Article

Empowerment: Analysing Technologies of Multiple Variable Visibility

Ariane Ellerbrok

University of Alberta, Canada. ellerbro@ualberta.ca

Abstract

This paper notes the emergence of technologies of multiple variable visibility – that is, technologies that render individuals visible to diverse interests simultaneously via the corporate ownership of intimate personal data generated in a peer-to-peer information context. Focusing on Facebook, a classic example of technology of this genre, I argue that the various levels of visibility that are facilitated by these technologies cannot and should not be analysed in isolation from one another. The complex dynamics of power that are mobilised via the strategic employment of multiple visibilities complicates the typical representation of Facebook and other surveillance technologies of its ilk as one-dimensional conduits for either empowerment *or* exploitation. Rather, in the context of these technologies, I argue that visibilities (plural) facilitate combined experiences of empowerment and disempowerment, a process that not only speaks to the type of data collection enabled through this process but also implies a whole series of implications specific to their use.

Introduction

Surveillance technologies are increasingly embedded in the minutiae of our daily lives, tracking our more significant activities such as movement across national borders and through the healthcare system, as well as our seemingly innocuous activities such as our debit and credit purchases, our online surfing habits, and even our personal communications via mobile phone, email, and online social networks. In a report prepared for the UK Information Commissioner, Murakami Wood et al. (2006) declare that we are now living in a ‘surveillance society’ where massive surveillance systems underpin our everyday activities. While many of these systems may seem harmless enough, others – and especially those relating to national security – have attracted the attention of critics who argue that their unmitigated use conflicts with constitutional safeguards (Andrejevic 2007; Lyon 2007). This has raised the question of exploitation, and whether the expansive and largely unregulated creation of information databases may enable social sorting along lines of socio-economic status, ethnicity, religion, or political affiliation. DNA databanks (Nelkin and Andrews 1999), Face Recognition software (Introna and Wood 2004; Gates 2006), and internet dragnets (Andrejevic 2007) have all been criticised along these lines, as have select communication technologies such as online social networks (Wills and Reeves 2009).

Despite the widespread concern over the risks associated with our continually expanding surveillance systems, there is one feature of their development that has posed a theoretical hurdle for many surveillance researchers: if it is the case that individuals are unwilling cogs caught up in a giant surveillance wheel that operates against their best interests, how do we account for the fact that often individuals *willingly choose* to use those technologies identified as exploitative? This willingness to adopt the latest and greatest

technology on the market despite invasiveness has the unfortunate habit of undoing the tidy claims of disempowerment made by surveillance researchers and civil libertarians alike. So what are we to make of this anomaly? Is this a case of false consciousness – where individuals naively believe that the technologies that disempower them are somehow to their benefit – or is there something more at work here?

This question has manifested in the form of a debate in surveillance and technology studies. In an effort to explain the paradox presented by the willing use of supposedly exploitative technologies, some have argued that perhaps surveillance technologies are not *always* necessarily exploitative, but instead might be viewed as empowering those who use them (Koskela 2004; Albrechtslund 2008). If individuals are presumed to be rational actors, then this explanation ought to make the most sense. Thus the question has become: can surveillance technologies be viewed as having the potential to empower those who are ‘watched’? Or put another way, as an individual is made increasingly *visible* through their exposure to surveillance, is this visibility fundamentally exploitative, or might a person turn it to their own ends? The internet, web blogs, online social networks, and mobile phones all come to mind here, where increased visibility may allow for the “building of self as brand” (Senft 2008:8) and other forms of identity empowerment (Zhao et al. 2008).

The relationship between visibility and power is central here, and the question of empowerment is fundamental. This debate follows on the heels of a shift in mainstream representations of surveillance more generally, from the omnipresent Big Brother of 1984 to the increasingly benign images of pleasurable consumer technologies with which we are now so familiar (Andrejevic 2004). But behind the celebratory clamour of media advertisement remains the question: what, exactly, are the dynamics of power when it comes to surveillance technologies? Lyon summarises the position of many when he notes that in practice, surveillance usually involves “relations of power in which [the] watchers are privileged” (2007, 15). While this assumption still underpins much surveillance studies research, it is this very premise that comes under fire via claims to technological empowerment.

In this paper I take the question of visibility as a starting point to interrogate the dynamics of power in online social networking. I choose this particular technology over many others that seek to increase user visibility because it has recently become the focus of the empowerment debate, serving as the shining star for many surveillance-empowerment claims. Media representations in particular tend to divide themselves according to this question of power, arguing that online social networks either i) benefit individuals in their interactions with others, facilitating identity empowerment, or alternatively that they ii) pose a substantial privacy risk to those who post their personal details in a public forum, thus exploiting individuals for financial gain. While this polarisation is primarily characteristic of media representations of online social networks, scholars have also struggled to place these technologies in relation to their tendency towards empowerment/disempowerment.

In this paper I rethink this debate. My underlying premise is that there are multiple levels of visibility at work in online social networks, rendering even the most well-meaning dispute unnecessary, for these various levels of visibility interact in ways that preclude one-dimensional characterisations of either empowerment or exploitation. When accessing an online social network, individuals are made visible in a number of different ways simultaneously, and these forms of visibility interact with one another. First, they are made visible to one another; Katie can see her friend Judy, and vice versa. Second, individuals are made visible to marketing interests, to those corporations and data warehouses that collect and aggregate data from social networks and use them for consumer research or targeted marketing. Third, there is the prospect of regulatory visibility, given that online social networks are increasingly the focus of law enforcement investigations and security dragnets. And finally, the fourth level of visibility produced in online social networks relates to ‘function creep’, or the open ended potential for the data to be used in a number of unforeseen ways down the line. These various levels of visibility preclude a simplistic

identification of online social networks as either empowering or disempowering, for the multiple variable visibility at work on these sites may enable many combinations of each at once. As such, power in online social networking is not uniform or homogeneous, for, depending on the level of visibility that we look at there will be a very different dynamics of ‘watching’, and quite different experiences of power.

To think through some of the dynamics of multiple variable visibility I focus on Facebook¹, a website that dominates the online social networking scene. While Facebook is often presented in glowing terms, or alternatively as a corporate villain intent on obliterating our last remaining shreds of privacy, I argue for a storyline that emphasises the interaction between these conflicting facets. Due to the multiple realms of visibility at work on the website, Facebook enables the simultaneous experience of empowerment and disempowerment to its members, often in unexpected combinations. This multiplex of power is *a key characteristic of the website* that has important implications for the long-term trajectory of Facebook use and Facebook data. And this dynamic is also intentional – it is a formula for disclosure carefully designed by and operating in the interest of the social networking industry. The nuanced dynamics of power that flow through technologies of multiple variable visibility encourage the increased disclosure of individuals, supporting the profit logic of the venture as well as a cultural shift toward a transparent populace more generally. However, while I choose to focus on Facebook in order to provide an example of multiple variable visibility at work, the implications go beyond that of the website itself, and indeed beyond online social networking. Rather, it points to a shift in surveillance technologies more generally, highlighting the development of an industry-wide formula that relies heavily on the use of multiple variable visibility to facilitate the profitability of individual disclosure. This disclosure clearly benefits the industry that seeks it out, but the benefits to individual members are much less clear, as will be elaborated in this paper.

To consider how multiple variable visibility works, I first provide a brief overview of Facebook’s development and popularity. Following this, discussion is organised according to the various levels of visibility attributable to Facebook use, and aims to tease out the dynamics of power that operate in each domain. This includes peer-to-peer visibility, marketing visibility, regulatory visibility, and visibility in the context of ‘function creep’. I conclude by considering how these dynamics operate in tandem, and how they may present us with a picture that is useful for theorising emerging methods of surveillance on a broad scale. Ultimately, each of these framings presents their own issues, and allow us to think through some of the potential long term implications of Facebook’s extreme popularity, but they also allow us to work through some of the implications of multiple variable visibility more generally as they may apply to other technologies currently on the market.

Facebook: A Brief Overview

In the early 2000s² online social networks emerged as a popular tool for socialising on the internet, and millions of individuals integrated them into their daily lives (Boyd 2007; Gross and Acquisti 2005). The extent to which they have been adopted suggests their use has become nearly ubiquitous within certain populations, fostering “new relations of information exchange” amongst family members, friends, co-workers, and even romantic partners (Trottiend, 3). In 2004 Facebook came on the scene, competing with networks such as MySpace and Hi5. Developed by American undergraduate Mark Zuckerberg (Sanchez 2009), the website was initially intended for Harvard students, but quickly spread to other campuses throughout the United States (Phillips 2007). As early as 2007, research on undergraduates at Michigan State University found that 94% of their undergraduate sample were registered on Facebook (Ellison et al. 2007). This was followed by growth amongst non-university demographics, initially focused on young adults, but that now includes the 35-54 age group (Facebook Statistics a 2008; Nielsen ratings 2009).

¹ Facebook: <http://www.facebook.com>

² The first recognizable social networking website was launched in 1997, called SixDegrees.com (Boyd 2007). As a social development however online social networking only began gaining momentum in the early 2000s.

As Facebook has shifted toward mainstream use it has gone global, becoming one of the most heavily trafficked websites (Facebook Statistics a 2008) as well as the most popular online social network worldwide (Nielsen ratings 2009). Overall the network has 500 million active members (Facebook Statistics c 2010), a statistic that I have had to change numerous times over the course of writing this paper. It has spread from its initial base in the United States to countries all over the world, with the notable exception of large parts of China, where its use has recently been blocked (MacDonald 2009), as well as Syria, Vietnam, and Iran, where access is reportedly intermittent at best (Damascus 2007; hamsaweb.org 2007; Marsh 2009). While Facebook membership is largely concentrated in the United States (with over 100,000,000 active users), and other 'western' countries such as the UK and Canada (claiming more than 22,000,000 and 14,000,000 active users respectively) (Burcher 2009), it has recently begun targeting smaller 'developing' countries in the hopes of expanding its readership (BBC News 2009b).

