self-identified Muslims and Christians, some of whom were born in Africa and Asia, appeared to give them more information or at least a different perspective from what was being communicated through American media. When one co-researcher noted that 'everything they had heard' indicated Gaddafi was a good guy, it was clear this wasn't heard on the local or national news but from within their respective communities.

---

[59] See Chapter Three for a discussion of the Interview Vlog and a list of the questions asked by the YDRC.

I took this as an opportunity to broadly outline how the Egyptian government shut down the internet by instructing its ISPs operating within the country to close their Border Gateway Protocols (BGP) and thus cut off most data flows going in and coming out of Egypt's national borders.[60] While sympathetic to the rebels in each country, the shutting down of the internet was discussed amongst the YDRC as inevitable; something to be expected when revolutions take place. As on co-research noted:

> They want to lead, and to hold on to it. And when the public resists it really destroy the business world. So they react.

This was not a defense of the Egyptian government, but an acknowledgment of the ways people in power, try to hold on it by any means necessary. That shutting down the internet wasn't a violent act by these states, in and of itself, also made it more tolerable to the YDRC. With legislation being considered in Congress that would provide the executive branch with these same abilities to shut down the internet during a state of national emergency, I asked the YDRC how they would feel about their president having the same power.[61] The YRDC largely, and rather quickly, concluded that if the president felt it was warranted it would be ok to shut down the internet. Their reasoning was presented along the lines of 'if shutting down the internet could have prevented 9/11, then why wouldn't you shut it down?' They specifically noted that they "trusted Obama" suggesting that who held the office of the president had much influence in their conclusion.

---

[60] BGP is a software that affords the decentralized facilitation of internet-based communication.

[61] At the time, the bill being considered was the Cybersecurity Act of 2009. Although this bill did not pass, it continues to be proposed with various modifications during each legislative session.

I then asked how long should the president be able to shut down the internet in an attempt to prevent another 9/11. There was a pause before one member cautiously stated, “until night time -- I think.” Another member decided they could go a week if necessary, but the rest agreed even a full day without the internet was too long. They reasoned that the loss of connectivity would cause so much disruption to their lives and the lives of others that it would create a national emergency far greater than the one it was intended to prevent. In connecting their experiences with those elsewhere, the YDRC reconsidered such affairs transpiring in Egypt and Libya within their own life space and recognized a mutual affinity for freely communicating with and within information ecologies.

Considered practically, and in the context of their own lives, shutting down the internet for more than a day no longer seemed like a reasonable proposition for most of the YDRC. Unlike Egypt’s use of BGP, cyberspace in this case helped provide a translocal gateway through for co-researchers. Such a consideration countered the common social admonitions the YDRC encountered, which framed the internet and its associated cyberspaces as a gateway to disengagement, distraction, and even drugs. Within the US, media campaigns such as “Parents. The Anti-Drug” warn parents that cyberspace is a gateway to drugs for their “teen” (Figure 4.5).

While interviewees described an addiction to products provided by corporations such as Facebook and Google, the ‘Parents. The Anti Drug’ campaign's take on the internet only warns parents that it can be used to obtain and become addicted to drugs. There is no discussion of the unbridled and unregulated mediation of the internet in young people’s everyday life, and the

expressed addiction to such connectivity. One advertisement, Figure 4.5, warns parents that their children's online privacy is being invaded by threatening others, "online, their space is everyone's space" above an image of a large pixelated eye. This slogan is fitting for a campaign that dedicated an entire section of its site to encouraging and helping parents spy on their children's online activities.[62] This vertical barrage of media frames young people in a constant state of danger within the public imagination thus rationalizing drastic action. Considering government inaction and the shortcomings of formal education, young people and particularly their parents are encouraged to seek protection from cyberspace through corporate products. Where the state has neglected to legislate or regulate the privacy of young people in cyberspace, corporations offer privatized solutions at a price.

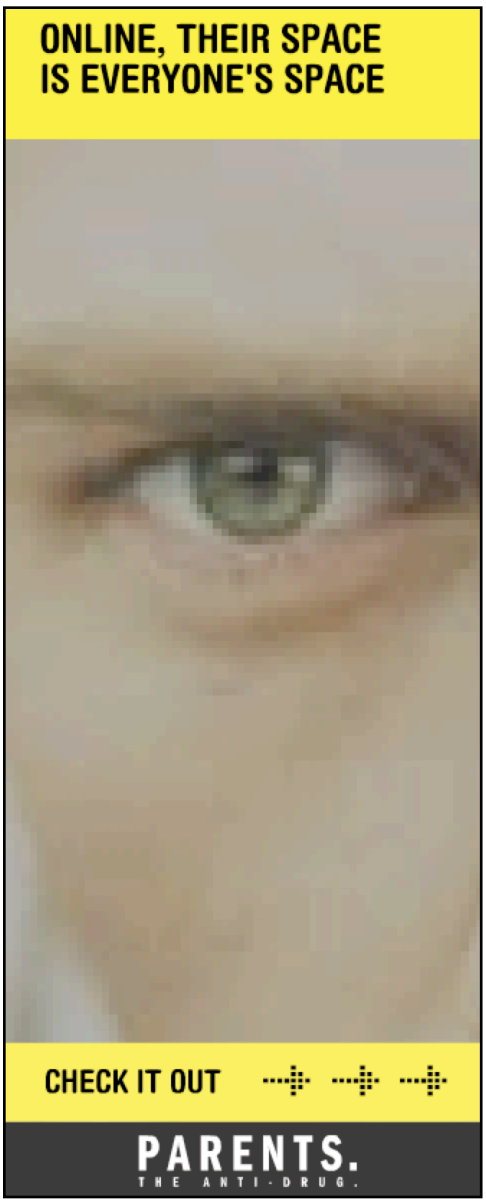

Figure 4.5 Online, Their Space is Everyone's Space ©2011 Parents. The Anti-Drug.

Of the prominent laws passed since the 1990s regarding young people's use of the internet, only one, the 1998 Children's Online Privacy

[62] The "Parents. The Ant-Drug" site is now defunct, but an 15 February 2009 archive of its section dedicated to "Teens and Technology" can be found via the Internet Archive's Way Back Machine at http://web.archive.org/web/20090215014608/http://www.theantidrug.com/E-Monitoring/index.asp

Protection Act (COPPA), actually deals with young people's privacy.[63] COPPA grants the federal government the authority to regulate the collection of personal information over the internet from individuals under 13 years of age. While COPPA has slowed the collection of information from those younger than 13, it falls short of the regulation it was intended to do (Montgomery, 2007). In a study of 162 popular websites that collected personal information from young people, only four were found to fully comply with COPPA (Cai et al., 2003). In 2012 the Federal Trade Commission (FTC) evaluated 400 apps intended for kids from the iTunes and Google Play stores, and found that 59% of the applications were transmitting kids' information to the apps' developers or a third party, and only 20% contained any privacy-related disclosure (Mohapatra & Hasty, 2012).

To simply leave this discussion with a sense that corporations offer solutions where governance and education has failed would be incorrect. Prominent federal legislation passed since the 1990s, in the name of young people's safety, reveal that state and corporate responses to public concerns are deeply intertwined (see Figure 4.6). The Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (N-CIPA), both passed in 2000, work in tandem to tie federal funds for technology in schools and libraries to surveillance and censorship programs.[64] Schools and libraries that participate in the federal E-Rate and LSTA programs, for instance, are required to certify that safety policies and filtering technologies are in place before receiving funds. Since E-Rate and LSTA are programs designed to provide

---

[63] The Children's Online Privacy Protection Act can be found at http://www.ftc.gov/ogc/coppa1.htm

[64] The Children's Internet Protection Act can be found at: http://www.ifea.net/cipa.pdf. The Neighborhood Children's Internet Protection Act can be found at: http://thomas.loc.gov/cgi-bin/query/z?c106:S.1545

Legislation	Abbreviation	Enacted	Summary
Child Pornography Prevention Act	**CPPA**	*1996**	CPPA extended the federal ban on child pornography to include virtual simulations of such pornography. CPPA was struck down in 2002.
Children's Online Privacy Protection Act	**COPPA**	1998	COPPA Grants the federal government the authority to regulate the collection of personal information over the internet from individuals under 13 years of age
Child Online Protection Act	**COPA**	*1998**	COPA restricted online access to any material defined as harmful to people under the age 18. COPA was struck down in 1999 by courts and litigated until 2009.
Children's Internet Protection Act	**CIPA**	2000	CIPA requires adoption and implementation of an "Internet Safety Policy" For all LSTA, ESEA, and E-rate fund applicants.
Neighborhood Children's Internet Protection Act	**N-CIPA**	2000	N-CIPA focuses on what has to be included in a school or library Internet safety policy.
Protect Our Children Act	**POCA**	2008	POCA requires ISPs who know of possible child pornography transmissions within their network to report such activity to the authorities.

Figure 4.6 Prominent Federal Legislation Enacted Since 1990

discounted technology to financially disadvantaged institutions, and since schools and libraries must pay out of pocket to implement surveillance and censorship programs, CIPA and N-CIPA expand the digital divide by targeting schools and libraries that need money and encouraging them to spend a portion of their budget on private surveillance and censorship technologies.[65] This comports with other circuits of dispossession operating within public education (cf. Fine & Ruglis, 2009) and thus encouraging public institutions to rely on corporate products to protect young people from perceived dangers in cyberspace.

