Fast Capitalism
Volume 8 • Issue 1 • 2011

ISSN 1930-014X
doi:10.32855/fcapital.201101.008

A Research Agenda for Social Media Surveillance

Daniel Trottier

Introduction

In comparing one type of information leak to another, a comedian portraying Julian Assange stated, "I give you private information on corporations for free, and I'm a villain. [Facebook creator Mark] Zuckerberg gives your information to corporations, for money, and he's [Time Magazine's] Man of the Year" (SNL 2010). The real Assange had much harsher words for Facebook, calling it "the most appalling spying machine that has ever been invented" (Emmett 2011). Facebook is now synonymous with surveillance. Interpersonal, institutional, and other kinds of scrutiny take place on social media. Moreover, they interact with each other in ways that scholars and users are only beginning to understand. The full consequences of social media's expansion remain to be felt. Uncertain conditions of visibility are a certainty on social media.

In adopting a surveillance studies approach, this paper will examine the complex and multi-faceted nature of social media. Facebook and other social media are online services where users submit personal information for any number of reasons. Surveillance on social media involves numerous kinds of watchers. These include friends, family and employers, but also law enforcement agencies and those who control sites like Facebook. This paper reflects on the growth of social media services, and considers their implications for surveillance studies. It proposes a framework for understanding how social media brings together different social spheres, making a range of personal data from those spheres searchable and visible. It also considers two topics that warrant specific focus: investigative surveillance on social media and surveillance by social media developers themselves. This approach is aligned with a science and technology studies perspective that focuses on technologies as they are taken up in society (Grint and Woolgar 1997; Nye 2006). Such a perspective highlights the design stage as well as the circumstances surrounding technological growth. Facebook is perpetually redesigning itself, and its overall trajectory remains opaque to users.

While scholars from various disciplines are studying social media, the increased visibility of personal information through services like Facebook makes them a crucial topic for surveillance studies. This perspective considers surveillance to be the focused and systematic collection of personal information (Lyon 2001). Moreover, the leak is the principal means by which information from one context migrates to other contexts. Leaks often result from malice or incompetence, but Facebook operates precisely to exchange information from one context to another. The leak becomes standard. Surveillance practices result in privacy violations (boyd 2008), but also compromised social relations, social sorting, and an ever-mutating political economy of personal information (Cohen 2008). Surveillance on social media comprises a range of activities, from casual, consensual sociality to covert scrutiny. We can distinguish between instances that are harmless and those that have devastating effects, but they operate on the same interface and use the same information. Moreover, harmless surveillance on social media can trigger harmful consequences, as sites like Facebook lift the boundaries separating peer sociality from large-scale information management and social sorting.

This paper addresses social media more generally, with Facebook as its focal point. In less than eight years, Facebook has accumulated nearly one billion users (FB Statistics 2011). These users share their lives with each other, including over thirty billion pieces of content per month (ibid.). Facebook was launched for university students,

but its users have become demographically and culturally vast. As well, businesses, employers, and politicians now maintain a presence on the site. These official presences enable public relations and promotional efforts, but they also facilitate watching over a specific population, market, or demographic. Facebook and other social media carry a significant cultural impact. These technologies are synonymous with new media communication. Yet on first pass, services like Facebook are quite unremarkable. Facebook does not perform any novel functions: its users exchange personal information and other digital media in a routine manner. Facebook's social impact can also be understated. Its users rapidly grew accustomed to sharing content with 'friends', to the point that it became yet another mundane service that is embedded in social life. Facebook is remarkable in presenting itself as being very unremarkable. Social media are almost-forgettable interfaces that mediate social relations.

Social media are now central to the visibility of personal information. They fuel contemporary identity construction through micro-level relations. A pervasive and situated engagement means that users maintain their reputations through everyday interactions. Goffman's (1959) work on staging social activity has a renewed relevance here, as social media complicates distinctions between the front and back stage in social performances. While some of Facebook's features are more public or performative than others, Facebook has a habit of leaking backstage information into the front. For example, the news feed broadcasts information that would otherwise be restricted to a more intimate audience. The routine breaching of contextual boundaries is especially troubling given the ubiquity of stigmatizing information that individuals hide from public scrutiny (Goffman 1963). As a site that is firmly rooted in multiple social realms, Facebook collects and distributes stigmatizing content. Organizations are changing their practices in response to these conditions. The fact that individuals and institutions operate on the same platform suggests a rise of cross-contextual circuits of visibility.