Facebook is primarily an internet-based communication technology, but it also operates as a space for personal entertainment. Upon registering with the network, members create a community of 'friends' where users can access one another's personal profiles and communicate (Boyd 2007). As part of this communicative venture individuals list detailed personal information about themselves, chat via the 'wall' or private messaging, post and 'tag' one another in photos (creating a link to the friend's page), and even play interactive games on the Facebook interface including Scrabble, Farmville, and Mafia Wars. The average user logs almost an hour a day on the Facebook interface (Facebook statistics b 2009), and 25% of active users access their profile through mobile phone (Facebook Statistics b 2009). These individuals are said to be twice as active on the website, and consequently new mobile devices are being introduced to exploit this rapidly expanding market (BBC News 2009a). These developments speak to the extent to which the network has been taken up as a routine part of individuals' daily lives, particularly in the US, UK and Canada.

Central to the popularity of the network is the lack of membership fees – access to Facebook is 'free' in the sense that what people give in return for their membership is not a direct cash payment, but rather data regarding their preferences and daily habits. The financial structure of the website is based on advertising revenue (Phillips 2007) and the sale of this aggregated data. The interface serves at least partially as a platform for advertising, with product endorsements specifically tailored to each user based on their self-entered profile information (gender, age, interests, etc.), as well as on keyword searches of items posted to their page. It also serves as a venue for collecting consumer data of considerable value. Both targeted marketing and this data collection are enabled by the proprietary nature of the website – upon registration individuals are asked to disclose 'accurate' personal information, and to accept the 'Terms of Use' and 'Privacy Policy' that governs the use of their personal data. Research suggests that a large percentage of individuals do indeed post accurate biographical information, including their name, birth date, contact information (such as an email address, or to a lesser extent sometimes a cell phone number), city of residence, relationship status (often with a link identifying their romantic partner), and in many cases even their sexual, political and religious orientation (Gross and Acquisti 2005; Lenhart and Madden 2007).

Given these characteristics, Facebook operates as a *de facto* surveillance technology, generating a "focused, systematic and routine attention to personal details for the purposes of influence, management, protection or direction" (Lyon 2007, 14). As online marketing research has increasingly turned to this form of 'dataveillance' (Clarke 1991) Facebook has developed a powerful niche, capitalising on its ability to capture the ever desirable 'data double' (Haggerty and Ericson 2000) of its members. How they manage to do so with such success is only partially the focus of this paper. As we shall see, it requires multiple levels of visibility for a venture such as Facebook to succeed, and each of these levels has implications in its own right.

Visibility 1 – Peer-to-Peer Surveillance

The first form of visibility enabled through Facebook use is the one that is likely the most evident to its members. Peer-to-peer surveillance (see also Andrejevic 2005 regarding lateral surveillance) entails a mutual surveillance where individuals willingly participate in using an interactive technology as a way of keeping track of one another. In effect, individuals ‘watch’ one another, and do so with full awareness that they are being watched in return (Albrechtslund 2008). As Andrejevic points out, peer-to-peer surveillance is distinct from the mutual monitoring that has always been common to human interaction specifically because it is mediated by communication technology (2007, 41). Where information gathered through more traditional versions of mutual monitoring (say, by observing your neighbour’s daily activities through your window) tends to degrade over time as memory wanes, the information collected via peer-to-peer surveillance has a more permanent character. Peer-to-peer also suggests a willing involvement in being monitored via communication technology, or what Albrechtslund refers to as “participatory surveillance” (2008). When Facebook is discussed as something that empowers its members, quite often this claim to empowerment is based on an analysis of the peer-to-peer visibility of the website.

Presenting online social networking as a tool for empowerment is rooted in a much larger tradition of celebratory approaches to new technological developments (Winner 1986). The internet, within this tradition, is often portrayed as the great leveller – a space of democratic potential where individuals are provided opportunity to participate in public discussion (Saco 2002). It has also been presented as a tool that enables activities that individuals might not otherwise be capable of in an offline setting, such as connecting with friends and family across geographic distance, participating in group support networks, or researching topics of personal importance (Amichai-Hamburger et al. 2008). Similar celebratory notions often characterise the discussion on webcams, mobile phones, and online social networks (Albrechtslund 2008; Ellison et. al. 2007; Koskela 2004; Senft 2008). The increased visibility that results from using these communication technologies allow individuals to “reclaim the copyright of their own lives” (Koskela 2004, 206) and to “write themselves into being” (Boyd 2007). What is understood to be *enabled* via these technologies, then, is visibility to one’s peers for the purpose of identity management, or in the case of online social networking specifically the ability to create an online presentation of self within a networked community. Individuals are thus empowered to represent themselves to one another in the manner of their choosing, accruing whatever benefits may be associated with this representation.

This speaks to a very specific definition of empowerment, one that highlights the importance of identity politics and the transference of power within *micro-level* power relations. And despite the vigour with which it is now mobilised in relation to online social networks, it is worth noting that this notion of empowerment is relatively new. As Fraser (1997) has noted, definitions of empowerment changed in the late 20th century, marking a shift from the politics of redistribution to a politics of recognition. Within this shift political activism increasingly became focused on the *representation* of minority groups rather than on economic redistribution (Fraser 1997, 31), such that individuals came to view identity politics as a key route to power. This led the way for arguments on technological empowerment, which similarly bypass discussion of socio-economic redistribution and instead conceptualise empowerment as technological enablement for self-representation. Specifically, empowerment is now often conceived of as something that “links the individual and his or her well-being to the wider social and political environment in which he or she functions” involving “mutual help and the creation of a responsive community” to aid in goal attainment (Amichai-Hamburger et al. 2008, 1776-7). Thus, the wider shift of empowerment from redistribution to recognition has paved the way for those who note that internet technologies empower individuals through ‘networking’, contributing to individual goal achievement by virtue of an increased capacity for identity management within a large network of peers. The result of this shift, however, is a series of competing definitions on what it means to be ‘empowered’, with some implying socio-structural change, and still others referencing the politics of identity and interpersonal communication. This definitional shift is important because it is at the root of much of the debate on online social networks.

Examples of this latter, more recent, notion of empowerment proliferate in the research on peer-to-peer visibility. To this end, one of the main arguments regarding the empowering nature of Facebook involves the extent to which individuals use the network to make implicit and explicit identity claims (Zhao et al. 2008, 1824). These identity claims are broadcast within a wide arena of acquaintances – including friends and family, but also colleagues and friends-of-friends – thus facilitating “identity empowerment” (Zhao et al. 2008, 1818) by allowing individuals to craft a desirable online persona that benefits them in their interactions with others. Notably, this identity is not limited to one already recognised in an offline setting, for individuals can also express an idealised identity, or their “hoped for possible selves” (Zhao et al. 2008, 1832). This is done by carefully configuring the photos they display, their listed interests, and other means of self-expression. To the extent that these idealised identities are positive and affirmed by others, they can have tangible rewards. The benefits to this process are at least partly psychological, leading to an increased sense of mastery for many networking members (Albrechtslund 2008); an accomplishment that much psychological and social-psychological literature recognises as positively connected to goal attainment (Amichai-Hamburger et al. 2008, 1778).

Over and above the psychological value of identity empowerment, however, is the impact that this improved identity management may have on an individual’s ability to maintain a large network of contacts as a source of social capital. Drawing on Bourdieu’s notion of the concept (Bourdieu and Wacquant 1992), several studies have found that Facebook use is significantly associated with increased social capital because of the long term social connections enabled by the ‘friends’ feature (Ellison et al. 2007, Zhao et al. 2008). Maintaining a wide network of friendships can have tangible rewards by generating increased access to information and resources in other areas of the individual’s life (Ellison et al. 2007). Further, Facebook can help members nurture close personal relationships and a sense of social connectedness even across geographic distance (Ellison et al. 2007). In so doing, the network allows individuals to establish reciprocal relations of support and contacts they may call on in a time of need.

Some note that this ability to maintain a large network of contacts in addition to the capacity for image management is a powerful combination that may contribute to small scale socio-economic mobility. An example involves the story of a young woman who used her Facebook page to let her online community know about her yoga classes, which then resulted in an economic windfall when the classes subsequently filled up with students (George-Cosh 2007). For those who are on the job market, Facebook networks may have “strong payoffs in terms of jobs, internships, and other opportunities” (Ellison et al. 2007), especially for individuals who have maintained connections with past university acquaintances. One can imagine that the small scale socio-economic benefits could also extend beyond employment opportunities to include the improved ability of an individual to find cheaper housing, or even inexpensive childcare amongst one’s ‘friends’.

That Facebook can empower its members – at least at the level of peer-to-peer visibility and using a very specific definition of what it means to be empowered – is clear. Individuals experience a certain degree of control over their representation of self in combination with an increased network of contacts, providing them with a whole host of opportunities for goal attainment. Thus, the technology can have positive implications for their day-to-day lives, both in terms of their social connections and their psychological state. And while there are some features of peer-to-peer visibility on Facebook where this degree of control is open to question – especially given that individuals do not have complete control over what is actually posted in their personal profiles due to features such as photo ‘tagging’ – it seems that Facebook users negotiate these more problematic features as part of a costs/benefits analysis, choosing to accept momentary losses of control as part and parcel of a larger project of self-representation (Soghoian 2008). By and large, users claim to experience increased peer-to-peer visibility as a source of tangible rewards (Albrechtslund 2008; Ellison et al. 2007; Koskela 2004; Zhao et al. 2008), and thus see themselves as empowered by their use of online social networks such as Facebook.