The Child Pornography Prevention Act (CPPA) and the Child Online Protection Act (COPA) were both subsequently struck down by the federal courts.[66] According to Kathryn

[65] Concerned that CIPA would worsen the digital divide within the U.S. and that the censorship required by the law would regulate free speech, the American Library Association challenged the constitutionality of CIPA. On 23 June 2003, the Supreme Court of the United States upheld CIPA.

[66] The Child Online Protection Act (COPA) can be found at: http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000231----000-.html.

Montgomery (2007, p. 100), the former director of the Center for Media Education that lobbied for the passage of the previously discussed COPPA, the abbreviation of COPA was purposely constructed to emulate COPPA and thus obfuscate its objectives within the public imagination. COPA and CPPA focus little on young people's privacy, but rather almost exclusively on the regulation of pornography. CPPA, passed in 1996, was intended to extend the federal ban on child pornography to include virtual simulations of such pornography.[67] In 2002, CPPA was struck down by the US Supreme Court for being too broad and violating free speech.[68]

COPA, passed in 1998, has been struck down three times by federal courts for being too broad in using community standards as part of its definition of harmful materials and for violating the First and Fifth Amendments of the US Constitution. Most notable, is the way COPA has been used by the government to fuse private databases with public institutions. In preparation for a trial in 2006 the Department of Justice (DOJ) subpoenaed search engines for web addresses and search records. The DOJ argued that such data was necessary to support their case that COPA was warranted and should be upheld. Major search engines such as Yahoo! and MSN Search (now Bing) complied, while Google challenged the subpoena and thus achieved a minor victory by having to provide only a sample of URLs from their database and not full searches conducted by its users.

In 2007, during the third rejection of COPA by the courts, US District Judge Lowell A. Reed, Jr. noted in his ruling that "perhaps we do the minors of this country harm if First

---

[67] The Child Pornography Prevention Act (CPPA) can be found on the Internet at: http://www.politechbot.com/docs/cppa.text.html.

[68] The syllabus of Ashcroft v. Free Speech Coalition, which led the Supreme Court to strike down the Child Pornography Prevention Act (CPPA) can be found at: http://en.wikisource.org/wiki/Ashcroft_v._Free_Speech_Coalition?oldid=420606

Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection."[69] Indeed, as COPA, CIPA and N-CIPA work to place public surveillance and censorship in the hands of corporations, and private data in the hands of public institutions, questioning what we are taking away from young people in the name of their safety appears to be in order as well as questioning whose security is being ensured through such measures if not young people's.

In one way 'youth' is taken up by legislators and corporations as a red herring. The red herring metaphor is analyzed by Lippmann (1913) as a political practice designed to obfuscate or distract from a particular objective and can be presented as either a pest or benefit. It is a political maneuver that can be employed as "a matter of misrepresentation and spite" or as an "honest attempt to enlarge the scope of politics" (p. 261). Within informational development, young people emerge as a feared and fearful point of tension where a dialectic of domination and empowerment plays out in troubling and overt, if also familiar, ways. As a pest, a misrepresentation of 'youth' is employed in CPPA and COPA to justify the erosion of civil liberties. A similar misrepresentation deploys 'youth' to sell commodities for protecting young people from certain information ecologies as well as for protecting certain information ecologies from young people. Corporations such as LifeLock, which specialize in selling private security services for preventing identity theft, specifically target parents. They stoke a fear of young people's identities being "easy targets" for theft and subsequent circulation in shadowy information ecologies:

---

[69] Judge Lowell A. Reed, Jr.'s full opinion was accessed on 23 March 2012 from http://www.paed.uscourts.gov/documents/opinions/07D0346P.pdf

> The Identities of children are now being stolen by thousands. They are easy targets because no one ever monitors them. These kids aren't finding out until they graduate from high school and apply for their first job or a student loan. By then, thieves have often been using their Identities for years and the kid's good name is ruined before he or she even has a chance to start.[70]

All this, "because no one ever monitors them." Less public service announcement and more advertisement, the solution offered for this crisis is a private one: "LifeLock now offers protection for kids under the age of 16 for only $25 per year." This service is part of a growing child protection industry that feeds off public concerns for the well-being of the young. Young people, of course, are monitored constantly and are frequently disclosing their everyday data through a variety of proprietary ecologies. Private security services such as the one offered by LifeLock stoke parents' fears, and aims at their wallets by raising their children's safety as a red herring.

In another way, 'youth' as a red herring can also be taken up by young people to enlarge the scope of politics around themselves and their life space. When discussing how the YDRC wanted to identify themselves within the social network, and what personal information they were comfortable disclosing in a shared "YDRC social profile," they all agreed they wanted a profile pic. A few of the youth co-researchers were particularly adamant that these profile pics be "professional." In this sense, professional meant they wanted to be in control of their representations. With photography being an almost instantaneous and continuous social practice, slowing this process down and carefully planning to take a photo of themselves seemed both fun and personally valuable to the YDRC.

---

[70] The following quote is from LifeLock's official website and was retrieved on 01 December, 2007 from http://www.lifelock.com/lifelock-for-people/how-we-do-it/how-can-lifelock-protect-my-kids-and-family

Following this discussion, I arranged for a professional photographer, Tracy, to attend one of our workshops. Tracy provided us with a short PDF, '*Tips for Conceptualizing Your Portrait*' that served as our introduction to basic portraiture; it introduced concepts of lighting, posing, negative space, the use of props, and the use of keywords to focus artistic direction. A week before our photo shoot, we read and discussed the PDF together. I encouraged the YDRC to take these tips not as instructions to follow but aspects to consider when planning their portraits. Co-researchers were particularly drawn to the idea of self-describing keywords that they could communicate through their portraits. As such, we agreed that they would each think of two keywords to focus their photo shoot. Since some felt self-conscious about disclosing what their keywords were, we also agreed that they could be shared or kept private. Apart from discussing their keywords with Tracy, it was up to them who else knew.

When the photographer arrived, she began to setup a space in our room with lighting, an assortment of cables, and a large camera (Figure 4.7). Each co-researcher took a turn with Tracy to discuss their keywords and ideas. Some wanted to only disclose their keywords to Tracy while others announced theirs,"robotic and bold," "professional and classy," and "pretty and serious." The YDRC's approach to the photo shoot was playfully deliberate. Deliberate in that each co-

Figure 4.7 YDRC Photo Shoot

researcher had an agenda; they had already picked out their clothes, prepared their hair and in some cases make-up, and had a pose in mind before coming to the photo shoot. This process was also playful in the ways they mocked themselves and each other for being so conscious of their image. Planned poses were mixed between poses with a purposefully distorted face intended to make the rest of us laugh. Through this playful production of their portraits, co-researchers' participation gave them a sense of the work and -- importantly -- the intention behind images. This knowledge carried over well after the photo shoot had ended.

At our next workshop I brought in a number of online advertisements and magazine covers featuring informational youth. Among these images were a Yahoo! advertisement I saw on a New York City pay phone featuring an ecstatic young white woman taking a photo of herself with a smartphone, the Oxygen Network subway advertisements analyzed in Chapter 2, the infamous 1995 Time Magazine cover that featured a shocked young boy's face illuminated by a computer screen under a bolded CYBERPORN headline, and a number of the 'Parents. The Anti Drug' advertisements.[71] I projected these images so we could consider what the youth co-researchers tried to communicate with their portraits in the context of what these images of youth were communicating.

The YDRC treated their analysis of these images as something of a game. When I flashed an image they would laugh and then eagerly begin to dissect the lighting, posing, and positioning of the youthful images. Even when shocked or annoyed by a particular misrepresentation of

---

[71] On 03 July 1995, Time Magazine published a front cover article titled "On a Screen Near You: Cyberporn" which was later found to be based on a report containing several errors. An Electronic Frontier Foundation response to Time Magazine's decision to publish this story can be found here: http://w2.eff.org/Misc/Publications/Declan_McCullagh/www/rimm/time.html

youth, they still seemed to ultimately shrug it off before calling for the next image. I displayed

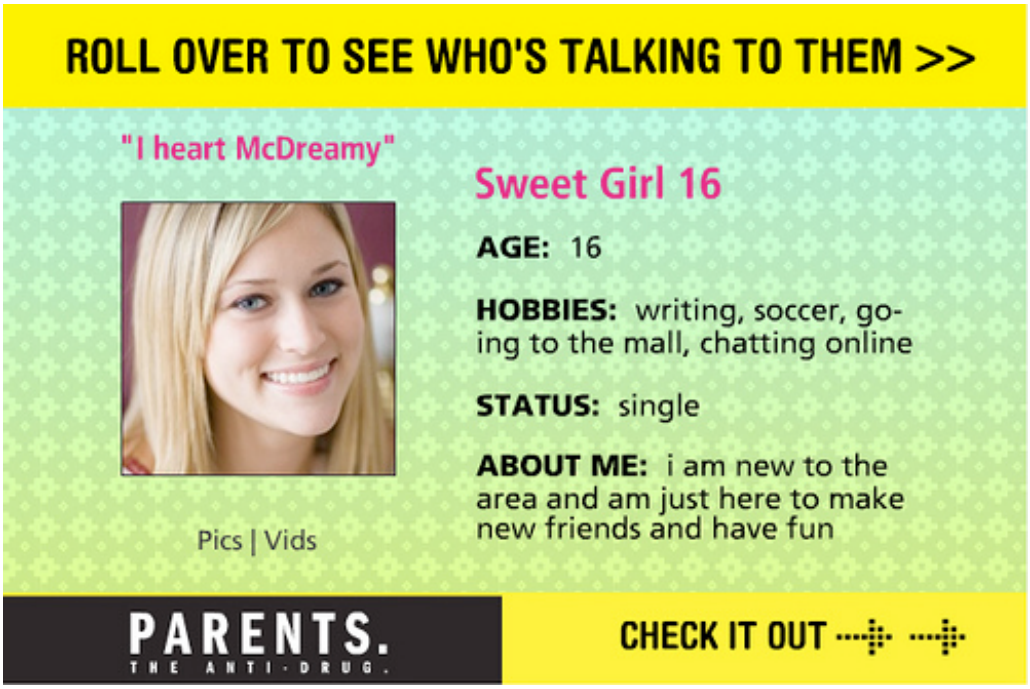

Figure 4.8 Sweet Girl 16 ©2011 Parents. The Anti-Drug.