Facebook has undergone an exponential growth in recent years, and with this growth comes the assumption that it is a de facto site for sociality. Facebook has very quickly dispensed with its novelty, and non-users increasingly have to justify their abstention from the site. Social media are a default location for social life. By extension, they also become a default location and means for identification. This is a paradigm shift for identity construction, but also for identifying individuals. Facebook marks a consolidation of attention among individuals and institutions. Its social relevance is greatly augmented as more attention and engagement is directed towards its interface. Not only does it become the primary location to communicate with people - often in plain sight of a very broad audience - but it also becomes the first location where people are identified. Users invest their attention towards their profiles. But they also invest their reputations, as their profile comes to have a greater monopoly of their identity. Facebook's increasing control of individual identities can be compared to attempts to implement national identity cards. Identity card schemes dictate that every citizen possesses a card, and that the card becomes the frontline means to identify citizens (Lyon 2009). Yet while mandatory schemes are routinely met with resistance, Facebook's emphasis on peer relations and mutual visibility makes it a more attractive option. Moreover, social media adds a networked dimension to identity, as users are also judged by their friends' identities and content (Wills and Reeves 2009).

This paper begins by presenting an overview of surveillance features on social media. This is substantiated by a close look at Facebook's recent development, with an emphasis on cross-contextual exchanges that contribute to a mutual augmentation of surveillance practices. These findings are informed by semi-structured interviews with fifty-six individual and institutional Facebook users. Next, this paper focuses on two categories of surveillance that warrant specific attention: investigations on social media, and Facebook's own efforts to oversee its users. These kinds of monitoring matter to surveillance studies, not only because of their privileged view of social media content, but also because of a current opacity surrounding these practices. This paper identifies the properties that give these watchers a unique vantage over social data, and assesses how they affect conventional understandings of surveillance practices.

Mutual Augmentation of Social Media Surveillance

Social media surveillance is characterized by the expansive growth of these services. Social media continuously adopt new features, to an extent that challenge efforts to understand them. User experiences, scholarly descriptions, and other attempts to know social media are complicated by this growth.

In 2009, I briefly put my social media research on hold in order to focus on other projects. When returning to this research I was stunned by how outdated it had become. Basic facts about its population and valuation were

starkly inaccurate. Furthermore, Facebook had since introduced a number of features that impacted the crux of my arguments, both descriptively and analytically. I had to reconsider my research in light of what Facebook was becoming. Social media in general and Facebook in particular are growing to a degree that greatly complicates any assertion about 'what it is' or 'what it does.' This is a challenge for scholars wanting to speak authoritatively about social media. But it is also a challenge that users are facing in their prolonged engagement with the site. They invest their time and their identities when creating a presence on the site, and this investment is tied to assumptions about what the platform is, how it is used, who is using it, and what values govern its use. All of these features have changed extensively, leaving users to cope with this volatility.

Consider the introduction of the news feed in September 2006. This feature aggregates users' personal information and displays it on a prominent section of the site for others to see. Users were not prepared for this kind of exposure. They protested, but eventually accepted the feed. The news feed has become a fixture in their everyday use of the site. One student reflects on this feature, stating:

> **I remember when the News Feed was first created, the outrage that came from a great number of people. But as they got used to being able to see so much, it became an asset, I suppose, for Facebook creeping and Facebook stalking and keeping tabs on what's going on (Samantha).**

User concerns about their own exposure are tempered by Facebook's function in watching over their peers. Other changes to the interface include new kinds of information submission, new ways to distribute that information, and new privacy settings that regulate how far this information can be distributed. Users are routinely appalled by these developments, but with time and experience they come to accept Facebook as an ever-changing platform. This means that their personal information will likely be disseminated in ways that are unexpected and non-consensual. Users grow accustomed to the volatility of information control on social media.

Social media interfaces change over time. But growing user populations also hold a social impact. Facebook's recent growth comes from an older, geographically diverse population that are linked to a broader range of institutions (Madden 2010). This growing population has an impact on what it means to use Facebook, but also what it means to be seen on Facebook. It marks a growing body of personal information, as well as a rise of contexts from which this information is made meaningful. Facebook itself performs a unique kind of surveillance, and the fact that this is overlooked will be addressed below. But what is also remarkable about surveillance on Facebook is that so many kinds of watchers are involved. Facebook is a public face to a constellation of surveillant agents. In addition to speaking about these separate kinds of monitoring as part of a broader category, we can also see how each of these practices changes by virtue of adopting social media.