Given the centrality of peer-to-peer visibility to Facebook's operation, this 'networked' identity empowerment is a key feature of the website, fundamental to our understanding of its success. But the heady glow of technological empowerment notwithstanding, this is only one amongst many of the visibilities facilitated by the network, and as such provides us with only one part of the picture in terms of the larger power dynamics that are at work.

Visibility 2 – Marketing Surveillance

The second form of visibility at work on the website is the big eye of marketing, where Facebook members are routinely made more visible to third-party groups so that these groups may advertise to niche demographics and/or collect aggregated data. This level of visibility, like peer-to-peer before it, is in fact central to the structure of the website, and provides the financial impetus upon which the entire enterprise operates. And yet, while individuals are well aware of the implications of visibility at the level of peer-to-peer, research shows that many Facebook users do not have a clear understanding of the ways that they are made visible to marketing interests, much less the implications (Gross and Acquisti 2005). This has raised the question of meaningful consent in regard to the collection and use of Facebook data (Privacy Commissioner of Canada 2009), and has led some to conclude that Facebook exploits its members (Arrington 2009; Bonneau 2009; Conley 2009).

When Facebook is presented as exploitative, the focus is typically on marketing visibility. The definition of disempowerment mobilised is drawn out of early literature on surveillance as a tool for control, but is tailored specifically to the more recent development of corporate data collection. Thus disempowerment in this arena occurs when an individual loses control over which corporate or business entities have access to their personal information, as well as the purposes to which this information might be put (the growth of telemarketing databases and the routine sale of phone lists present us with rather mundane examples of this process). This notion of disempowerment suggests a process that may occur over an extended period of time, with implications that are neither immediate nor necessarily obvious to those who are subject to data collection. The development of comprehensive information databases means that individuals have little control over the trajectory of their personal data, resulting in marketing harassment (Petty 2000; Goodwin 1991), an increased risk of identity theft (Whitson and Haggerty 2008; Monahan 2009), vulnerability to cybercrime (Acofido 2010) and other harms relating to the corporate mismanagement of information. Thus disempowerment becomes synonymous with infringing on an individual's privacy through the collection, storage and sale of their personal information, where individuals lose control over who has access to their 'data double', putting them at risk of tangible personal (often financial) harm. Such undesirable outcomes can also go beyond personal financial concerns to include the 'identity fixing' that occurs when consumer identities are inscribed onto individual bodies (Gandy 1993; Phillips 2005; Haggerty and Ericson 2006). This process not only inhibits an individual's *personal* identity management, but also inhibits the negotiation or re-imagining of identities amongst entire groups, thereby undermining a potential route to empowerment for marginalised populations (Phillips 2005). Thus the risks associated with increased marketing visibility are recognised as both financial and socio-political. Notably, this conception of power is not limited to micro-level power relations and interactions amongst individuals, but rather includes interactions between individuals and larger institutions. As such, while the peer-to-peer arguments tend to view power as control over data access and presentation as it occurs amongst Facebook friends, when discussing marketing visibility power is instead conceptualised in terms of the control that individuals have (or do not have) over corporate and institutional access to, and use of, their information, as well as corporate control in ascribing identity onto both individuals and groups.

In the context of Facebook specifically, marketing visibility is enabled by one of two processes: by capitalising on members' profile information (such as their self-entered personal data and lists of preferences), sharing this information with third party groups; and also by collecting information about the user and their activities *outside* of the Facebook website. The latter is accomplished by installing cookies

and other tracking technology on Facebook members' computers, or via website integration. These technologies are used to collect information about the individual's purchase patterns, the other websites that they may visit, and miscellaneous data from "newspapers, blogs, instant messaging services" and more (Facebook Privacy Policy nd). Each approach has been the subject of critique by researchers, civil libertarians, and the Privacy Commissioner of Canada (2009), who question the potential for exploitation and the legality of the data collection involved. To this end, the focus has been on several programmes operating via the Facebook interface: Facebook Beacon, the Application Platform, and Facebook Connect. Each of these programmes operates as a mechanism to transmit user information to third party groups, allowing private-interest access to substantial amounts of user data.

Facebook Beacon was launched in 2007, installing cookies on members' computers in order to track their online spending outside of the Facebook interface (Perez 2007). What makes this programme distinct from many other tracking and spyware technologies, however, is what Beacon then did with this information – it *reported* this outside spending back on the individual's Facebook profile as a 'social ad'. Thus when an individual shopped on E-Bay (or in any other participating online venue), Beacon would import information regarding the purchased item back to Facebook interface and post it on their profile, an action that friends would see listed in their newsfeed.³ Notably, this entire process occurred without the knowledge *or* explicit permission of the Facebook member. Many individuals only learned of the Beacon programme when they suddenly discovered that ostensibly personal information regarding their spending had been posted publicly on their Facebook profile. As an advertising platform Beacon was expected to operate as a form of personal recommendation, where if a person sees that a friend has purchased a product, they will be more inclined to purchase the same product themselves. As a marketing tactic, however, Beacon was a stunning failure – one that garnered immediate negative publicity over the obvious invasiveness of the programme.

The strength of this negative response forced Facebook to scale back some of the more noticeable elements of the programme, such as notifying an individual's friends of their online purchases. However, while the broadcasting feature was fairly quickly withdrawn, the *tracking* of members' purchases has continued (Perez 2007) as the corporation has imagined new uses for data collected under the Beacon programme.

Similar to Beacon in intent, if not form, is a second feature of the Facebook interface that renders individuals visible to marketing interests: the Application Platform. 'Applications' are a series of interactive games, quizzes, and other activities available to users when they are logged on to the network. They are largely created and run by developers who are not directly associated with Facebook, and who, in return for providing these 'free' games and activities, access certain data posted on the user's profile page. However, while many other social networking websites host applications on their own servers – thus allowing them to control the flow of information and what sensitive data the developers might have access to – Facebook does *not* host the hundreds of thousands of applications they offer on Facebook servers (Kelly 2008). Therefore when a user adds an application to their profile, they are agreeing to the transfer of their personal information to an outside developer on the grounds that some of this information may be required for the application to run (Felt 2007). In so doing, however, the developers have routinely been given access to more data than is actually necessary to run the applications, allowing for substantial abuse of the system (Felt 2007; Soghoian 2008; BBC Newsbeat 2010). While this 'unrestricted access' has been challenged by the Privacy Commissioner of Canada (2009), forcing developers to reveal to users exactly what data they intend to collect, the potential for abuse has remained given the ease with which Facebook

³ The Facebook 'newsfeed' is a feature that pumps a continuous flow of 'news' into a Facebook user's homepage. This can include recent changes to their friends' profiles, photos and albums that have been recently uploaded, upcoming events, upcoming birthdays of 'friends', and more. It is a bit like reading a personalized newspaper, but about your 'friends' lives rather than the lives of strangers.

applications can be developed by almost anyone (Kelly 2008)⁴ and the lack of an appropriate vetting system (Mackenzie 2009), features that have allowed for the development of ‘rogue’ applications where individuals become vulnerable to cybercrime (Acohido 2010).

Moreover, the data collection enabled by the games platform has not been limited to those individuals who actually *add* an application to their profile. Rather, application developers are also granted access to the profile data of the user’s friends. Thus, when your Facebook friend adds an application, that application is able to access your personal data by virtue of your friend having accepting the terms of service on your behalf (Felt 2007; Soghoian 2008). Given that individuals often have several hundred ‘friends’ connected to their Facebook profile (Wills and Reeves 2009; Zhao et al. 2008), this suggests exponential access to personal information such that thousands of applications may have access to an individual’s profile data even if they never added an application to their own page. Unauthorised data flows of this nature are reportedly occurring on an “epic scale” (Bonneau 2009), raising, once again, the question of meaningful consent. Particularly problematic levels of data collection have been connected with the widely popular quiz applications (Bonneau 2009), as well as interactive games like Farmville and Mafia Wars, owned by Zynga, and Pet Society owned by Playfish (Arrington 2009; Langton 2010).

And finally, a third method by which Facebook has increased the visibility of its members to marketing interests involves website integration via programmes such as Facebook Connect. Generally speaking, integration between Facebook and other popular websites means that individuals take their Facebook ‘identities’ with them into other spaces on the internet (Facebook Developers 2010). Thus individuals are saved from the purportedly tedious task of having to re-enter their demographic information every time they wish to interact with a new website, for Facebook shares this information on their behalf with any established partner websites.

The concerns associated with these features are, by now, becoming a familiar story. Meaningful consent has once again been a central issue, for the privacy features associated with the introduction of website integration was initially such that it was difficult for individuals to opt out of having their Facebook data shared with third-party websites they visited (Kincaid 2010). Similarly, the issue of gathering data on an individual’s friends reappeared, so that even if users opted out of the programme, or chose not to visit those websites, the sites could still collect information on them via the Facebook friends who did visit (Kincaid 2010). Predictably, these features generated yet another public backlash (Facebook ‘Millions against’ Petition, nd). Facebook responded to the criticism by withdrawing or altering some of the more contentious Facebook Connect features, while almost simultaneously introducing Open Graph API and social plugins such as the ‘like’ button (Kincaid 2010) which still allow for newer forms of website integration and data transfer between sites, but under another name.