Figure 4.8 after several images. This was another advertisement from the 'Parents. The Anti-Drug' campaign warning parents of online predators. With Figure 4.8 the discussion turned less playful.

The YDRC seemed to have grown tired of seeing the same misrepresentation in every ad. One co-researcher pointed out how Sweet Girl 16 and Angela from the Oxygen ads "are basically the same blonde white girl." Two co-researchers took on a high-pitched and decidedly 'girly' Barbie-like voice and, while cocking their heads to the side like Sweet Girl 16, mockingly cried out "save me" with a forced teeth-bearing smile. These co-researchers were not laughing at abduction. They were laughing at the notion that Figure 4.8 was abduction. As one co-researcher explained "no one does that." By which they meant, no one sets up their profile to make themselves appear so innocent and vulnerable. This moment raised the notion that there was a

commonality in how these advertisements presented young people as hapless victims in a dangerous environment; a representation they found inconsistent with the ways they and their friends presented themselves online.

Conclusion

Cyberdominance does not present us with new global actors, rather it presents a new way to consider and analyze what have been persistent global actors; namely governments, corporations, political groups, civic institutions, individuals and so on. In other words, cyberdominance gets at how a 'banal nationalism' and 'banal terrorism' operate through proprietary ecologies to produce and reproduce a range of social material relations at various scales. As a boundary-making mode of informational development, US cyberdominance works to enclose and privatize cyberspace under a banner of national security and at the expense of other people, places, and things that are viewed as threats to US dominance. That cyberspace, like all space, is produced through human practice indicates that this attempt to occupy a cyberdomain for profit and control is thus also an attempt to control and profit from material social practices. That behaviors and relations as well as people, and places, are encouraged and discouraged through proprietary ecologies does not make this sorting determinative. Yet, proprietary ecologies and expressions of cyberdominance do introduce a banal influence that is felt and negotiated by everyday people.

In returning to the notion of 'informational youth,' this means that young people negotiate these cultural expectations in relation to their own lived experiences. This also means that engaging young people in the production of information ecologies, also helps them build

literacies and capacities for better negotiating such expectations in relation to their own situated interests and concerns. If Pratt & Rosner (2006) are correct in their argument that there is no "territorial defense" between global forces and the intimate experiences of everyday life, then it is imperative that we question why territorial defense strategies have become so central to informational development and are so often justified through securitization practices. As I have shown, the securitization of cyberspace plays out in the intimate spaces of youth yet it does not protect them from the global processes of informationalism nor does it ensure their freedom of action. Indeed, it seems more often to protect informational processes *from* the common practices of youth.

The abstract application of young people as a political tool acts to remove their agency while cultivating a public that is normalized to surveillance and censorship. As Katz (2001, 2006, 2008) argues, the home is being turned into a reflection of the state where surveillance, through hypervigilant parenting practices, is embedded in the geography of childhood. Government and corporate development of proprietary ecologies for purposes of cyberdominance further this argument. In bypassing the parent and interacting directly with young people through the built environments of cyberspace, traditional power holders are extending their influence in contemporary childhood while simultaneously cautioning parents about precisely the hazards of these practices. By engaging the YDRC in collaborative research and design to build an open source social network, they began to question the subtle ways they consent to the politics of proprietary ecologies. This often played out in overt ways, such as how the YDRC had to negotiate what our social networks consent form would and would not say. They began to question the ways Facebook encourages them to submit to a long and complicated Terms of

Service agreement, and reworked this process by developing a short and concise Terms of Participation that focused on informing participants of what was being done with their data in an easy to understand format.

Parallel to government and corporate cybderdominance, and often because of such attempts to subjugate, young people have proven adept at using media to engage in meaningful political engagement to protect their privacy and assert their autonomy. If corporate and state interests aim to rework the architectures of cyberspace so as to vertically structure the flow of information and capital across a transnational cyberdomain, then young people, through their political engagement, puncture the inevitability of this trend toward cyberspatial hegemony (cf. Gramsci, 1971). In the communicative environment of cyberspace, young people challenge their abstract employment in mass media and emerge as actors, thus ensuring that the road to hegemony remains a contested terrain.

Chapter Five
From Here to Affinity

A new social reality emerges when young people are routinely surveilled, rationalized, and objectified in proprietary ecologies of information systems and algorithms for purposes of national security and corporate profit. While affording access to friends, family, news, play, healthcare, sex, and love the increasing presence of ICTs in daily environments also advances the feasibility of a surveillance state. As the canaries in this contemporary data mine, young people exist in the thorny nexus of government and corporate aims to privatize and police various cyberdomains. Such a social reality problematizes young people's security as it compromises their privacy by embedding them in circuits of dispossession that privatize increasingly opaque aspects of their information environment. This reality is also contested terrain and young people, as resilient and empowered social actors, stand for more than dupes and red herrings in corporate and government aims for cyberdominance. In considering the situated experiences of youth, this chapter poses the question: where do we go from here? Despite the often dominating and dystopian realities of young people's informational experiences, the answer is not less participation but more. More critical participation in information ecologies, even the proprietary ones, is necessary for opening these opaque aspects of the environment and raising environmental consciousness.

Despite the technophobic mythology of the original Luddite movement, their aim was not to grind the machine to a halt but to orient the machine toward their own socioeconomic

interests. At the dawn of the 19th century, English workers were upset with the way they were being replaced by machines in the workplace amidst widespread unemployment and inflation. They thus took in droves to the factories of Northern England to destroy the machinery they saw as unjust reproductions of the skilled labor they themselves rightfully represented and should thus be paid to perform. As Jones (2006) tells it:

> The Luddites of 1811 to 1812 smashed machines. They did so in protest and sabotaged specific owners' looms and finishing shops. They did *not* voluntarily give up technologies of convenience or status, as do many neo-Luddites today. ... Luddite direct action can be seen as taking from the relatively rich in order to give back (or keep) what was due to the workers (many of whom were poor) (p. 47).

The original Luddite movement was a working class revolt against a socioeconomic environment produced by a dominant class through technological innovation; it was a revolt against material social relations that made their work 'redundant', not machines in and of themselves. The original Luddites came to expect more than they had come to experience in their restructuring workplace. Based on their lived experiences of industrialism, they came to resent the ends to which technology was being put and collectively realized a common affinity for more equitable working conditions.

In Haraway's (1985) *Cyborg Manifesto* an affinity group is offered as a political coalition formed by choice that can "hold together witches, engineers, elders, perverts, Christians, mothers, and Leninists long enough to disarm the state" (p. 155). Such a motley crew can be found in the recent opposition to the US Senate's attempted passage of the Stop Online Piracy Act (SOPA). Supported strongly by the Motion Picture Association of America and the Recording Industry Association of America among a number of other business interests, SOPA was intended to enhance the Digital Millennium Copyright Act (DMCA) by increasing penalties

for copyright infringement, expanding the definition of what it meant to pirate content, and to require network operates to surveil the data within their own networks to filter out pirated content along with copyright infringers. This last stipulation was particularly egregious as it would have forced the operators of even small networks, like the MyDigitalFootprint.ORG social network, to not only police their participants on behalf of the state but invest their own money to retrofit their networks for such deep surveillance and censorship. This provoked a broad backlash against elected officials among both left and right-leaning individuals and political groups who recognized a common affinity for personal privacy, property, and security in information ecologies. Network operators large and small organized a day of protest where they fully or partially shut down their websites so that visitors and users saw a "Stop SOPA" or "Stop Online Censorship" banner with information about the legislation alongside ways to contact a local legislator. Echoing the original Luddites, networked machines were taken down to protest material social relations and power structures that represented an undesirable socioeconomic environment. In light of these protests, the Senate chose not to bring up the proposed legislation for a vote as Senators who were once co-sponsors of the legislation began to publicly distance themselves from the legislation.

In developing an open source social network the YDRC often found themselves designing in opposition to their known surroundings of proprietary ecologies that operated for profit. Through this oppositional positioning, the youth co-researchers also ironically realized various affinities in their surroundings and began to articulate certain expectations of privacy, property, and security. They began to recognize their connections to broader matters of personal privacy, intellectual property, and national security and to negotiate their expectations in kind.