Understanding these effects rests on understanding how social media enable information convergence. Different kinds of audiences – and more of each of these different watchers – are turning to the same interface, to access the same information. A converging audience enables a convergence of social contexts. Personal relations are more closely linked to commerce and the workplace. Henry Jenkins (2006) describes convergence as content flows that are more liberated and volatile, notably through the rise of user-generated content. This imagery supports a leak-based view of Facebook. While information leaks were formerly exceptional and unforeseen events, Facebook's exponential increase of leaks amounts to a kind of convergence of social contexts. Facebook's continued growth amounts to a consolidation of visibility (all can be seen on one site), and of watching (all can watch on one site). Surveillance becomes democratizing and decentralized, but this convergence also facilitates a centralized kind of watching. This is important when considering that some groups may have access to information that exceeds privacy settings put in place by users, and that those groups can shield their practices from visibility and maintain a selective presence on the site.

Formerly discrete surveillance practices feed off each other through their prolonged engagement with Facebook. This mutual augmentation is a product of social media's social convergence. In order to understand mutual augmentation, consider three tangible kinds of surveillance: (a) individuals watching over one another, (b) institutions watching over a target population, and (c) businesses watching over their market. Individual, institutional, and market scrutiny all rely on the same interface and information. This means that personal information that has been uploaded for any single purpose will potentially be used for several kinds of surveillance. All three types of watching are augmented by Facebook's exponential growth, as more users are joining the site to watch over peers, populations, and markets. With every additional set of eyes affixed to Facebook, any content already on the site has a larger audience. Moreover, that increased audience is situated in a greater variety of social contexts, starting

with Facebook's growth beyond the university sector. In addition these users all augment each other's visibility by uploading content that implicates each other.

All three populations also share the potential of being watched. They may be visible as a result of information that they upload, or because of content uploaded by other users. Mutual augmentation results in a shared risk and visibility as well as shared tools to watch over others. Individuals, institutions, and businesses report that their own visibility on Facebook is a primary motivation to watch over the site. The potential of being watched by others contextualizes their own surveillance. Not only does this suggest that surveillance is rampant on the site, but it also dampens users' ethical concerns about covertly watching others. Employees in public relations or marketing are keenly aware of this condition, and routinely scrutinize user conversations for mention of the brands that they represent. Use and scrutiny are fuelled by the idea that other users contribute to one's own visibility. Individuals, institutions, and businesses believe that social media endangers their reputation. Out of necessity they scrutinize what others are saying.

Individual users, especially students, were the first to join Facebook. However, they soon discovered that other populations were signing up. These original users are aware of tangible and visible forms of surveillance. They are more likely to be concerned with their parents watching over them than they are with marketers, but they are increasingly aware of both, as well as other types of watchers. As one student remarks:

> I'm just aware that what I do on Facebook is available to a lot of people. (...) You're representing yourself through something that a lot of people can access, so to be aware of how you use that information and what you post (Maggie).

Users are aware of the criteria that other watchers are employing, and will self-scrutinize based on these criteria. Moreover, they will watch over friends and family with an eye for harmful content. This scrutiny serves to protect that person's reputation. These users watch over their peers in the same way that they watch over their own profiles, under the assumption that potential employers and other professionals may be watching. Interpersonal scrutiny becomes professionalized in recognition that professionals are watching.

Institutional surveillance on social media is a direct product of interpersonal scrutiny. Employees use their personal knowledge as Facebook users to watch over populations in a professional context. Their ability to access the site, as well as effectively navigate and search for content, rests on employees' familiarity through their own personal accounts. Moreover, they are able to see content that was uploaded as a result of individual users wanting to remain visible to one another. This kind of interpersonal reciprocation augments institutional scrutiny. Businesses also draw on interpersonal scrutiny by employing early adopters of social media to manage their presence. Not only do businesses watch over interpersonal conversations and exchanges, but a conversational approach is also adopted as a best strategy for remaining visible to their markets. Providing targeted and immediate feedback to clients is increasingly treated as a 'best practice' for online communications, as this feedback is framed as an effective public relations effort.