Beacon, the Applications, and the programmes associated with website integration all operate under a similar incentive, to use the data generated on the network as a source of revenue. And while Facebook itself and many other corporations have undoubtedly benefited from this degree of marketing visibility, the benefit to Facebook members is less clear. Users are assured that their information is under their own control (Fb Principles), and yet at the level of marketing visibility this control is clearly undermined. Members have increasingly pressured Facebook to address this worry, but what will come of this pressure remains to be seen; given that the website derives its revenue from marketing sources, it seems unlikely that anything beyond token changes will occur. Indeed, Facebook has a strong economic incentive to ignore these security issues for as long as they are able (Bonneau 2009; Wills and Reeves 2009).

⁴ The position of ‘application developer’ can be assumed by almost anyone with minimal software knowledge. A BBC news article recently revealed that journalists were able to easily write an application and install it on Facebook. They indicated that “Anyone with a basic understanding of web programming can write an application... We wrote an evil data mining application called Miner, which, if we wanted, could masquerade as a game, a test, or a joke of the day. It took us less than three hours” (Kelly 2008).

Given these dynamics, it is perhaps not surprising that many view the Facebook monolith as routinely disempowering its members. In terms of marketing visibility, individuals have little control over who may access their information, regardless of how they configure their privacy settings at the level of peer-to-peer interaction. The programmes elicit information covertly, transferring it to locations outside of the Facebook interface and ostensibly outside of the control of the Facebook members themselves. This raises the question of meaningful consent, as well as the legality of the data transfer occurring on the website (Privacy Commissioner of Canada 2009). For many, it also raises the question of human rights violations – specifically the right to privacy (Conley 2009). Finally, it raises the question of consumer identity fixing, where individuals become envisioned primarily as sources of corporate revenue to the erasure of any other identities they may wish to create – a feature which problematises our earlier arguments on identity empowerment well beyond the recognised risks to personal finance.

Visibility 3 – Regulatory Surveillance

The third form of visibility enabled by technologies such as Facebook is perhaps less evident than the two previously discussed, in part because it is not central to the financial structure of the website. Visibility in the context of regulation and governance implies that individuals are made more visible to groups associated with some level of law enforcement, be it a local police force or government intelligence. While there are an abundance of news reports detailing how information is gleaned from online social networks for use in criminal investigations by police (CBC News 2009a), there is considerably less debate about the extent to which this same information is used by government intelligence agencies following the last decade's 'war on terror'.

Traditionally, regulatory visibility has been discussed within the framework of governance, where the increased scrutiny of a population embodies opportunities for social control, providing some groups with dominion over others. The definition of disempowerment usually mobilised in this realm is similar to that discussed in the previous section on marketing visibility; that is, as individuals are made increasingly visible to powerful interests they are thereby rendered vulnerable to manipulation and harm, a process that may occur over an extended period of time and, once again, may not be evident while occurring. But it is here where the similarities between the two definitions end, for what constitutes *harm* differs substantially depending on the form of visibility discussed. Where for marketing visibility harm was understood to connote marketing harassment, increased risk of identity theft, or vulnerability to cybercrime, at the level of regulatory visibility harm indicates *social sorting* via the discriminatory uses of personal data by members of the state. Through social sorting individuals are categorised in ways that can limit their life chances (Lyon 2003b), where designation along the lines of ethnicity, religion, class, and other categories lead to their "cumulative disadvantage" (Gandy 2006, 331). And while social sorting can occur in many venues, such as marketing campaigns (Gandy 1993), its implications are particularly salient in relation to the state use of personal information. In other words, massive electronic databases that collect and store detailed information on the population of a nation state may be used to the detriment of the relatively less privileged members of society, not only because such databases allow for the sorting of privileged from less privileged citizens, but because this sorting can then result in their differential treatment. Historically this kind of state coordinated social sorting has included racial profiling, economic impoverishment, restricted mobility, and in some cases even the bodily harm and death of marginalised members of the population (Bowker and Star 2000; Gillom 2001; Gandy 2006; Haggerty and Ericson 2006; Los 2010; Lyon 2003b; Lyon 2007; Lyon 2009; Minnaar 2010; Nelkin and Andrews 1999). In its extreme form, the increased visibility of populations for state regulation has allowed for the complete subjugation of marginal populations – as demonstrated during apartheid and the Holocaust (Bowker and Star 2000; Black 2002). As a consequence, increased visibility to the state has long been held suspect by those who recognise the potential abuse of power that it enables. While a certain degree of population visibility is necessary for the administration of a nation state, allowing for democratic processes such as voting and

delivery of benefits (Lyon 1994), when taken to extremes such visibility is often characterised as disempowering to the extent that it is historically connected with the subjugation of marginalised groups.

Fears of totalitarianism notwithstanding, the reality is that we are seeing a surge in interest when it comes to tracking the identities and daily activities of large swaths of the population. That online social network data could be targeted by regulatory surveillance becomes increasingly likely given the substantial changes in surveillance culture over the last decade. Following 9/11 and the subsequent ‘war on terror’, the US, UK, and many other countries saw radical policy changes relating to both policing and national security. Most notable among these was the introduction of the *Patriot Act* in the United States – legislation that was pushed through congress within a week of 9/11 in order to significantly loosen the legal restrictions on electronic surveillance (Lyon 2007; Whitaker 2006). The *Patriot Act* and similar policies have changed the face of surveillance dramatically, allowing for entire domestic populations to come under increased scrutiny as a matter of routine, often without the constitutional safeguard of warrants or other legislative oversight (Andrejevic 2007; Lyon 2003; Lyon 2007; Whitaker 2006). This has led to a massive expansion of government surveillance across the board, not least of which involved the development of giant spin off industries that have produced a seemingly unending supply of new cutting edge monitoring technologies (Andrejevic 2007; Haggerty and Ericson 2006; Lyon 2007; Whitaker 2006). Thus the changes during this era were twofold, involving increasingly invasive levels of surveillance over domestic populations as well as the creation of new surveillance technologies for which there would have been little market before the events of 2001.

What this shift toward routine surveillance means is that internet data in particular has, in recent years, become the focus of government security dragnets. Search engines (such as Carnivore, deployed before 9/11) trawl through internet data and use key word recognition to scan emails, blogs, online purchases and other information in the hopes of flagging conversations or activities that may be of interest to government intelligence (Whitaker 2006). When an individual is flagged, automated algorithms are then employed to assess their probability of risk, a process which may eliminate them as a potential suspect or prompt further investigation. Security dragnets differ from traditional law enforcement activities because while traditionally officials would need to have a particular suspect in mind before they could acquire a warrant providing access to their communication data, in the case of security dragnets terrorism suspects are instead *generated* by sifting through the data of the population wholesale (Andrejevic 2007, 176-7; Lyon 2003). Within this framework the intimate and comprehensive data generated by online social networks becomes a particularly valuable resource (Albrechtslund 2008). Some note that sharing personal details in this type of venue may be akin to creating a government dossier on oneself, where any reference to deviant activity could trigger an investigation (Andrejevic 2007, 176-7). Indeed, the director general of the UK’s MI5 intelligence service, Jonathan Evans, recently commented on the need for the agency to hire those with the relevant IT skills for navigating online social network data (Kisiel 2010). And in the United States, the Electronic Frontiers Foundation recently filed suit against a number of government agencies for refusing to disclose their policies relating to the collection and use of online social networking data (Wayne 2010). These developments go hand in hand with changes in national security research more generally – in particular the renewed focus on ‘social network analysis’ in the years since 9/11, where online social networks such as Facebook and MySpace have been explicitly identified as relevant to the development of new prediction models that aim to identify decentralised terrorist networks (Ressler 2006).

The potential use of online social network data for these purposes requires a reconsideration of the power dynamics of visibility on websites such as Facebook. Databases generated by Facebook include an almost stunning amount of information on each member, including self-entered profile information such as name, birth date, university attended, discipline of study, favourite books, political views and religion, and even photos that are in many cases “suitable for direct identification (61%)” (Gross and Acquisti 2005). It also includes data beyond that which an individual has chosen to make public, such as ‘tagged’ photos and videos of an individual posted by friends. Finally, the database includes information derived from outside

the Facebook interface, including purchasing patterns, the websites they visit, their instant messenger conversations, and even data collected from blogs and newspapers (Facebook Privacy Policy nd). That an individual could become a terrorism suspect based on this kind of information is a chilling prospect, especially given the lack of transparency regarding the automated algorithms used to flag potential suspects. Exactly what might be flagged here? Ethnicity, religion, and political views are perhaps the obvious categories, especially given the increased attention to Muslim groups following 9/11 (Haggerty and Samatas 2010). History also tells us that an individual's academic discipline (Lyon 2007, 19), or even the books they read (Whitaker 2006, 153) can be deciding factors that lead to an individual being targeted by government intelligence. And data on one's 'friends' is also not likely to escape scrutiny, for the old adage 'guilty by association' takes on a whole new meaning in the context of online social networks (Wills and Reeves 2009), where relations are mapped out and identified complete with commentary on how an individual knows each person. Indeed, news reports suggest that friendship networks on Facebook have already come to the attention of certain political regimes, with Canadian journalist Maziar Bahari claiming to have been tortured in Tehran by Iranian officials who, among other things, asked about his Facebook friends (Hammer 2009).