They came to question how the social networks they were regular consumers of were being produced, and for what purposes. This lead them to design a social network more inline with their own values, but it also turned them on to an aspect of their environment previously unseen.

It excited some of the co-researchers that there was freely available open source software that could be drawn on to build a familiar social network but for different purposes. That the YDRC had to learn about Secure Socket Layer (SSL) certificates and a two-step registration process to comply with Institutional Review Board requirements for enhancing participant privacy, made them more aware that their privacy could also be enhanced by similar means. There was nothing dystopian or depressing about our workshops. In building a social network, the YDRC built capacities for unpacking and manipulating their own information environment while realizing commonalities between what they expected in terms of privacy, property, and security and what situated others expected. In the following sections I outline the importance of considering social expectations and of negotiating competing and contradictory cyberdominances to build more open ecologies that can better support and foster the complex affinities of youth.

Evolving Expectations

A recent ruling by the US Supreme Court brings into focus the importance of societal perceptions of privacy and personal property in shaping government and corporate security practices. In United States v. Jones (2012) the Supreme Court ruled that attaching a GPS device to a vehicle for the purpose of tracking a citizen's pubic movements constitutes a search under

the Fourth Amendment and thus unconstitutional.[72] More notable than the unanimity of this decision, is that the majority opinion was premised on the fact that the federal government physically trespassed on Antoine Jones' private property to install the GPS device on his car. In doing so, the Supreme Court left open the question of whether such surveillance would have been constitutional had the government not physically installed the device. If, for example, the government had instead decided to remotely access a commercial GPS device that had been voluntarily installed by Antoine Jones or some other non-government actor, then there would have been no physical trespassing and thus, potentially, no violation of the Fourth Amendment. This is a notable distinction considering the diminishing need to physically place a GPS device on most people now that cars are increasingly sold containing GPS units and most smartphones contain the same or similar functionality.

United States v. Jones (2012) raises more questions than it answers regarding the constitutionality and morality of state surveillance amidst expanding proprietary ecologies. It also raises the importance of considering societal expectations and understandings in hegemonic practices such as cyberdominance. If hegemony is an attempt to foster public consent for the policies and practices of a dominant social formation (Gramsci, 1971), then negotiations over what people expect in terms of personal and collective privacy, property, and security becomes central to their consent. Governments, corporations, and individuals no longer need to physically enter a house or tap a phone line to gain access to the multitude of personal information that

---

[72] The Fourth Amendment of the United States Constitution states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (U.S. Const. amend. IV).

flows through everyday environments. What privacy may have been possible behind closed doors and within the physical confines of a home space is now throughly problematized by the pervasive presence of ICTs. What people expect is happening to their privacy, property, and security in this context indicates what they will and will not accept.

As my interviews indicate, what young people expect in terms of privacy, property, and security is often complex and contradictory. Yet, as my participatory research and design with the YDRC shows, when young people are engaged as producers of their own social network they begin to develop and articulate more focused expectations. In developing a Terms of Participation they came to expect terms of service policies that they could read and make sense of themselves. If they could do it, why couldn't large corporations with scores of lawyers? In seeing the kinds of data generated in a social network from an administrator's perspective, they came to expect explanations for why certain personal information was being aggregated by other social networks in their environment, and what was being done with this information. In thinking through the consequences that would result from the internet being shutdown within their own country, they critically reconsidered Egypt's decision to shutdown the internet within its borders as a result of protests.

The YDRC would have cared if the internet had been shutdown before participating in the MyDigitalFootprint.ORG Project. However, if someone asked them what they thought about the government shutting down the internet during a national emergency, they likely would have given an answer similar to the one they gave me when I first posed the question: 'it would be OK, if it were an emergency.' Upon reflection and critical consideration this off-the-cuff assessment gained depth when considered in multiple contexts during our workshop discussion.

Eventually, the YDRCs assessment evolved into 'it would be ok ... until night time.' This latter response to the same question conveys a different expectation of what is acceptable and of how security is understood. At first blush, many interviewees were similarly quick to proclaim how unconcerned they were about their 'online privacy.' As long as their parents couldn't see everything they were doing online then they had plenty of privacy. Then as they continued to talk and discuss their relations with the internet they would articulate several contexts in which they were concerned about their privacy. The more they reflected and discussed their expectations, the more complex and indeterminate their statements on privacy, property, and security became.

In separate concurring opinions, Justice Alito and Justice Sotomayor both problematize the majority opinion's focus on "physical intrusion" in United States v. Jones (2012). Yet, only Sotomayor's concurring opinion offers a contextualized consideration of the expectations of citizens who currently exist in what is a largely mystified and little understood information ecology:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society" (p.17).

Sotomayor contends that if citizens were aware of how details of their identity were being aggregated by the government, it would have a chilling effect on associational and expressive freedoms. In interviews, it was routinely expressed that the government 'could be watching' yet solace was typically found in a conveyed sense that they themselves weren't the ones being

watched. ‘Others’ such as criminals, hackers, pedophiles, or terrorists were the ones being watched. Sometimes, it was their own younger siblings or cousins that they felt should be watched more. Then, when working with the YDRC, I projected my *iTracker* screenshots to help visualize the kinds of data that is routinely aggregated on people with smartphones. These visuals left the YDRC almost speechless as seemingly for the first time they got a sense of the very personal information that perhaps was being collected *on them*. As one co-researcher blurted out: “how is *that* legal?!”

Much as the YDRC concluded that having to shutdown the internet for a full day or more ‘wasn’t worth it,’ Sotomayor concludes that the potential abuse associated with the unbridled aggregation of everyday data out weighs the potential security benefits of this surveillance practice. Sotomayor then implores her colleagues on the Supreme Court to consider societal expectations of privacy in public:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on (p. 18).

The young people I interviewed as well as the YDRC felt that their daily movements and behaviors could be tracked by the government and other actors, but few expected that their personal data could be aggregated and used to ascertain such intimate details. It's what this aggregation could enable that was largely unconsidered. Sotomayor’s focus on “a reasonable societal expectation of privacy in the sum of one’s public movements” is important as most of society is unaware of the extent to which they’re being tracked and what processes can be

enabled with this everyday data, nor is there a social consensus on what constitutes 'being in public.'

When young people learn about the most basic ways that their personal information is being aggregated, they begin to articulate more sophisticated privacy concerns alongside a general amazement that such surveillance is actually happening — legally — in what they think of as private places such as their social profile, instant messages, email, or texts. Interviewees regularly indicated that 'they knew' certain aspects of a particular space was not private, such as wall posts or status updates in Facebook, but would then also insist that other spaces, most often their email inbox, was more private and secured. Their inboxes, of course, were anything by private considering all interviewees and the YDRC utilized 'no-fee' email services that mined the content of their emails.

Sotomayor concludes her concurring opinion by arguing that society expects more privacy than it currently has in "the digital age," and calls for a decoupling of secrecy and privacy to develop more situated judicial considerations of when and where people expect privacy:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties … This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection (p. 19).

The crux of Sotomayor's argument for decoupling secrecy and privacy, a coupling advanced by Justice Alito in his concurring opinion, is that people may not be acting secretively when volunteering information to a corporation in a specific context yet that does not mean they have no expectation of privacy. When a person 'checks in' to Facebook to tell their friends and Facebook where they are at any given moment, they are not acting secretively but they are not necessarily acting publicly either. Regardless of what the terms of service they submitted to states, few people would expect this information to be made available to other corporations and/or governments.

People's everyday data circulates within multiple proprietary ecologies that are nested within each other. A person might deliberately and voluntarily interact with one of these ecologies, such as Google, but beyond that it becomes difficult to infer exactly what's happening to one's data and where it is circulating. This is, in part, by design. If you're an information company that wants to encourage your users to share, like, enter, submit, and disclose all kinds of everyday data then you don't want to slow the process down with pesky privacy concerns or complicated engineering. Much like a fast food business model, mystifying the production process makes the product taste better. This production process, however, can be slowed down and opened up particularly through modes of research, education, and even play. As my work with the YDRC indicates, when this happens expectations evolve.

Negotiating Cyberdominance

Cyberspaces can operate to reinforce the dominance of nation states over their citizens through boundary-makings that are both mundane and staggering. Recent events in the Republic

of Estonia have also shown how citizens can reorient cyberspaces towards their own ends. These events point less to citizen domination and more to the open struggle between governments and citizens to negotiate competing desires of cyberdominance. In 2007, the Estonian government relocated a Russian war memorial from its capital Tallinn to the city's suburbs. This relocation of a memorial built in 1947 by the Soviets to commemorate their soldiers who died during WWII caused the local, and more distant, Russian population to rebel. Instructions for how to manually and automatically ping Estonian web servers were disseminated across blogs, chat rooms, and bulletin boards resulting in a distributed denial of service (DDoS) attack that compromised the Estonian government's information infrastructure for several days.