Facebook is invisible in the sense that it is ubiquitous. It is pervasive to an extent that it hardly evokes our attention. Its expansion into various social spheres elicits little concern or controversy. As a result, information contained on the site can easily migrate to new contexts. While these sites serve to make their users visible to the social world, their own inner-workings remain opaque. Facebook users do not know what to expect from a site that hosts so much of their online presence. Social media are complex networks where different actors and contexts influence each other. These broader effects warrant more attention, but scholars should also look at key actors in this complexity. Two specific kinds of monitoring are considered below. They are not only under-represented in scholarly research, but they also benefit from being relatively covert to users. Their lack of transparency is a concern that should be addressed by empirical research.

Investigative Surveillance on Social Media

When a Wayne Gretzky jersey was stolen from a shop in Ottawa, it only took fifteen minutes for staff to identify one of the shoplifters on Facebook (Butler 2010). While Facebook's history is peppered with student indiscretions becoming public knowledge, police and other investigative agencies are turning to social media in order to collect information about criminal activity. Police consider social media to be part of their jurisdiction, as a source of evidence as well as a location for offences to occur. For instance, threats that are uttered online are treated as

punishable offences (Protalinski 2011). Online venues are not treated as representations of real life spaces, but rather as spaces in their own right. In the United States, Department of Homeland Security officials are 'friending' applicants for citizenship in order to scrutinize them (Lynch 2010). These agencies take advantage of social networks by placing themselves within a context of information sharing and personal disclosure. They also take advantage of users' so-called 'narcissism' (Cheng 2010), as even people who have something to hide want to share their lives with other users.

Social media are increasingly harnessed by law enforcement and investigative agencies. These practices and tendencies also spill out in other sectors, like the investigation of insurance claims (Millan 2011) as well as divorces (Popken 2011). But this remains a critically under-theorized and understudied topic. Social media make large sections of social life visible, and investigative agencies are taking advantage of that visibility. Surveillance studies needs to focus on how this visibility is being used by these agencies. This topic sheds light on contemporary investigation techniques, but it also illustrates the pathways and dynamics of contemporary social media visibility.

Police can obtain information on social media through conventional and unconventional means. Social media services have opened up official channels for police to obtain private information from their servers. These services know their value as a source of evidence for these agencies, to the extent that Facebook, Twitter, MySpace, and others have produced compliance documents (Lynch 2011) that dictate what kind of information can be obtained from warrants, court orders, and other legal procedures. When starting an investigation, it is increasingly common for police to first turn to Facebook and other social media. Not only is it a low-cost and low-risk option, but investigators also benefit from not being identified as such. Professional watchers are often personal users, and this knowledge and access are assets. A lot of information on social media can be obtained simply by logging on to these sites. When information is protected by privacy settings, investigators can use a personal profile to establish a connection with the suspect. They may pretend to be a stranger, or even of a trusted friend or family member of the suspect (Zetter 2010; Kerrigan 2011). Although it is not the first time that individuals close to a suspect are used against them, social media offer novel kinds of insight. Police can covertly monitor interaction between a suspect and their peers. This can be done with or without subpoenas, depending on the suspect's privacy settings. As well, visible social ties can themselves be informative. In the case of the stolen hockey jersey, it was the suspect's friends that gave him away, as one of these friends belonged to a Facebook fan community for the store.

Social media policing goes beyond simply gathering information about suspects. Events ranging from house parties to political protests are also made visible through social media. Not only is information about these events public by default, this information is also searchable and archived, making sites like Facebook optimal for investigations. Finally, social media are not just a new kind of watching for police. They can also make crime and criminals visible by quickly broadcasting information about subjects to a vast audience. Social media like Twitter and Facebook are employed to disseminate time-sensitive information, including AMBER Alerts (O'Connor 2011). This suggests enrolling entire social networks to report suspicious activity. A campus security director involved with this kind of initiative elaborates on its implications for surveillance practices:

> I always find it very interesting that when people talk about Facebook and then the next word is security, automatically they have the George Orwell kind of 1984, Big Brother's watching. In our department, it's the exact opposite, right? We're all about sharing information. Our philosophy here is security is everybody's responsibility. Our philosophy here is giving you all the information that you need to make informed decisions about your own safety (Daryl).