For many, the possibility that online social networks have become fodder for government intelligence in the 'war on terror' is, after all, old news (Andrejevic 2007; Albrechtslund 2008). Realistically, it would be surprising if the data was *not* being used for this purpose. Albrechtslund (2008) even goes so far as to argue that the government collection of online networking data is unproblematic, for "[p]eople themselves are publishing this information in question, free for all to see and collect". This argument is of course deeply problematic in the context of Facebook privacy settings, where individuals believe they have more control over their information than they actually do, leading them to share intimate personal information they may never have intended to share outside of their 'friends' (Ellison et al. 2007; Gross and Acquisti 2005). His argument also misses a fundamental point regarding the regulatory visibility of online social networks: the issue has never been whether the information is easily available, but rather the contextual uses to which this information might be put (Nissenbaum 2009) – especially in circumstances where the categorisation of the data may be discriminatory, leading to the disproportionate allocation of life chances.

Another critique of regulatory visibility in relation to security dragnets involves the question of democratic oversight. Not only does scanning internet communication data wholesale potentially violate the old adage of 'innocent until proven guilty', but it also contributes to an asymmetric visibility between population and state. Given that the actions of citizens are made more visible while the actions of the state are made less so, the question remains whether this type of scrutiny violates constitutional rights (Andrejevic 2007, 259). This is especially problematic because the extent to which security dragnets are being used is unknown – the American *Patriot Act*, for example, prohibits internet service providers and other data sources from sharing information on government monitoring (Haggerty and Ericson 2006, 10). It is also exempt from the Federal Freedom of Information Act, suggesting that while the government's surveillance capabilities have been expanded, political accountability is severely reduced (Andrejevic 2007). Thus while data retention policies are an increasing concern (Mitrou 2010) citizens often have little say in whether, or even knowledge of the extent to which, their data may be being used for these purposes. And given the number of false positive identifications associated with many surveillance technologies (Saetnan 2007), it is increasingly likely that innocent individuals will be targeted, some of whom may then be placed on 'watch lists' with serious implications for their life trajectory.

While it is clearly beyond the scope of this paper to discern the extent to which intelligence agencies use data collected through the Facebook interface, or through any other online social network, their doing so is in keeping with everything that we know about the intentions and capabilities of our intensified surveillance culture following 9/11. Given the intimacy of the data collected, most of which is subject to the verification of an individual's closest friends and colleagues (Wills and Reeves 2009), not considering online social networks as a resource in the 'war on terror' would be nothing short of an incredible

oversight on the part of intelligence agencies, whose purview is pre-emptive surveillance of the population for the purpose of identifying potential threats. Given this orientation, it is vital to contemplate regulatory visibility among the categories of multiple variable visibility, for this form of visibility is increasingly relevant for emerging communication technologies in the years since 9/11. The potential for social sorting is too great, and the dynamics of power too complex, for this level of visibility to be ignored.

Visibility 4 – Data Legacies

In the multiple variable visibility generated by Facebook, the final form of visibility for consideration concerns the open-ended possible uses to which the data could be put at any point in the future. This obviously treads into more speculative terrain, but given the proprietary nature of the data generated on Facebook, and the possibility that it be sold for any number of purposes with little available recourse from the individuals involved, any serious consideration of the technology (or others of multiple variable visibility, for that matter) must attend to the question of how the data is likely to be used long-term.

Here the operation of ‘function creep’ becomes central. Function creep refers to the process whereby “devices and laws justified for one purpose find new applications not originally part of their mandate” (Haggerty and Ericson 2006, 18; Innes 2001), which can lead to new and unforeseen uses for already established technological systems. Sometimes also referred to as ‘surveillance creep’ in the context of surveillance technology (Marx 1998), the dynamics of these new uses are limited only by human imagination, funding initiatives, and shifts in public policy. And while an old technology being put to new unforeseen application is not necessarily a bad thing, it is particularly vital to contemplate the negative aspects of this process given that the ‘creeping’ nature of these new developments often mean that they are not subject to rigorous public scrutiny or political debate. While unforeseen new uses for a given system can empower individuals, they can also (and often do) conflict with basic human rights.

Research shows that when information systems are put to new use, new forms of abuse often follow that seriously impact marginal populations (Gandy 2006; Michael and Michael 2006; Nelkin and Andrews 1999). Databases become an opportunistic grab bag for those who may envision new applications and opportunities for profit, with DNA databanks (Nelkin and Andrews 1999), census data (Michael and Michael 2006), and commercial data brokers (Hoofnagle 2004) providing only a few examples of how this process works. When new uses are envisioned for an existing technology or data set, there follows a common pattern whereby “legal restrictions are loosened and political promises are ignored” (Haggerty and Ericson 2006, 19) as enthusiasm and investment in the new system builds. In the case of information technology, this often involves a violation of “contextual integrity” where information is taken out of one context and used in another that may be deemed inappropriate by, or harmful to, the individuals from whom it was originally collected (Nissenbaum 2009). For information technology, then, the task becomes one of imagination, envisioning the potential uses to which data might be put down the line — considering not only who would benefit from each use but also who is likely to be harmed in the process. This is particularly vital with Facebook given the speed with which it mutates, continually adding and modifying functions.

Given the comprehensive nature of the data collected on Facebook, its proprietary nature, the expanding market for information more generally, and the location of its corporate headquarters in a country with little legislative oversight of the data collected in online social networks, it follows that the potential for function creep is quite high. There are many possible routes that Facebook function creep might take, each requiring further consideration and debate. Some of these will be new, while others may intensify the forms of peer-to-peer, marketing and security surveillance mentioned previously.

It might seem the stuff of television fiction to contemplate a scenario where online social networking data is used to restrict the mobility of some individuals across national borders, for racial or religious profiling,

or to generate terrorism suspects. That an individual might be identified, detained and tortured on the basis of information gleaned from a social network might seem even more surreal, unless we recognise the flimsy nature of information used in recent official instances of rendition and torture. Given the sense of surreality that characterises these scenarios, it is worth considering another possible use for Facebook data that may help place the issue of function creep into perspective. Here I consider the opportunistic use of Facebook data by insurance companies, something that is already occurring on a comparatively small scale, but which has the potential to expand exponentially.

Consider the following: a colleague of mineworkers for an insurance company, and uses the typically low peer-to-peer privacy settings of Facebook profiles to monitor individuals who have made insurance claims. He looks on their profile for evidence of a fraudulent claim (such as photos of an individual out dancing when they have claimed benefits due to a back injury), or for clues about where the person spends their time so that he may conduct more hands-on surveillance. When he finds potential evidence of fraud, or of an activity that might otherwise support denial of the claim, he turns it over to his employer. While this might seem like an isolated venture, it is becoming increasingly common for insurance firms and workers compensation boards to use Facebook data in order to investigate an individual's eligibility for payout (CBC News November 21 2009; Gallagher 2008; Cenicerros 2009; Kelner and Kelner 2009).

While we might sympathise with the right of insurance companies to seek out evidence of fraud, or chastise individual users for not configuring their privacy settings so as to preclude insurance companies from monitoring them by virtue of peer-to-peer access to their profiles, such responses miss the larger point of this scenario – which involves the ways in which Facebook promises to transform a whole host of institutional routines and investigative practices. Evidently insurance companies are already viewing the information generated by Facebook as an invaluable source for profitably conducting business. Investigations that might have been cost-prohibitive in previous years (following an insurance claimant around and video taping their daily activities is expensive!) become, with access to Facebook data, profitable to conduct on a much larger scale, allowing firms to gather more data on claimants and potential customers alike. So much so that an entire industry of online investigators has sprung up to capitalise on internet data, and in particular online social networks, selling their investigative services to the insurance industry (Cenicerros 2009). Given this development, and the financial incentive for the industry to manage profit margins by reducing payouts as much as possible, it is entirely possible that at some point in the not too distant future insurance firms will begin purchasing (or otherwise accessing) the data generated by Facebook on a broad scale, bypassing the peer-to-peer privacy settings and instead accessing the data at the level of marketing visibility. If this were to occur, the implications of function creep would become decidedly less abstract for many individuals. In the United States specifically, where the acquisition of quality health insurance plays a key role in whether an individual is able to access life saving medical services, wide scale access to Facebook data by insurance companies could have disastrous consequences, such that individuals could be refused health coverage on the basis of information that has been posted in their Facebook profile (either of their own accord, or by their 'friends').

Equally problematic is the possibility that insurance industry access to Facebook data might lead to differential rates of insurance based on the cached details of one's profile, such as an individual's purchase preferences, their explicitly stated hobbies, status updates, and even the implicit bits of information found in comments and photos posted by friends. Information that will likely be of interest to potential insurers might include evidence of routine alcohol consumption (photos of partying, for example), participation in high-risk sports, and even any indication of one's sexual orientation (see Chin-Wen Li 1996 regarding the routine denial of insurance coverage for those suspected of homosexuality or bisexuality). Just as DNA databases are attractive to insurers for their presumed potential to predict long term health problems (Nelkin and Andrews 1999), so too might Facebook data be viewed in a similar light, potentially leading to cost-prohibitive insurance rates for those who are deemed to have 'risky' or 'unhealthy' lifestyles. Thus the consequences of Facebook data for those seeking insurance could involve the denial of coverage

altogether, denial of benefit payout or even cost-prohibitive rate setting. It should go without saying that already vulnerable populations are the ones who are most likely to bear the brunt of their data being used for this purpose – with the most dire consequences targeting those of lower socio-economic status.