A 'ping' is a call-and-response practice where one computer sends a signal to a host on a network. If this signal is returned it means a connection with a particular host is possible, and the length of time the signal takes to return indicates the strength of the connection. Pinging is a routine practice everyone engages in when visiting a website, and these pings entail only minimal amounts of data that can be handled easily by a host. However, when multiplied to a significant degree these small and common queries can overwhelm and thus crash a host, rendering it inaccesible to the public and thus 'denying service.' In defining and attacking an Estionian cyberspace, this DDoS overwhelmed Estonia's information infrastructure and effectively disabled government websites and email systems as well as ISPs, banks, news organizations, and telecommunication companies over a five-day period (cf. Davis, 2007; Finn, 2007). This event was not the first of its kind, as similar events had transpired on a smaller scale between China and Taiwan as well as between Palestine and Israel. This event was notable because the Estonian government publicly accused the Russian government of coordinating this

act of "cyber-warfare" and requested that the North Atlantic Treaty Organization (NATO) take military action against Russia. NATO declined to act but began to bolster the cyberdominance capacities of its member countries with the aim of preventing future cyberattacks. This interest in cyberdominance can also be seen in the 2007 establishment of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence [*sic*]; one of 19 NATO centers established to provide knowledge and expertise on various subjects deemed important to the security of its member countries.[73]

Subsequent analyses of this incident were unable to implicate the Russian government. A horizontal network of semiautonomous 'botnets,' 'hackers,' and 'script kiddies' were instead identified as culprits with IP addresses originating primarily from Estonia and Russia (cf. Borland, 2007; Davis, 2007). Experienced hackers functioned as the organizers, posting instructions on websites, blogs and message boards, detailing how to ping Estonian web servers. 'Script kiddies,' defined as young foot soldiers, reportedly accessed these instructions and began to manually ping Estonia's web servers. Finally, software programs referred to as 'botnets' subversively operated hundreds of thousands of individual computers across the globe to automate and accelerate the pinging process, creating an internationally distributed cyberattack. That identities were configured around these banal acts, speaks again to an informational dialectic. While the rebels' realized a shared affinity for having their heritage represented in Estonia's capital that led to participatory practices which at least temporarily dominated the Estonia government, their affiliations as 'script kiddies' also made them more visible and subject

[73] The NATO Cooperative Cyber Defence Centre of Excellence can be found at http://www.ccdcoe.org

to state retribution as individuals. Estonia, and NATO, may not have retaliated against Russia but they began to increasingly police individual citizens.

Participants in this DDoS attack utilized cyberspace to facilitate lateral communication and coordinated action by circumventing physical, social, legal and economic barriers constructed to prevent collective action. According to one Israeli security expert, who assisted Estonia with its response to the attack, such instances where decentralized crowds are the source of attacks should be thought of more in terms of "policing metaphors than military" (Borland, 2007). Crowds, he argued, must be controlled and subdued, not attacked. In this context, proprietary social media such as Facebook or Google, become an object of interest to governments in that they provide the means for identifying and policing the more wired segments of its citizenry; that includes both the ‘script kiddies’ as well as your everyday kid. In making national borders around a cyberspace, nation states claim jurisdiction to control and police activities within those borders; regardless of whether such activities are domestic or foreign, commercial or personal. As United States v. Jones (2012) highlights, this extends as much to the US as Estonia.

The merging of military and policing tactics undergird attempts by governments such as the US and Estonia as well as inter-governmental organizations such as NATO to develop cyberspatial military operations at home and elsewhere. Although this form of crowd control to suit the purposes of a ruling class has a long social history (cf. Le Bon, 1910), the neoliberal roots of this desire to develop such cyber-operations in the US can be found in a 2000 report from the Project for the New American Century (PNAC). PNAC was a foreign policy think thank tasked with enhancing America’s global supremacy and organized by prominent politicians such as Donald Rumsfeld, Paul Wolfowitz, Jeb Bush, and Dick Cheney; all of whom had

significant influence in shaping foreign policy during George W. Bush's presidency. PNAC is perhaps best know for the public call to invade Iraq well before the attacks of 9/11 in their report *Rebuilding America's Defenses: Strategy, Forces and Resources For a New Century*. Yet this same report also argued prominently for the US to "control the new 'international commons' of space and 'cyberspace,' and pave the way for the creation of a new military service – U.S. Space Forces – with the mission of space control" (Donnelly, 2000). In PNACs view, outer space and cyberspace were both untapped resources ripe for exploitation. New markets could be made in and around these 'spaces' and specialized military forces were necessary to ensure America's continued dominance in the global economy.

The Space Forces eventually took shape in the US Air Force's 2007 proposal of an Air Force Cyber Command. As Figure 5.1 shows, the Air Force's "Above All" slogan was rebranded to include "cyberspace" alongside "air" and "space." By 2009 the government's expressed need for a coordinated cyberdominance strategy across all branches of the US Military was addressed through the establishment of US Cyber Command in Meade, Maryland. The official emblem of the Cyber Command, in true sci-fi geek form, contains an

Figure 5.1 US Air Force Advertisement

encrypted algorithm that when decoded paradoxically reveals a cryptic mission statement (see Figure 5.2). When decoded, the algorithm 9ec4c12949a4f31474f299058ce2b22a reads:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[74]

Figure 5.2 US Cyber Command Emblem

[74] This translation was retrieved from the Marine Corps Times on 11 December 2012 from http://www.marinecorpstimes.com/news/2010/07/ap_military_cyber_command_logo_070810/

The Department of Defense's defining of a cyberspace according to a historical geography of nation-states thus gives form to a new domain for military intervention aimed at ensuring "US/ Allied freedom of action."

In challenging traditional modes of production by reworking geopolitical borders as well as the roles of producer, consumer and distributor, cyberdominance encloses common modes of communication, education, identity and group formation as well as political engagement. As the DDoS on Estonian servers and the constitutional debate over a societal expectation of privacy in the US indicate, governments must negotiate their own aims for cyberdominance in relation to the aims and expectations of their citizens. Castells (2007b) argues that state and corporate interests are engaging cyberspace to protect their role as global power holders. This means the use of surveillance and censorship to protect the intellectual property rights of corporations, to monitor political activity on social networks, or to regulate the flow of data within and across national borders. Such policing has been primarily rationalized by the public with a desire to take action against pedophilia, pornography and abduction for the sake of young people's cyber safety and security. Whether the US government or Apple, both aim for cyberdominance through the defining and enclosing of proprietary ecologies, and capitalizing on such fears. At the same time, young people still manage to negotiate empowering cyberspaces capable of addressing their own situated interests and concerns. It can take the form of a private file sharing site, the circumvention of web filters at school, participation in a DDoS attack, or an open source social network, among other manifestations. Each represents a boundary-making process that makes sense of the interplay between cultural expectations and lived experience.

Conclusion

While cyberdominance may be an emerging US war doctrine, as a territorial project of informational development it operates more broadly in federal legislation such as the DMCA and SOPA as well as in the proprietary trading algorithms of transnational financial markets and the mundane operations of common proprietary software. Globally, cyberdominance can also be found in the internet governance policies of the International Corporation for Assigned Names and Numbers (ICANN). At an intimate scale we can see cyberdominance play out in home-based surveillance programs such as Net Nanny and common location technologies such as GPS devices and RFID chips (Katz, 2001). Each of these practices is an expression of, or a will to, cyberdominance justified through securitization and typically carried out through privatization. Each contributes to an environment that produces and reproduces historically rooted power structures in myriad ways and renegotiate personal and public understandings of privacy, property, and security.

ICANN is a California-based nonprofit corporation that governs the global management and assignment of internet domain names and IP addresses; a responsibility handled directly by the US government until 1998. While the creation of ICANN is a process of privatization by which the US transferred management of public resources to a private corporation, it is notable that the adopted multi-stakeholder model of ICANN governance provides participatory mechanisms that were previously unavailable to those outside the US.[75] As Low, Donovan, and Gieseking (2012) discuss, the history of cooperative housing in New York City is steeped in a

[75] ICANNs multi-stakeholder model is intended to involve corporations, governments, research and educational institutions, civil society organizations and non-government organizations in the global governance of the internet.

dialectic of constituting private governance structures for the enclosure of the powerful and the exclusion of perceived others, as well as to empower working class and immigrant communities. I do not wish to argue that ICANN is an empowering governance structure, but I do want to emphasize that its private governance is not by default a dominating practice in certain contexts. After all, anyone who registers a private domain name such as MyDigitalFootprint.ORG must do so through one of several for-profit corporate registrars that mediate interactions with this nonprofit international corporation. This inserts a profit motive into the registration and renewal of internet domains that gives much influence to corporations such as GoDaddy.

As the proprietor of the MyDigitalFootprint.ORG I lease exclusive rights to this domain from ICANN through a corporate intermediary; and I pay annual fees to both entities. Holding this lease allows me alone to assign this particular domain to a server that I privately lease from a web hosting company. In an international context, one could see how a translocally networked public could be better represented by a transnational private governance structure than a single government or consortium of governments that they are not a citizen of. As discussed in Chapter Four regarding Elena's private file sharing collective and my ownership of a vinyl record, private property represents a set of material social relations that can be oriented towards many ends. Wether or not an object or space is organized as private property, it is the material social relations and power structures entailed within this property that require closer consideration to foster more open and participatory information ecologies.

A convincing critique can be made that North American, European, and Japanese governments maintain too much control over the transnational internet infrastructure through their clout in ICANN, and to the detriment of developing nations primarily in the global south

(cf. Mueller, 2010). Further, it is not clear what means everyday people have to participate directly in ICANNs multi-stakeholder model. As a domain owner I am entitled to no vote in ICANNs governance the way I would were I the owner of a cooperative housing unit. I also have little control over how the web hosting company I lease my server from chooses to operate. In acknowledging these caveats, I still wish to hold on to the general premise that private governance and private property can still be participatory and even empowering if the material social relations and power structures associated with it are kept open. Too often open source is taken as an empowering end in and of itself simply because the core of these software systems are propertized in a way that allow anyone to access and manipulate for their own purposes.