This officer positions sharing information with a population in direct contrast to watching over that population. Yet these two operate in tandem, as social media users can be both a target and an extension of a surveillance apparatus. Users not only make themselves visible in a way that augments investigative surveillance, but they also directly contribute to this watching on behalf of the investigative agencies. Social media offer multiple avenues for individuals to augment institutional scrutiny.

These developments are situated alongside existing research on crime and surveillance. First, they suggest a further expansion of a surveillant assemblage (Haggerty and Ericson 2000) of global information flows. This model illustrates how discrete information flows are assembled in order to amplify the scrutiny of social life. At its core, Facebook attempts to link its users together in order to encourage them to share content. Often these users were not previously exchanging information. The emergence of an assemblage is evident when law enforcement and other agencies get involved. Prior to Facebook these agencies could not access much of the personal information contained on this site. But this information is now part of their scope. A social media surveillance assemblage is composed of multiple agencies taking advantage of a staggering amount of personal information. As well,

information on social media becomes even more trans-contextual. Haggerty and Ericson point to how CCTV footage becomes material for entertainment. Social media further exemplify that kind of reconfiguration, as personal exchanges become material for investigations. Social media also furthers a "disappearance of disappearance" (ibid.: 619). Abstaining from Facebook is a diminishing possibility when users upload information about peers who avoid an official presence on the site.

Social media also forces a reconsideration of the nature and effectiveness of undercover policing. This refers to a set of practices to infiltrate criminal spaces and obtain access to otherwise private and closely guarded information. Undercover approaches enhance police surveillance by using deceit and an asymmetry of visibility to locate and incriminate suspects. Policing becomes proactive and based on categorical suspicion, as undercover strategies enable a focus on suspects rather than incident-led scrutiny (Marx 1988). Police efforts on social media greatly facilitate this process. Undercover policing becomes low risk, as police visibility and exposure are negligible. As stated above, investigators can also impersonate trusted peers, a further deception in order to access and watch over suspect in a candid state. Social media also facilitates the use of criminal informants, or 'snitches' (Natapoff 2009; Marx 1984). Social media policing resembles snitching in the sense that investigators direct their attention to a suspect's peers in order to obtain information. Yet this marks a shift in procedure, as these 'snitches' are seldom aware of their involvement in this process. The costs associated with both undercover police work and snitching are lowered through social media (cf. Shirky 2008). As more users live more of their lives on sites like Facebook, their interpersonal visibility becomes an increasingly valuable component of police investigations. Of particular concern is that users may not be aware of these implications.

In briefly considering what is already known about social media capacities and police work, we see that these services mark an enhanced police presence in - and scrutiny of - everyday life. Moreover, police benefit from an as-yet-unidentified quality of social media. This has to do with their indirect involvement with sites like Facebook. Police are not formally associated with social media, and their presence is not public knowledge. Indeed, they are barely visible on Facebook. Unaware that they might be subject to police scrutiny, users are bridging multiple social contexts through Facebook, making their lives – and those of their peers - visible in ways that benefit investigations. Institutionalized scrutiny reaches into depths of everyday sociality (Haggerty and Ericson 2000).

Social media users have countless reasons to engage with these services. But these different users are not simply watching in parallel. Their engagements with services like Facebook have a distinct effect on the kinds of watching and visibility that are made possible through social media. Mutual augmentation suggests that different watchers trigger each other's surveillance. Interpersonal transparency and disclosure is a specific kind of visibility that enhances formal types of surveillance. Users are increasingly comfortable on a platform that is the first line of scrutiny for police investigations. Subsequent research should interrogate the boundary between personal and investigative use, but also between police suspects and their peers. This technology is not a complete disruption of police practices, but their investigative scope is enhanced in a way that is largely undetected, and as such warrants academic scrutiny.

Social Media as (Meta-)Watchers: What Will They Do Next?

Facebook's exponential growth makes it ideal for many kinds of monitoring. These developments only underscore the urgency of looking at Facebook and other social media companies' own surveillance practices. The visibility of users on these interfaces gives the impression that they are directing the growth of social media, that the tail is wagging the dog. To be sure, the entirety of the tail is staggering, but the dog still wields control. For all the talk about coping with and taking advantage of social media, little attention is paid to its configuration. These companies are highly publicized, yet scholars and the broader public have little knowledge about their knowledge of users, as well as their intentions surrounding this knowledge. A specific type of social media surveillance, one that includes the construction and continued maintenance of a digital enclosure, is central to a scholarly understanding of social media, as well as the continued domestication of surveillance technologies.