Such a use for Facebook data may seem an unlikely development to some, but we would do well to remember that intimate personal data has a long shelf life (Mayer-Schönberger 2009), and that Facebook reserves the right to change its ‘Privacy Policy’ or its ‘Terms of Use’ at any time, as it sees fit (Facebook Privacy Policy nd). Furthermore, the data passes through many hands once it moves beyond the Facebook interface, rendering any assurance that it will not be used for a particular purpose highly problematic. That many different groups might have an interest in the data is already clear. Beyond law enforcement and intelligence agencies Facebook data has also made inroads into the American judiciary system, and is routinely collected by lawyers (sometimes by unethical means, such as creating a fake profile and then ‘friending’ the relevant individual) in order to use the intimacies posted on Facebook to defame defendants in divorce and custody settlements (Kelner and Kelner 2009). The use of Facebook data by employers to assess potential applicants has also been widely documented, with some requiring access to an individual’s Facebook profile as a part of the application process (Gouras 2009; Marco 2009). It may only be a matter of time before insurance companies implement similar provisions, or go about accessing wide swaths of cached Facebook data of their own accord, and regardless of whether the data is presumed to be on lockdown via privacy settings.

The scenarios for Facebook function creep are many (see Wills and Reeves 2009 for a detailed consideration of the potential for electioneering, for example). Given the proprietary nature of the data and the wealth of those industries that might see fit to use it, it can (and will likely) be used for any number of purposes that will go against the interests of those individuals who have made online social networks such as Facebook a part of their daily lives. This is particularly probable given that many of the industries that are apt to view this data as a valuable resource (such as commercial data brokers, the insurance industry, etc.) are high-profile corporations with lobbyists in key political arenas. That such a development might reinforce the lot of marginalised populations while simultaneously contributing to the wealth of major corporations requires us to consider social networking data for what it is – a highly sensitive political bounty.

Admittedly, all such future uses are at this point speculative, and necessarily so. In order to grasp the significance of technologies such as Facebook it is vital to contemplate not only how they are currently being used, but also the forces that are apt to push future use of their data in particular directions. While this may be difficult to foresee, it is a critical task given that new applications for social networking data may increasingly shape the life chances of various populations. The data legacies involved include the long-term visibility of Facebook members, with implications that are distinct from, yet largely reliant on, the previous forms of visibility discussed.

Multiple Variable Visibility – Visibilities in Tandem

Gloomy scenarios notwithstanding, it is clear that multi-faceted technologies such as Facebook involve so much more than the simple exploitation of individuals. It is here where we return to the initial concern highlighted in this paper, the role of ‘empowerment’ in understanding surveillance technology – especially in the context of those technologies that facilitate multiple variable visibility.

Empowerment is a tricky concept, but it is also one that has serious implications for how we understand the technologies around us, and which of those technologies we choose to make part of our daily lives (Winner 1986). While traditional notions of empowerment might have focused on an individual’s ability to foster socio-structural change and redistribution of wealth, more recent notions of empowerment instead champion an individual’s ability to manage their identity, and to have that identity realised via the

acknowledgement of others (Fraser 1997). This concept of power clearly fits within a larger shift towards a 'consumer democracy', where constitutional notions of freedom and democratic participation have become watered down into a perceived right to consumer choice (Andrejevic 2007). In this frame, to have access to a large network within which an individual can negotiate their identity, enabled via access to new consumer technology, is to be empowered. For Fraser, however, this shift towards identity politics – and the consumer self-expression that it implies – has undermined the ability of many groups to lobby for socio-economic change. In shifting focus to the need for recognition, the goal of redistribution is quite often left to the wayside (Fraser 1997, 31).

This suggests that when we focus on the networking empowerment associated with new technologies of multiple variable visibility, what is often left behind are deeper questions regarding the potential for the same technology to facilitate socio-structural discrimination. When empowerment becomes conceptualised as the ability to control one's representation of self within a large network of acquaintances, we ignore the fact that individuals are not only interacting with their friends and family via these technologies, they are also interacting with larger institutions such as corporations and the state. To this end, mobilising claims to empowerment may miss, or even obscure, larger questions about how these technologies may facilitate specific kinds of relationships between individuals and institutions. Speaking in the language of empowerment may actually work to conceal relations of exploitation (Pease 2002).

When Facebook is hailed as an empowering technology it is done using this relatively new definition, while simultaneously focusing on peer-to-peer visibility to the exclusion of the other visibilities generated by the network. So what are we to make of this claim, given the competing assertions that this same technology exploits its members? Beyond peer interactions, at the levels of marketing and regulatory visibility individuals are very clearly disempowered. What's more, via function creep members lose control over who has access to sensitive personal information on a grand scale, suggesting that regardless of the outcome of this scenario they are, here too, disempowered. So which is it, then, are individuals ultimately empowered or disempowered by their Facebook use? Does one conclusion trump, or somehow 'cancel out', the other?

What this paper suggests is that for technologies of multiple variable visibility, discussions about empowerment alone, or even disempowerment alone, are insufficient. For these emerging technologies there is a complex interaction of many levels of visibility, a process that produces results fundamental to our understanding of how these technologies work. Individuals quite often *experience* social networking technology as empowering, and our contention about conceptual definitions notwithstanding, if they experience it to be so then it is indeed something that empowers them. However they are also exploited by the same technology, often under the radar, and the combination of visibilities produced by this dynamic has important implications for the kinds of data that Facebook is able to collect.

Central to this process is the quest for disclosure. Technologies such as Facebook rely on the disclosure of members to keep the venture afloat (whether explicit or covert, by virtue of tracking technology). Either way, that an individual enables access to the intimate details of their life is central to the operation of the website, and its financial structure. And it is here where the multiple variable visibility of the site comes into play. While individuals are unlikely to subject themselves willingly to the invasive gaze of marketing or regulatory interests *prima facie*, these more contentious forms of surveillance are too often eclipsed by the benefits of peer-to-peer visibility. Thus it is only via the empowerment of peer-to-peer visibility that the associated loss of control over personal information is enabled.

What this means is that the scale of disempowerment that occurs at the level of marketing, regulatory, and long-term visibility is only *made possible* by the very real and tangible empowerment that individuals experience through peer-to-peer interaction. The dynamics of these interactions encourage individuals to 'let their guard down', disclosing information that they may never have intended to reveal outside of their

‘friends’, sharing intimacies that benefit them explicitly in terms of the social capital that shapes their personal relationships. Thus this ‘networked identity empowerment’ becomes the precondition for the collection and sale of unprecedented amounts of intimate data by institutions that operate outside the realm of peer-to-peer visibility. It is a carefully orchestrated system; designed to encourage the willing and *comfortable* revelation of day-to-day intimacies over an extended period of time, explicitly for the financial benefit of major institutions.

That individuals choose to disclose personal information in this type of venue does not suggest some kind of lapse into false consciousness, however. It is not that individuals *naïvely believe* that Facebook empowers them, for in the context of their lived experience, it does. When people claim to be empowered by a technology we should take them at their word. To do any less is to deny how these technologies are legitimately experienced. But we also need to be sensitive to the definition of empowerment that is being employed in order to ascertain this claim, as well as the implications of the multiple axes of visibility involved. Different forms of visibility will have different implications (Brighenti 2007), and while the implications of peer-to-peer visibility are a clear and acknowledged part of a person’s every day use of the technology, the implications of other levels of visibility are instead more covert, and considerably less evident to most users. That an individual might evaluate the costs of their disclosure primarily in terms of the implications of peer-to-peer visibility does not suggest their naivety or lack of sophistication, rather it suggests an unreasonable degree of responsibilisation. In an information culture replete with identity theft and other potentially damaging uses for personal data, members of the general public are expected to routinely monitor the ways in which their information could be exploited, a task that requires a degree of ‘hyper-vigilance’ that is unrealistic for most citizens to maintain (Whitson and Haggerty 2008). In the face of a monstrous market for data this focus on individual responsibility protects the interests of major institutions, who are able to put profit ahead of data concerns, while individuals are simultaneously left vulnerable, further entrenching existing social inequalities (Monahan 2009; Whitson and Haggerty 2008). False consciousness is hardly a useful conclusion in light of this ethos, for individuals are not naïve so much as left unprotected by current data legislation.

Multiple variable visibility must be considered in light of this neoliberal notion of individual responsibility. It is clear that responsibilising individuals – which in the context of this paper might involve educating the public about the implications of multiple variable visibility – is an unrealistic approach to managing the consequences of these new forms of data collection. Rather, change must be solicited at the level of the information systems themselves (Wills and Reeves 2009), requiring legislative oversight of those technologies that facilitate numerous levels of visibility. While online social networks and other similar technologies may have an economic incentive to disempower individuals (Bonneau 2009; Wills and Reeves 2009), this does not mean that there are no alternatives to this scenario.

To be clear, I see multiple variable visibility as an issue that goes well beyond Facebook, pointing to an industry-wide formula employed to solicit increased disclosure. While Facebook may have introduced new dynamics to the online collection of intimate data, other internet and communication venues are developing a similar surveillance agenda in its wake, using peer-to-peer visibility as a draw for facilitating new forms of profit. In assessing these new technologies, visibilities cannot and should not be discussed in isolation from one another, for considering how they interact is vital to creating a broad picture of the power dynamics at work. The outcomes of these kinds of analyses are critical, for claims regarding the empowerment/disempowerment associated with any given business practice can, at critical junctures, facilitate shifts in public policy, thereby impacting the lived experience of millions of individuals.