When the New York Police Department (NYPD) decided to make troves of proprietary data on their 'stop and frisk' policing tactics open to the public, new and potentially empowering modes of understanding and knowledge production became possible. For the first time, the public could see the data the NYPD was seeing, and they could draw their own conclusions as well as build their own arguments regarding this racist policing tactic that disproportionately targets young black and latino men. But, it is hardly empowering to everyday people when Google builds an open source operating system and web browser like Chrome. In this case, Google keeps its source code open to attract app developers as well as encourage consumers to download this 'no-fee' software so they can aggregate and mine more detailed aspects of people's mediated behaviors. This empowers Google in their competition with Apple and Microsoft for platform dominance but offers little difference for consumers from proprietary alternatives.

Through the MyDigitalFootprint.ORG Project, the YDRC built a social network using open source software but also proprietary hardware, private domains, and leased server space. While our specific focus on open source software helped the YDRC develop understandings of how proprietary software operated by comparison, we focused mainly on opening up our own research relationships (cf. Luttrell, 2012) and configuring an information ecology that could account for their own complex and contradictory expectations around privacy, property, and security. An open source publishing platform such as WordPress was technically essential and epistemologically important to this process, but it was the participatory process itself that allowed us to build what we might consider an 'open ecology.' Where as a proprietary ecology is oriented towards the interest and concerns of a select group of owners an open ecology takes a participatory approach. As these are ecologies, the distinction rests in the quality of human-environment interactions afforded by each. Where as proprietary ecologies strive for ownership of everyday data, a participatory ecology orients itself towards affinity by taking action around the shared interests and concerns of those participating while remaining open enough to accommodate the situated experiences of each participant. It is thus more than the source we should be keeping open. The relations and means of production entailed in and revolving around these sources is precisely what is being enclosed through circuits of dispossession. Information and knowledges once considered outside the domain of capitalist production are now being brought into the fold and at a time when their empowering potential is heightened by diminishing costs of interpersonal communication and information processing.

In conclusion, I wish to consider another expression of cyberdominance in state surveillance programs such as China's Green Dam Youth Escort so as to question the social cost

of proprietary ecologies. China's Green Dam Youth Escort is an internet filtering technology that the Chinese government has required be installed on all PCs sold within China beginning in 2010. China frames the Green Dam Youth Escort as "green software" that helps ensure a "green and harmonious online environment" for China's youth. The presentation of this technology as 'green' makes an affective appeal to parents feeling alienated from an increasingly informationalized and privatized environment. Through the integration of this filter into people's literal and metaphorical operating systems, they are encouraged to protect children by blocking them from harmful content. Content deemed harmful by a central authority. 'Being green' is thus associated with both being healthy as well as safe and secure in information ecologies. This greenness is achieved by giving up control and turning over critical capacities to external entities who insist they know better. When discussing what concerned fifteen-year-old Megan about the internet, she questions what 'going green' means and who it assists:

> That one day, like, nothing will be possible without internet because I feel like that's the age that's coming really soon. They say it's going green, but what is the cost of going green? What about the people who can't afford the internet or computers and how are they going to function? That means that's extra money coming out of their pockets to use someone else's internet and computer services and things like that.

Like the original Luddites, what concerns Megan about the growing presence of the internet in everyday life is the effect this presence has on structuring the socioeconomic environment.

Who and where is left out of this geography, or forced to sacrifice more to access and navigate it, concerns Megan. The material social relations that are fostered, or not, by 'going green' suggests to Megan that there are consequences to such dispossession. Many of the young people I interviewed navigated broken home computers, heavily filtered school computers, lost,

stolen, or broken mobile phones, as well as expensive monthly phone and/or wifi bills so that they could access the internet. This made them attuned to the precariousness of connectivity and the downsides of being unable to access the internet, even temporarily. This was expressed parallel to feelings that they were too connected or 'addicted' to the internet. Such contradictions were common and expressed elsewhere in relation to matters such as privacy where they both morally opposed to surveillance and also felt everyone should be surveilled to prevent practices like cyberbullying and child abduction.

As canaries in the contemporary data mine young people are at the forefront of these complex negotiations over societal understandings and expectations. They have no personal and embodied experience of what phenomena like privacy, property, and security meant before the internet and thus the influence of corporations and governments that aim to orient these phenomena towards profit and control cannot be understated. An action approach makes possible involving the subjects of domination in developing situated and practical forms of engagement with and within their world.

The people, places, and things most disadvantaged by uneven informational development deserve representation not just in the social and material configuration of our environments as Harvey (2008) has argued, but also in our modes of research as Appadurai (2006) has argued. More methods and more literacies aimed at the production of space as well as knowledge are necessary to engage a population in considering what their interests and concerns are in relation to these broader matters. Through the production of an open source social network the YDRC asked questions they had not previously conceived and developed ideas about the internet and

cyberspace they had not previously imagined. I argue that more participation not less is necessary in the media within which we are developing.

Appendix A: Creative Common License

MyDigitalFootprint.ORG: Young People and the Proprietary Ecology of Everyday Data by Gregory T. Donovan is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

The following is the Creative Commons "human-readable summary" of this license:

> You are free:
> - to Share — to copy, distribute and transmit the work
>
> Under the following conditions:
> - Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
> - Noncommercial — You may not use this work for commercial purposes.
> - No Derivative Works — You may not alter, transform, or build upon this work.
>
> With the understanding that:
> - Waiver — Any of the above conditions can be waived if you get permission from the copyright holder.
> - Public Domain — Where the work or any of its elements is in the public domain under applicable law, that status is in no way affected by the license.
> - Other Rights — In no way are any of the following rights affected by the license:
>   - Your fair dealing or fair use rights, or other applicable copyright exceptions and limitations;
>   - The author's moral rights;
>   - Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.
>
> Notice — For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.[76]

[76] See: http://creativecommons.org/licenses/by-nc-nd/3.0/

The following is the full text of the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License:

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

a. **"Adaptation"** means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.

b. **"Collection"** means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined above) for the purposes of this License.

c. **"Distribute"** means to make available to the public the original and copies of the Work through sale or other transfer of ownership.

d. **"Licensor"** means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

e. **"Original Author"** means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

f. **"Work"** means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

g. **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

h. **"Publicly Perform"** means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

i. **"Reproduce"** means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing

fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections; and,

b. to Distribute and Publicly Perform the Work including as incorporated in Collections.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Adaptations. Subject to 8(f), all rights not expressly granted by Licensor are hereby reserved, including but not limited to the rights set forth in Section 4(d).

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested.

b. You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c. If You Distribute, or Publicly Perform the Work or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Collection, at a minimum such credit will appear, if a credit for all contributing authors of Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

d. For the avoidance of doubt:

> i. **Non-waivable Compulsory License Schemes**. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;
>
> ii. **Waivable Compulsory License Schemes**. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License if Your exercise of such rights is for a purpose or use which is otherwise than noncommercial as permitted under Section 4(b) and otherwise waives the right to collect royalties through any statutory or compulsory licensing scheme; and,

iii. **Voluntary License Schemes**. The Licensor reserves the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License that is for a purpose or use which is otherwise than noncommercial as permitted under Section 4(b).

e. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor

reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

a. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

b. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

e. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of this License.

Creative Commons may be contacted at http://creativecommons.org/.[77]

[77] See: http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday* 13(3). Retrieved from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949

Appadurai, A. (2006). The right to research. *Globalisation, Societies and Education* 4 (2), 167-177.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society* 2(4): 479-497.

_____ (2013). Estranged free labor. In T. Scholz (Ed.), *Digital labor: The internet as playground and factory*. New York: Routledge. (149-164).

Arnstein, S. R. (1969). A ladder of citizen participation. *Journal of the American Institute of Planners 35*(4), 216-224.

Bannon, L.J., & Ehn, P. (2012). Design: Design matters in participatory design. In J. Simonsen, & T. Robertson (Eds.), *The Routledge international handbook of participatory design*. New York: Routledge. 37-65.

Berners-Lee, T. (1999). *Weaving the web: The original design and ultimate destiny of the World Wide Web by its inventor*. Harper Business.

Bilandzic, M., & Venable, J. (2011). Towards participatory action design research: Adapting action research and design science research methods for urban informatics. *The Journal Of Community Informatics 7*(3). Retrieved from http://ci-journal.net/index.php/ciej/article/view/786/804.

Billig, M. (1995). *Banal nationalism*. SAGE Publications.

Breitbart, J. (2006). Where's my open access? *Civil Defense Blog*. 6 August. Available from: http://www.freepress.net/news/16943.

Bureau of Labor Statistics (2012). Employment and unemployment among youth: Summer 2012. Retrieved from http://www.bls.gov/news.release/youth.nr0.htm

Borland, J. (2007). Estonia's lesson for "cyberwar" fighters: Learn digital crowd control. *Wired*, 10 August. Available from: http://blog.wired.com/27bstroke6/2007/08/stonias-lesson-.html

Boyle, J. (2008). *The public domain: Enclosing the commons of the mind*. New Haven: Yale University Press. Retrieved from http://thepublicdomain.org

Cahill, C. (2004). Defying gravity? Raising consciousness through collective research. *Children's Geographies 2*(2). 273-286.