Information on Facebook leaks from one context to another. Yet the site is designed to retain both content and users. Facebook is internally leaky, but has rigid boundaries. In this sense, it is a kind of enclosure. Mark Andrejevic refers to the digital enclosure as "an interactive realm wherein every action, interaction, and transaction generates information about itself" (2009: 53). This definition suggests an infrastructure where personal information is produced and made meaningful insofar as it generates more information. The enclosure suggests a return to a

kind of pre-modern sociality where everybody knows everybody else's business. Yet the presence of surveillance technology suggests new kinds of visibility. As Andrejevic suggests:

> Interactivity promises not a return to the relative lack of anonymity of village life, but rather to a state of affairs in which producers have more information about consumers than ever before, and consumers have less knowledge about and control over how this information is being used (2007: 27).

On first pass it seems that all social media users have the potential to watch over each other. But those who manage the enclosure have a privileged view of its contents. As a result, user behaviour can trigger revisions to the interface. Users may develop their own practices within an enclosure, and this can be framed as a kind of customization, or even resistance. However, the enclosure's owners can observe and either subsume or eliminate those practices. Manovich (2008) draws on de Certeau (1988) to assert that user tactics become an owner's strategies. Users may develop tactics to manage their presence on sites like Facebook, but these tactics are visible to Facebook itself. Likewise, visible protests within the enclosure and discussions about disengagement from the enclosure can be exploited to retain users. As Cohen indicates:

> Not only is surveillance the method by which Facebook aggregates user information for third-party use and specifically targets demographics for marketing purposes, but surveillance is the main strategy by which the company retains members and keeps them returning to the site. (...) [I]t is the unpaid labour of producer-consumers that facilitates this surveillance (2008: 8).

The increased focus on everyday life is in itself a concerning development. Poster remarks that everyday life was formerly the remainder of institutional action and scrutiny (2004). However, the rapid onset of information and communication technologies in the domestic sphere means it is increasingly subject to commoditization and surveillance.

Treating social media as enclosures provides an important balance to perspectives that regard these services as ephemeral in use and consequence. Users do submit information with immediate and localized contexts in mind. Yet their privileging of these contexts does not diminish long term consequences made possible by the retention of this information. There is a disjuncture between immediate use and long-term consequences of exposure in social media enclosures. People live their lives through social media, and these enclosures are the interface in relations between individuals, businesses and institutions. The mutual augmentation described here is the result of the increased co-habitation of these groups. Facebook as an enclosure retains extensive information about its users, yet little is known about what Facebook is doing with this information, or the kind of watching that it performs.

Facebook and other social media are growing, and their growth is difficult to assess. But these services follow a deliberate trajectory, even if this is only evident to its designers. Specific features are chosen instead of others, and specific purposes are privileged over others. These decisions are part of a larger vision that Facebook's developers are pursuing, and focusing on these developments will contribute to a better understanding of social media surveillance. Research on social media often treats it as sui generis, and assumes that it functions independently of human intervention. This overlooks the intentions and efforts of companies like Facebook. Moreover, this approach is troubling when talking about a platform that adopts new features on a regular basis.

Facebook is distinct from other online services in terms of the possibilities that it extends to users. Users can always upload and distribute content, and they can partially control the flow of their information, but they cannot control the interface that distributes their information. Users can report a troubling photo, or block someone from seeing their profile, but they are otherwise passive to emerging schemes for distributing information. Below are some key features that have been designed by Facebook to regulate the flow of personal information. As these become standard features of social media, we should question their inevitability, and consider alternative efforts.

- Soliciting information from users, and enrolling friends in this effort. Facebook treats incomplete profiles as problems in need of remedy. Not only is the user faced with this concern, but their friends are also asked to provide information about the delinquent user. New users are repeatedly solicited by Facebook to provide personal information, including biographic details, social contacts, and profile pictures. Users encounter these requests when they first log on, but they also appear on their profiles as highlighted alerts. Moreover, their friends will also be asked to supply these details. These efforts guide Facebook users to obtain content from their friends. Generating personal information on social networks rests on relations between users and their peers.
- Restricting the outward flow of information. Facebook has long followed a 'walled garden' approach. As a site of social and informational convergence, it hinders efforts to export content to other spaces. In doing so Facebook obliges

users to inhabit - or dwell (DeCerteau 1988) - rather than simply visit the site. Facebook has recently augmented its messaging service in order to obviate email (Gaudin 2010), and its search feature is meant to rival Google (Vogelstein 2009). These efforts limit not only the outward flow of information, but also the outward flow of attention by users. This produces a kind of watching based on a monopolization of social activity by one company.