This analysis also has implications for surveillance studies more broadly. If we wish to reconcile the potential for exploitation with the fact that these technologies are voluntarily used by individuals, we will need to broaden our approach. Empowerment and disempowerment are often mobilised in relation to surveillance practice, but tend to be treated as opposing ends of a continuum, where less of one necessarily

implies more of the other. This does not have to be the case, however, and if anything, is an assumption that works against us when analysing technologies of multiple variable visibility. Just as speaking in the language of empowerment can conceal relations of exploitation (Pease 2002), so too can speaking exclusively in the language of *disempowerment* risk concealing its driving force. Empowerment is becoming, now more than ever, a concept that must be central to our understanding of emerging surveillance technologies. This is the case regardless of how we may choose to define it, for any time that an individual claims to be empowered by a technology they are telling us something worth paying attention to.

It is clear that as a tool for the networking industry, 'empowerment', and indeed multiple variable visibility more generally, are *strategies* that allow the intimate disclosures of citizens to be repackaged as profitable data. And let's make no bones about it, this process renders individuals acutely vulnerable to the whims of major institutions. Historically speaking, the unprecedented degree of population visibility that we are now seeing does not bode well. The minutiae of daily life cached via the Facebook interface (and indeed by other technologies of multiple variable visibility as well) provide ample opportunity for individuals to be categorised on the basis of whatever classification system happens to be organising the perceived threat of the moment, across both time and space. This is a concern we would do well to consider, for if we accept the claim that technological change is an inherently political process (Winner 1986), then it only makes sense for us to interrogate those politics prioritised by an emerging multiple variable visibility.

Acknowledgements

I am indebted to Kevin Haggerty, whose ongoing advice and insightful comments have been central in shaping the development of this paper. Many thanks also to David Murakami Wood, David Phillips and Torin Monahan for putting together this special edition. My thanks to the blind reviewers, who offered constructive suggestions that helped strengthen various sections of my argument. And finally I am deeply grateful to my family and partner, who have provided me with their ongoing support.

References

- Acohidio, Byron. 2010. How Cybercriminals invade social networks, companies. *USA Today*. http://www.usatoday.com/tech/news/computersecurity/2010-03-04-1Anetsecurity04_CV_N.htm [Accessed 09/22/10]
- Albrecht, Anders. 2008. Online Social Networking as Participatory Surveillance. *First Monday* 13(3). <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949>
- Andrejevic, Mark. 2004. *Reality TV: The Work of Being Watched*. Maryland: Rowman and Littlefield Publishers, Inc.
- Andrejevic, Mark. 2005. The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society*, 2(4): 479-497.
- Andrejevic, Mark. 2007. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, Kansas: University Press of Kansas.
- Amichai-Hamburger, Yair, Katelyn Y.A. McKenna, Samuel-Azran Tal. 2008. E-empowerment: Empowerment by the Internet. *Computers in Human Behavior*. 24:1776-89.
- Arrington, Michael. 2009. Scamville. *TechCrunch*. <http://techcrunch.com/2009/10/31/scamville-the-social-gaming-ecosystem-of-hell/> [Accessed 03/20/10]
- BBC News. 2009a. Facebook driving mobile net usage. <http://news.bbc.co.uk/2/hi/technology/8149652.stm> [Accessed 03/08/10]
- BBC News. 2009b. Facebook strips down to Lite site. <http://news.bbc.co.uk/2/hi/technology/8249835.stm> [Accessed 03/04/10]
- BBC Newsbeat. 2010. Claim some Facebook apps pass on personal info on users. <http://www.bbc.co.uk/newsbeat/11565948> [Accessed 10/29/10]
- Black, Edwin. 2002. *IBM and the Holocaust*. Time Warner Paperbacks.
- Bonneau, Joseph. 2009. How Privacy Fails: The Facebook Applications Debacle. In *Light Blue Touchpaper*. Security Research Computer Laboratory, University of Cambridge. <http://www.lightbluetouchpaper.org/2009/06/09/how-privacy-fails-the-facebook-applications-debacle/> [Accessed 06/17/09]
- Bourdieu, Pierre and L. Wacquant. 1992. *An Invitation to Reflexive Sociology*. Chicago: University of Chicago Press.
- Bowker, Geoffrey C. and Susan Leigh Star. 2000. *Sorting Things Out: Classification and Its Consequences*, 195-225. Cambridge, MA: MIT.
- Boyd, d. m., and Ellison, N. B. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1). <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html> [Accessed 12/05/08]
- Boyd, danah. 2007. Why Youth (Heart) Social Networking Sites: The Role of Networked Publics in Teenage Social Life. In *MacArthur Foundation Series on Digital Learning—Youth, Identity and Digital Media Volume*. David Buckingham (ed). Cambridge MA: MIT Press.
- Brighenti, Andrea. 2007. Visibility: A Category for the Social Sciences. *Current Sociology*, 55(3): 323-42.

- Burcher, Nick. 2009. Facebook Usage Statistics by Country. <http://www.nickburcher.com/2009/12/facebook-usage-statistics-by-country.html#comment-5891775836786868733> [Accessed 02/28/10]
- CBC News. 2009a. Facebook crime-boasts help police nab cons. <http://www.cbc.ca/technology/story/2009/07/30/facebook-crime.html> [Accessed 03/29/10]
- CBC News. 2009b. Depressed woman loses benefits over Facebook photos. <http://www.cbc.ca/Canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html> [Accessed 11/21/09]
- Ceniceros, Roberto. 2009. Comp cheats confess all on social networking sites. *Workforce Management*. <http://www.workforce.com/section/benefits-compensation/feature/comp-cheats-confess-all-social-networking-sites/index.html> [Accessed 09/13/10]
- Chi-Wen Li, Katy. 1996. The Private Insurance Industry's Tactics Against Suspected Homosexuals: Redlining Based on Occupation, Residence, and Marital Status. *American Journal of Law and Medicine*. XXII(4).
- Clarke, R. 1991. Information technology and dataveillance. In *Controversies in Computing*, eds. D. Lyon and E. Zureik. San Diego: Academic Press.
- Conley, Chris. 2009. Quiz Facebook: Will We Have Control over Our Own Information?" *American Civil Liberties Union Blog of Rights*. <http://www.aclu.org/2009/08/27/quiz-facebook-will-we-have-control-over-our-own-information> [Accessed 03/30/10]
- Damascus, KhaledYacoubOweis. 2007. Syria blocks Facebook in Internet crackdown. *Reuters*. <http://www.reuters.com/article/idUSOWE37285020071123> [Accessed 03/08/10]
- Ellison, N. B., Steinfeld, C., and Lampe, C. 2007. The benefits of Facebook "friends": Social capital and college students' use of online social network sites. In *Journal of Computer-Mediated Communication*, 12(4). <http://jcmc.indiana.edu/vol12/issue4/ellison.html> [Accessed 12/05/08]
- Facebook Beacon Petition. nd. Petition: Facebook, stop invading my privacy! <http://www.facebook.com/group.php?gid=5930262681> [Accessed 12/09/08]
- Facebook Developers. 2010. Facebook for Websites. <http://developers.facebook.com/docs/guides/web> [Accessed 09/17/10].
- Facebook Factsheet. nd. <http://www.facebook.com/press/info.php?factsheet> [Accessed 03/30/10]
- Facebook Petition. nd. Millions against Facebook's Privacy Policies and Layout Redesign. <http://www.facebook.com/group.php?gid=27233634858> [Accessed 09/16/10].
- Facebook Press Releases. nd. Leading Websites offer Facebook Beacon for Social Distribution: Users gain ability to share their actions from 44 participating sites with their friends On Facebook. <http://www.facebook.com/press/releases.php?p=9166> [Accessed 12/05/08]
- Facebook Principles. 2008. <http://www.facebook.com/policy.php> [Accessed 12/05/08]
- Facebook Privacy Policy. 2008. <http://www.facebook.com/policy.php> [Accessed 12/05/08]
- Facebook Statistics a 2008. <http://www.facebook.com/press/info.php?statistics> [Accessed 12/05/08]
- Facebook Statistics b 2009. <http://www.facebook.com/press/info.php?statistics> [Accessed 06/20/09]
- Facebook Statistics c 2010. <http://www.facebook.com/press/info.php?statistics> [Accessed 09/17/10]
- Facebook Terms of Use. 2009. Statement of Rights and Responsibilities. <http://www.facebook.com/terms.php?ref=pf> [Accessed 06/24/09]
- Felt, Adrienne. 2007. Privacy protection for social networking APIs. <http://www.cs.virginia.edu/felt/privacy/> [Accessed 12/06/08]
- Fraser, Nancy. 1997. From Redistribution to Recognition: Dilemmas of Justice in a "Postsocialist" Age". In *Justice Interruptus*, 11-39. London: Routledge.
- Gallagher, Mary Pat. 2008. MySpace Facebook pages called key to dispute overinsurance coverage for eating disorders. In *law.com*, URL: <http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005559933> [Accessed 09/13/10]
- Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.
- Gandy, Oscar H. 2006. Quixotics Unite! Engaging the pragmatists on rational discrimination. In *Theorizing Surveillance*, 318-36. London: Willan.
- Gates, K. A. 2006. Identifying the 9/11 'faces of terror' - The promise and problem of facial recognition technology. *Cultural Studies*, 20(4-5): 417-440.
- George-Cosh, David. 2007. Facebook users embracing the Marketplace. *The Globe and Mail*. <http://www.theglobeandmail.com/servlet/story/RTGAM.20070705.wgtfacebook05/BNStory/Technology/> [Accessed 12/03/08]
- Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: The University of Chicago Press.
- Goodwin, Cathy. 1991. Privacy: Recognition of a consumer right. *Journal of Public Policy and Marketing*, 10(1): 149-66.
- Gouras, Matt. 2009. US city wants job applicants to hand over passwords for internet groups. *The Associated Press*. http://ca.news.yahoo.com/s/capress/090619/world/us_internet_background_checks [Accessed 06/21/09]
- Gross, Ralph and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks" In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (Alexandria, Va.) New York: ACM, 71-80. <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf> [Accessed 12/05/08]
- Haggerty, Kevin D., and Ericson, Richard V. 2000. The surveillant assemblage. *British Journal of Sociology* 51(4): 605-622.
- Haggerty, Kevin D. and Richard V. Ericson. 2006. The New Politics of Surveillance and Visibility. In *The New Politics of Surveillance and Visibility*, 3-25. eds K.D. Haggerty and R.V. Ericson. Toronto: University of Toronto Press.
- Haggerty, Kevin D. and Minas Samatas. 2010. *Surveillance and Democracy*. London: Routledge.