_____ (2007). Doing research with young people: Participatory research and the rituals of collective work. *Children's Geographies 5*(3). 297–312.

Cai, X., Gantz, W., Schwartz, N. & Wang, X. (2003). Children's website adherence to the FTC's online privacy protection rule. *Journal of Applied Communication Research* 31(4), 346–362.

Calvert, J. (2008). The commodification of emergence: systems biology, synthetic biology and intellectual property. *BioSocieties 3*(4), 385-400.

Capurro, R. (1990). Towards an information ecology. *Irene Wormell (Ed.): Information and Quality*, London: Taylor Graham. 122-139.

Castells, M. (1989). *The informational City: Information technology, economic restructuring and the urban-regional process*. Blackwell Publishers.

_____ (2000). *The Rise of the network society* (The information age: Economy, society and culture, Volume 1). Wiley-Blackwell.

_____ (2001). Informationalism and the network." In P. Himanen (Ed.) *The hacker ethic and the spirit of the information age*. New York: Random House. 155-178.

_____ (2003). The interaction between information and communication technologies and the network society: A process of historical change. *Coneixement I Societat*. 1, 8-21.

_____ (2007a). An introduction to the information age, City, 2(7), 6-16.

_____ (2007b). Communication, power and counter-power in the network society. *International Journal of Communication* [Online] 1(1). Available from: http://ijoc.org

Chozick, A. (2012, September 25). NBC unpacks trove of data From Olympics. *New York Times*. Retrieved from http://www.nytimes.com/2012/09/26/business/media/nbc-unpacks-trove-of-viewer-data-from-london-olympics.html?pagewanted=all&_r=0

Conti, G. (2009). *Googling security: How much does Google know about you?* Boston: Pearson Education Inc.

Crouch, M., & McKenzie, H (2006). The logic of small samples in interview-based qualitative research. *Social Science Information* 45, 483.

Davis, J. (2007). Hackers take down the most wired country in Europe, *Wired*, 21 August. Available from: http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

Dewey, J. (1916). *Democracy and education: An introduction to the philosophy of education*. New York: The Macmillan Company.

_____ (1938). *Experience and education*. New York: Touchstone.

Dodge, M., & Kitchen, R. (2005). Code and the transduction of space. *Annals of the Association of American Geographers* 95(1), 162–180.

Donnelly, T. (2000). Rebuilding America's defenses: Strategy, forces and resources for a new cen*tury*. Washington, DC: The Project for the New American Century. Retrieved from: http://www.newamericancentury.org/RebuildingAmericasDefenses.pdf.

Donovan, G.T., & Katz, C. (2009). Cookie monsters: Seeing young people's hacking as creative practice. *Children, Youth and Environments* 19(1), 197-222.

Ellerbrok, A. (2011). Playful biometrics: Controversial technology through the lens of play. *The Sociological Quarterly* 52 528–547.

Edison, T. (1878). The phonograph and its future. *North American Review* 126 (May-June), 526-536.

Erkison, E.H. (1982). *The life cycle completed*. New York: W.W. Norton & Company.

Etherington, D. (2012). iOS app store boasts 700K apps, 90% downloaded every month. *TechCrunch*. Retrieved from http://techcrunch.com/2012/09/12/ios-app-store-boasts-700k-apps-90-downloaded-every-month/

Ewen, S. (1976). *Captains of consciousness: advertising and the social roots of the consumer culture*. New York: Basic Books.

Fine, M. & Ruglis, J. (2009). Circuits and consequences of dispossession: The racialized realignment of the public sphere for U.S. youth. *Transforming Anthropology 17*(1), 20–33.

Fine, M., Torre, M.E., Boudin, K., Bowen, I., Clark, J., Hylton, D., Martinez, M., 'Missy', Rivera, M., Roberts, R.A., Smart, P. & Upegui, D. (2003). Participatory action research: Within and beyond bars. In P. Camic, J.E. Rhodes, & L. Yardley (Eds.), *Qualitative*

Research in Psychology: Expanding Perspectives in Methodology and Design. Washington, DC: American Psychological Association. 173-198.

Finn, P. (2007). Cyber assaults on Estonia typify a new battle tactic. *The Washington Post*, 19 May. Available from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

Florida, R. (2004). *The rise of the creative class and how it's transforming work, leisure, community and everyday life*. Basic Books.

Foth, M., & Adkins, B. (2006). A research design to build effective partnerships between city planners, developers, government and urban neighbourhood communities. *The Journal Of Community Informatics, 2*(2). Retrieved from http://ci-journal.net/index.php/ciej/article/view/292

Foth, M., Choi, J., & Satchell, C. (2011). Urban informatics. Paper presented at the *ACM Conference on Computer Supported Cooperative Work* (CSCW 2011).

Fuchs, C. (2009). A contribution to the critique of the political economy of transnational informational capitalism. *Rethinking Marxism* 21 (3), 387-402.

George, F. H. (1965). *Cybernetics and biology*. London: Oliver & Boyd.

Gibson, W. 1984. *Neuromancer*. New York: Ace Books.

Graham, S.D.N. (2005). Software-sorted geographies. *Progress in Human Geography* 29(5), 562–580.

Gramsci, A. (1971). *Selections from the prison notebooks*. International Publishers.

Greenbaum, J. (1979). *In the name of efficiency: Management theory and shopfloor practice in data-processing work*. Philadelphia:Temple University Press.

Greenbaum, J. & Kyng, M. (1991). Introduction: Situated design. In J. Greenbaum and M. Kyng (Eds.), *Design at work: Cooperative design of computer systems*. CRC, pp 1-21.

Greenbaum, J. & Loi, D. (2012). Participation, the camel and the elephant of design: An introduction. *CoDesign: International Journal of CoCreation in Design and the Arts, 8*(2-3). 81-85.

Glick, J. A. (1999). Focus groups in political campaigns. In D.D. Perlmutter (Ed.), *The Manship School guide to political communication*. Baton Rouge, LA: Louisiana State University Press. 114-21.

Haggerty, K.D., & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology 51*(4), 605–622.

Haraway, D. J. (1991). *Simians, cyborgs, and women: The reinvention of nature*. New York: Routledge.

_____ (2000). *How like a leaf: An interview with Thyrza Nichols Goodeve*. New York: Routledge.

Harris Interactive (2010). Trends & Tudes: YouthPulse 2010. 9(2). Retrieved from http://www.harrisinteractive.com/vault/HI_TrendsTudes_2010_v09_i02.pdf

Harvey, D. (1973). *Social justice and the city*. Baltimore: Johns Hopkins University Press.

_____ (2005). *A Brief History of Neoliberalism*. New York: Oxford University Press.

_____ (2008). The Right to the City. *New Left Review 53*. 23-53.

_____ (2010). *A Companion to Marx's Capital*. New York: Verso.

Hopkins, P. & Pain, R. (2007). Geographies of age: Thinking relationally. *Area 39*(3). 287–294.

Hunter, D. (2003). Cyberspace as place and the tragedy of the digital anticommons. *California Law Review*, 91(2), 439-519. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=306662

Hursh, D. (2007). Assessing no child left behind and the rise of neoliberal education policies. *American Educational Research Journal 44*(3), 493-518.

Indergaard, M. (2000). *Silicon alley: The rise and fall of a new media district*. New York: Routledge.

Introna, L.D., & Nissenbaum, H. (2000). Shaping the web: Why the politics of search engines matters. *The Information Society 16*, 169-185.

Jessop, B. (2004). Informational capitalism and empire: The postmarxist celebration of US hegemony in a new world order. *Studies in Political Economy* 72, 39-58.

Jones, S.E. (2006). Against technology: From the Luddites to Neo-Luddism. New York: Routledge.

Karaganis, J. (2011). Copyright infringement and enforcement in the US. *American Assembly*. Columbia University. Retrieved from http://piracy.ssrc.org/wp-content/uploads/2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf

Katz, C. (1998). Whose nature, whose culture? In B. Braun, & N. Castree (Eds.), *Remaking reality: Nature at the millennium*, London: Routledge, 46–63.

_____ (2001). "The state goes home: Local hypervigilance and the global retreat from social reproduction." *Social Justice* 28(3): 47-56.

_____ (2004). *Growing up global: Economic restructuring and children's everyday lives*. Minneapolis: University of Minnesota Press.

_____ (2006). Power, space, and terror: Social reproduction and the public environment. In S. Low, & N. Smith (Eds.), *The Politics of Public Space*. New York: Routledge. 105-122.

_____ (2007). Banal terrorism: Spatial fetishism and everyday insecurity. In Gregory, Derek and Allan Pred eds, *Violent geographies: Fear, terror, and political violence.* New York: Routledge, pp. 349-361.

_____ (2008). Me and my monkey: what's hiding in the security state. In: M. Sorkin, ed. *Indefensible space: The architecture of the national insecurity state*. New York: Routledge, 305-323.

Klaebe, H.G., Adkins, B.A., Foth, M., & Hearn, G.N. (2009). Embedding an ecology notion in the social production of urban space. In M. Foth (Ed.), *Handbook of research on urban informatics: The practice and promise of the real-time city*. Information Science Reference, IGI Global, Hershey, PA, 179- 194.

Koskela, H. (2000). 'The gaze without eyes': video surveillance and the changing nature of urban space. *Progress in Human Geography 24*, 243–265.