- Redirecting users towards each other as feeds. The promotion of information feeds suggests a deliberate strategy to organize and streamline the exchange of personal information. The feed represents Lash's (2006) description of information being pushed onto users. His assessment that "[t]he data find you" (ibid.: 580) can mean that relevant information is pushed onto profiled users, but it also suggests that our own personal information tracks and locates us, greatly augmenting our visibility. As stated above, this is a development that users first resisted, but have since come to treat as central to social media sociality. In that users rely heavily on these feeds, they diminish the importance of the user's construction of a profile as an identity marker, transforming self-presentation into a flow of real-time statements populated by several identities.
- Turning personal information into advertising. On numerous occasions, Facebook has attempted to merge personal information with branded advertising (Pearlman 2007; Zuckerberg 2007; Ling 2008; Zuckerberg 2010). A comment posted about a restaurant can become an advertisement that is directed at the user's friends. Users in turn have consistently opposed these schemes. Yet Facebook continues to push this model as an inevitable feature. Social media taps into a long history of marketers exploiting personal information (Gandy 1993). Advertising schemes increasingly resemble viral marketing (Boase and Wellman 2001). Again, this suggests a dramatic lowering of the costs associated with these activities, so much so that actual user involvement in these efforts is minimized. Facebook's business strategy alters relations between consumers and producers of content (Beer and Burrows 2007). Attaching personal information to a brand or product adds contextual relevance to the latter, while making the former visible in unanticipated ways.

Social media enclosures operate through a remarkable asymmetry of visibility. User activity is made incredibly visible, while the mechanics that govern these practices are themselves hidden from view. Facebook in particular is a database, and one that contains a robust range of content. But it is also an interface for all other kinds of watching. This suggests a kind of meta-surveillance, with Facebook watching over other watchers. As Facebook itself holds all information that passes through it, any kind of watching between users is under their scrutiny. All other kinds of watching on Facebook are a matter of using Facebook, and these practices leave traces that become part of the enclosure. Even actions intended to reduce visibility like removing content or changing privacy settings can be recorded as a kind of information.

Concluding Remarks

Facebook and other social media increasingly regulate social life. The way they collect, archive, and disseminate personal information is noteworthy for surveillance scholars. The Facebook profile has arguably overtaken the CCTV camera as the primary imagery for surveillance studies. Different surveillance models are manifest through Facebook. This suggests a complexity of social media surveillance. Understanding social media surveillance requires an understanding of the features that add to social media's volatility. Even when talking about one kind of surveillance, or one context, other contexts and practices are not far off. For instance, interpersonal visibility greatly augments state and institution-led surveillance. In addition to knowing how different types of visibility and watching are manifest on sites like Facebook, subsequent research should focus on practices that stand apart from the kind of co-visibility that is typical of social media. Police and other investigative agencies are developing a number of strategies to take advantage of the increased visibility of social life. Moreover, interfaces like Facebook themselves have a unique and privileged visibility and control over social media activity.

One lingering concern in the age of Facebook surveillance is the prominence of information leaks. While these were formerly a marginal but troubling occurrence, information now readily flows between social contexts. The rapid expansion of social media in a broader context of ubiquitous leaks suggests a "levelling of the hierarchy of surveillance" (Haggerty and Ericson 2000: 606), in the sense that more and more people are subject to public exposure. Yet this does not imply a democratization of visibility. Any democratizing potential is called into question when its users are entirely visible to agents whose practices remain opaque. Despite the complexity of relations and effects, it appears that new kinds of capital and control will endure through social media.

References

Andrejevic, Mark. 2007. iSpy: Surveillance and Power in the Interactive Era. Lawrence, KS: University Press of Kansas.

----. 2009. "Privacy, Exploitation, and the Digital Enclosure." Amsterdam Law Forum. 1(4): 47-62.