- Hammer, Kate. 2009. Considering suicide and finding comfort in Cohen, Canadian journalist recalls nightmare in Tehran Jail. *The Globe and Mail: Alberta Edition*. Page 1 and 8.
- hamsaweb.org. 2007. Facebook Faces Censorship in Iran. *Civil Rights in the Middle East Report*. <http://www.hamsaweb.org/crime/4.html> [Accessed 03/08/10]
- Hodgkinson, Tom. 2008. Why you should beware of Facebook. <http://www.theage.com.au/news/general/bewarefacebook/2008/01/18/1200620184398.html?page=fullpage#contentSwap2> [Accessed 12/03/08]
- Hoofnagle, Chris Jay. 2004. Big Brother's Little Helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement. *Int'l Law and Com*, Reg. 595.
- Innes, M. 2001. Control Creep. *Sociological Research Online* 6.
- Introna, L. D., and D. Wood. 2004. Picturing Algorithmic Surveillance: the politics of face recognition systems. *Surveillance & Society* 2(2/3): 177-198.
- Kelly, Spencer. 2008. Identity 'at risk' on Facebook. *BBC News*. http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm [Accessed 12/04/08]
- Kelner, Robert S. and Gail S. Kelner. 2009. Social Networks and Personal Injury Suits. *New York Law Journal: Law Technology News*. <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202434026615> [Accessed 09/13/10]
- Kincaid, Jason. 2010. Senators call out Facebook on "Instant Personalization", other issues. *TechCrunch*. <http://techcrunch.com/2010/04/27/senators-call-out-facebook-on-instant-personalization-other-privacy-issues/> [Accessed 09/08/10]
- Kisiel, Ryan. 2010. MI5 Pensions off spies who can't use IT. *Daily Mail*. <http://www.dailymail.co.uk/news/article-1265219/MI5-pensions-spies-use-I-T.html> [Accessed 09/26/10]
- Koskela, Hille. 2004. Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism. *Surveillance & Society* 2(2/3): 199-215.
- Langton, Jerry. 2010. Is FarmVille the future (of gaming)? *Tech and Gadgets*. <http://tech.ca.msn.com/article.aspx?cp-documentid=23245458> [Accessed 03/08/10]
- Lenhart, Amanda and Mary Madden. 2007. Teens, Privacy and Online Social Networks: How teens manage their online identities and personal information in the age of MySpace. *PEW Internet and American Life Project*. April 18, 2007.
- Los, Maria. 2010. A trans-systemic surveillance: The legacy of communist surveillance in the digital age. In *Surveillance and Democracy*, 173-94. Eds Kevin D. Haggerty and Minas Samatas. London: Routledge.
- Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
- Lyon, David. 2003. *Surveillance after September 11*. New Hampshire: Odyssey Press.
- Lyon, David. 2003b. *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.
- Lyon, David. 2007. *Surveillance Studies: An Overview*, 11-24. London: Polity.
- Lyon, David. 2009. Identification Practices: State Formation, Crime Control, Colonialism and War. In *Technologies of (In)Security*, 42-58. eds K.F. Aas, H.O. Gundhus and H.M. Lomell. London: Routledge.
- MacDonald, Emily. 2009. China's Facebook Status: Blocked. *ABC News*. <http://blogs.abcnews.com/theworldnewser/2009/07/chinas-facebook-status-blocked.html> [Accessed 03/08/10]
- Mackenzie, Iain. 2009. Facebook boss rejects app controls. *BBC Newsbeat*. http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7918000/7918582.stm [Accessed 10/12/10]
- Marco, Meg. June 19, 2009. Applying for a job? Give us your Google and Facebook passwords. *The Consumerist*. <http://consumerist.com/2009/06/applying-for-a-job-great-give-us-your-google-and-facebook-passwords.html> [Accessed 09/13/10]
- Marsh, Vivien. 2009. Vietnam government denies blocking networking site. *BBC News*. <http://news.bbc.co.uk/2/hi/asia-pacific/8370762.stm> [Accessed 03/08/10]
- Marx, G.T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
- Mayer-Schönberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press.
- Michael, Katina and M.G. Michael. 2006. Historical Lessons on ID Technology and the Consequences of Unchecked Trajectory. *Prometheus*, 24(4): 365-77.
- Minnaar, Anthony. 2010. Balancing public safety and security demands with civil liberties in a new constitutional democracy: The case of post-1994 South Africa and the growth of residential security and surveillance measures. In *Surveillance and Democracy*. Kevin Haggerty and Minas Samatas, eds. London: Routledge.
- Mitrou, Lilian. 2010. The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive" In *Surveillance and Democracy*, 127-47. Kevin D. Haggerty and Minas Samatas, eds. London: Routledge.
- Monahan, Torin. 2009. Identity Theft Vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology*, 13: 177-200.
- Murakami Wood, David, Kirstie Ball, David Lyon, Clive Norris, Charles Raab. 2006. *A Report on the Surveillance Society: For the Information Commissioner by the Surveillance Studies Network*. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf [Accessed 10/08/09]
- Nelkin, Dorothy and Lori Andrews. 1999. DNA identification and surveillance creep. *Sociology of Health and Illness* 21(5): 689-706.

- Nielsen Ratings. 2009. Global Faces and Networked Places: A Nielsen report on social networking's new global footprint. http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf [Accessed 09/20/10]
- Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford: Stanford Law Books.
- Pearce, Adrian. 2009. Facebook tweaks site to rival Twitter. *BBC News*. http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7925000/7925441.stm [Accessed 03/27/10]
- Pease, Bob. 2002. Rethinking Empowerment: A Postmodern Reappraisal for Emancipatory Practice. *British Journal of Social Work* 32: 135-47.
- Perez, Juan Carlos. 2007. Facebook's Beacon More Intrusive than Previously Thought. *PC World*. http://www.pcworld.com/article/140182/facebooksbeacon_more_intrusive_than_previously_thought.html [Accessed 12/03/08]
- Petty, Ross D. 2000. Marketing without consent: consumer choice and costs, privacy, and public policy. *Journal of Public Policy and Marketing* 19(1): 42-53.
- Phillips, David J. 2005. From Privacy to Visibility: Context, Identity, and Power in Ubiquitous Computing Environments. *Social Text* 83. Vol. 23(2).
- Phillips, Sarah. 2007. A Brief History of Facebook. *The Guardian*. <http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia> [Accessed 11/28/08]
- Privacy Commissioner of Canada. 2009. *Report of Findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*. Report prepared by Elizabeth Denham, Assistant Privacy Commissioner of Canada. http://www.priv.gc.ca/cf-de/2009/2009_008_0716_e.pdf [Accessed 09/03/09]
- Ressler, Steve. 2006. Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. *Homeland Security Affairs* 2(2). <http://www.hsaj.org/pages/volume2/issue2/pdfs/2.2.8.pdf> [Accessed 09/14/10]
- Saco, Diana. 2002. *Cybering Democracy: Public Space and the Internet*. Minnesota: University of Minnesota Press.
- Saetnan, Ann Rudinow. 2007. Nothing to Hide, Nothing to Fear?: Assessing Technologies for Diagnosis of Security Risks. *International Criminal Justice Review* 17(3): 193-206.
- Sanchez, Andres. 2009. Facebook Feeding Frenzy: Resistance-through-distance and resistance-through-persistence in the societied network. *Surveillance & Society* 6(3): 275-293.
- Senft, Theresa M. 2008. *CAMGIRLS: Celebrity and Community in the Age of Social Networks*. New York: Peter Lang Publishing Inc.
- Soghoian, Chris. 2008. Exclusive: the next Facebook privacy scandal. *cnet News Surveillance State*. http://news.cnet.com/8301-13739_3-9854409-46.html [Accessed 12/03/08]
- Trottier, Daniel.nd. Social Networking Sites and the Emergence of a Ubiquitous Surveillance. Unpublished manuscript.
- Whitaker, R. 2006. A Faustian Bargain: America and the Dream of Total Information Awareness. In *The New Politics of Surveillance and Visibility*, 141-70. eds. K. D. Haggerty and R. V. Ericson. Toronto: University of Toronto Press.
- Whitson, Jennifer and Kevin D. Haggerty. 2008. Identity Theft and the Care of the Virtual Self. *Economy and Society*, 37(4): 571-93.
- Wills, David and Stuart Reeves. 2009. Facebook as a political weapon: Information in social networks. *British Politics* 4(2): 265-81.
- Winner, Langdon. 1986. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: The University of Chicago Press.
- Zhao, Shanyang, Sherri Grasmuck, Jason Martin. 2008. Identity Construction on Facebook: Digital Empowerment in anchored relationships. *Computers in Human Behavior* 24: 1816-36.