Kücklich, J. (2005). Precarious playbour: Modders and the digital games industry. *Fibreculture* 5. Retrieved from http://www.journal.fibreculture.org/issue5/kucklich.html

LaRose, R., Lai, Y.-J., Lange, R., Love, B., and Wu, Y. (2005). Sharing or piracy? An exploration of downloading behavior. *Journal of Computer-Mediated Communication, 11*(1), article 1. http://jcmc.indiana.edu/vol11/issue1/larose.html

Latour, B. (1987). *Science In action*. Cambridge MA: Harvard University Press.

_____ (1998). To modernize or to ecologize? That's the question. In B. Braun, & N. Castree (Eds.), *Remaking reality: Nature at the millennium*, London: Routledge, 221-242

_____ (1999). *Pandora's hope: Essays on the reality of science studies.* Cambridge MA: Harvard University Press.

_____ (2005). *Reassembling the social: An introduction to actor-network-theory*. Wiley-Blackwell.

Le Bon, G. (1910). *The crowd, a study of the popular mind* ([7th impression] ed.). London,: T. F. Unwin.

Lemley, M. A. (2003). Place and cyberspace. *California Law Review*, 91(2). 521-542.

Lenhart, A. (2012). Teens, smartphones & texting. *Pew Internet & American Life Project*. Retrieved from http://pewinternet.org/Reports/2012/Teens-and-smartphones.aspx

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011). Teens, kindness and cruelty on social network sites. *Pew Internet & American Life Project*. Retrieved from http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press.

_____ (2006). *Code: Version 2.0* (2nd ed.). New York: Basic Books.

Lewin, K. (1935). *A dynamic Theory of Personality: Selected Papers of Kurt Lewin*. New York and London: McGraw-Hill Book Company Inc.

_____ (1997). *Resolving social conflicts: Field theory in social science*. D.C.: American Psychological Association.

Lippmann, W. (1922). *Public opinion*. Free Press.

Low, S., Donovan, G.T., & Gieseking, J. (2012). Shoestring democracy: Gated condominiums and market-rate cooperatives in New York. *Journal of Urban Affairs*, 34 (3), 279-296.

Low, S. (2006). How private interests take over public space: Zoning, taxes, and incorporation of gated communities. In S. Low, & N. Smith (Eds.), *The politics of public space*. New York: Routledge. 81-104.

Luttrell, W. (2010). Interactive and reflexive models of qualitative research design. In W. Luttrell (Ed.), *Qualitative educational research: Readings in reflexive methodology and transformative practice*. New York: Routledge. 159-164.

Mansbridge, J.J. (1973). Time, emotion, and inequality: Three problems of participatory groups. *Journal of Applied Behavioral Science, 9*(2-3). 351-368.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., Hung Byers, A. (2011, May). Big data: The next frontier for innovation, competition, and productivity. *McKinsey Global Institute*. Retrieved from http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation

McCarthy, J. & Wright, P. (2004). *Technology as experience*. Cambridge: MIT Press.

McLuhan, M. (1964). *Understanding media: The extensions of man*. Cambridge: MIT Press.

Meinrath, S. & Pickard, V. (2008). The new network neutrality: Criteria for internet freedom. *International Journal of Communications Law and Policy,* 12. 226-241.

Mohapatra, M. & Hasty, A. (2012). Mobile apps for kids: Disclosures still not making the grade. Federal Trade Commission Staff Report.

Meyrowitz, J. (1994). Medium theory. *Communication Theory Today*. Eds. David Crowley and David Mitchell. Stanford, California: Stanford University Press. 50-77.

Mitchell, W. J. (1995). *City of bits: Space, place, and the infobahn*. Cambridge, MA: MIT Press.

_____ (2003). *Me++: The cyborg self and the networked city*. Cambridge, MA: MIT Press.

Mitchell, K., Marston, S. A., & Katz, C. (2003). Life's work: An introduction, review and critique. *Antipode,* X. 415-442.

Monahan, T. (2006). The surveillance curriculum: Risk management and social control in the neoliberal school. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life*. New York: Routledge.

_____ (2011). The future of security? Surveillance operations at Homeland Security fusion centers. *Social Justice* 37 (2-3): 84-98.

Monahan, T., & Palmer, N.A. (2009). The emerging politics of DHS fusion centers. *Security Dialogue 40*(6), 617-636.

Montgomery, K. C. 2007. Generation digital : politics, commerce, and childhood in the age of *the internet*. Cambridge, MA: MIT Press.

Mueller, M.L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.

_____ (2010). *Networks and states: The global politics of internet governance*. Cambridge, MA: MIT Press.

Nielsen Wire (2011a). Average U.S. smartphone data usage up 89% as cost per MB goes down 46%. Retrieved from http://blog.nielsen.com/nielsenwire/online_mobile/average-u-s-smartphone-data-usage-up-89-as-cost-per-mb-goes-down-46/

_____ (2011b). New mobile obsession: U.S. teens triple data usage. Retrieved from http://blog.nielsen.com/nielsenwire/online_mobile/new-mobile-obsession-u-s-teens-triple-data-usage/

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57, 1701-2010.

Pariser, E. (2011).*The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin Books.

Parikka, J. (2005). Digital monsters, binary aliens – computer viruses, capitalism and the flow of information. *Fibreculture* 4. Retrieved from http://journal.fibreculture.org/issue4/issue4_parikka.html

Parry B., & Gere, C. (2006). Contested bodies: Property models and the commodification of human biological artefacts, *Science as Culture* 15(2), 139-58.

Piaget, J. (1951). *Origins of intelligence in children.* New York: International Universities Press.

Postman, N. (1992). *Technopoly: The surrender of culture to technology*. Vintage.

_____ (2000). The humanism of media ecology. *Proceedings of the Media Ecology Association*, Volume 1. Fordham University, New York, New York June. 16–17.

Pratt, G. & Rosner, V. (2006). Introduction: The global & the intimate. *Women's Studies Quarterly* 34 (1 & 2), 13-24.

Proshansky, H.M., Fabian, A.K., & Kaminoff, R. (1983). Place-Identity: Physical world socialization of the self. *Journal of Environmental Psychology* 3, 57-83.

Rose, N. S. (1998). *Inventing our selves: Psychology, power, and personhood*. Cambridge, England; New York: Cambridge University Press.

Saegert, S., Fields, D., & Libman, K. (2009). Deflating the dream: Radical risk and the neoliberalization of homeownership. *Journal of Urban Affairs*, 31(3), 297–317.

Sandvig, C. (2006). The internet at play: Child users of public Internet connections. *Journal of Computer- Mediated Communication, 11*(4), article 3.

Schuurman, N. (2004). Databases and bodies: a cyborg update. *Environment and Planning A* 36, 1333-1340.

Singel, R, (2010). Check the hype — There's no such thing as 'cyber.' *Wired*. Retrieved from http://www.wired.com/threatlevel/2010/03/cyber-hype/

Smith, N. (1996). *New urban frontier: Gentrification and the revanchist city*. New York: Routledge.

Turkle, S. (2005). *The second self: Computers and the human spirit, 20th anniversary edition*. New York: Simon and Schuster.

Turow, J. (2006). *Niche envy: Marketing discrimination in the digital age*. Cambridge: MIT Press.

U.S. Const. amend. IV

United States v. Jones. 565 U.S. ___. (2012). Retrieved from http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf

van Schewick, B. (2010). *Internet architecture and innovation*. Cambridge, MA: The MIT Press.

Vygotsky, L.S. (1978). *Mind in society: The development of higher psychological processes.* Cole, Michael, Vera John-Steiner, Sylvia Scribner, and Ellen Souberman, eds. Cambridge, MA: Harvard University Press.

Wilson, M.W. (2009). Cyborg geographies: towards hybrid epistemologies'. *Gender, Place & Culture* 16:5, 499-516.

Zook, M.A., & Graham, M. (2007). Mapping DigiPlace: Geocoded Internet data and the representation of place. *Environment and Planning B: Planning and Design* 34, 466-482.

Zickuhr, K. & Smith, A. (2012). Digital differences. *Pew Internet & American Life Project*. Retrieved from http://pewinternet.org/Reports/2012/Digital-differences/Main-Report/Internet-adoption-over-time.aspx

Autobiographical Statement

Gregory T. Donovan is a researcher, educator, and activist who focuses on young people's everyday development within proprietary ecologies of information. His aim is to make the world a more just and equitable place for young people to grow. Gregory holds a B.A. in Psychology from Marymount Manhattan College, a M.A. in Psychology from Hunter College, and a Ph.D. in Environmental Psychology from the Graduate Center of the City University of New York. He is a founder of the OpenCUNY Academic Medium, a member of the Journal of Interactive Technology and Pedagogy's Editorial Collective, and a researcher at the Public Science Project. His doctoral studies were generously supported by two CUNY Doctoral Student Research Grants (Competition #3 and #5), the Presidential Research Fund, the Leanne Rivlin Scholarship Fund, as well as through fellowships at the Macaulay Honors College, the Center for Place, Culture, and Politics, the Provost's Office of the CUNY Graduate Center, and the Stanton/Heiskell Center for Telecommunications Policy. Raised in Massachusetts, Gregory moved to New York City at eighteen and still calls it home. He can be found at http://gtdonovan.org.