Beer, David and Roger Burrows. 2007. "Sociology and, of and in Web 2.0: Some initial considerations." Sociological Research Online. 12(5). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1978/1853. Accessed May 10, 2011.

Boase, Jeffrey and Barry Wellman. 2001. "A Plague of Viruses: Biological, Computer and Marketing." Current Sociology. 49(6): 39-55.

boyd, danah. 2008. "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence." Convergence: The International Journal of Research into New Media Technologies. 14(1): 13-20.

Butler, Don. 2010. "Facebook helps store owner track thief: Security video checked against business's 'friends.'" Ottawa Citizen. October 31. http://www.ottawacitizen.com/technology/Facebook+helps+store+owner+track+thief/3753823/story.html. Accessed May 10, 2011.

Cohen, Nicole. 2008. "The Valorization of Surveillance: Towards a Political Economy of Facebook." Democratic Communiqué. 22(1): 5-22.

Cheng, Jacqui. 2010. "Govt relies on Facebook 'narcissism' to spot fake marriages, fraud." Ars Technica. October. http://arstechnica.com/tech-policy/news/2010/10/govt-takes-advantage-of-facebook-narcissism-to-check-on-users.ars. Accessed May 10, 2011.

de Certeau, Michel. 1988. The Practice of Everyday Life. Berkeley: University of California Press.

Emmett, Laura. 2011. "WikiLeaks revelations only tip of iceberg – Assange." RT.com. May 2. http://rt.com/news/wikileaks-revelations-assange-interview/. Accessed May 10 2011.

FB Statistics. 2011. "Statistics." http://www.facebook.com/press/info.php?statistics. Accessed May 10, 2011.

Gandy, Oscar. 1993. The Panoptic Sort: A Political Economy of Personal Information. Boulder, CO: Westview.

Gaudin, Sharon. 2010. "Facebook messaging throws a blow at Google: Facebook Messages could draw users from Gmail." Computerworld. November 16. http://www.computerworld.com/s/article/9196618/Facebook_messaging_throws_a_blow_at_Google. Accessed May 10, 2011.

Goffman, Erving. 1959. The Presentation of Self in Everyday Life. New York: Anchor Books.

----. 1963. Stigma: Notes on the Management of Spoiled Identity. New York: Simon and Schuster.

Grint, Keith and Steve Woolgar. 1997. The Machine at Work: Technology, Work and Organization. Cambridge: Polity Press.

Haggerty, Kevin D., and Richard V. Ericson. 2000. "The surveillant assemblage." British Journal of Sociology. 51(4): 605–22.

Jenkins, Henry. 2006. Convergence Culture: Where Old and New Media Collide. New York: New York University Press.

Kerrigan, Sean. 2011. "US Gov. Software Creates 'Fake People' on Social Networks." Examiner.com. February 18. http://www.examiner.com/social-media-in-national/us-gov-software-creates-fake-people-on-social-networks-to-promote-propoganda. Accessed May 10, 2011.

Lash, Scott. 2006. "Dialectic of Information? A response to Taylor." Information, Communication & Society. 9(5): 572-81.

Ling, Benjamin. 2008. "Platform: One Year(ish) later." The Facebook Blog. July 28. http://blog.facebook.com/blog.php?post=24577977130. Accessed May 10, 2011.

Lyon, David. 2001. Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press.

----. 2009. Identifying Citizens: ID Cards as Surveillance. Cambridge: Polity Press.

Lynch, Jennifer. 2010. "Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your 'Friend.'" Electronic Frontier Foundation. October 12. https://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and. Accessed May 10, 2011.

----. 2011. "Social Media and Law Enforcement: Who Gets What Data and When?" Electronic Frontier Foundation. January 20. https://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what. Accessed May 10, 2011.

Madden, Mary. 2010. "Older Adults and Social Media." http://www.pewinternet.org/Reports/2010/Older-Adults-and-Social-Media/Report.aspx. Accessed May 28, 2011.

Manovich, Lev. 2008. Software Takes Command. Unpublished. http://lab.softwarestudies.com/2008/11/softbook.html. Accessed May 10, 2011.

Marx, Gary. 1984. "Routinizing the Discovery of Secrets: Computers as Informants." American Behavioral Scientist. 27(4): 423-52.

----. 1988. Undercover: Police Surveillance in America. Berkeley: University of California Press.

Millan, Luis. 2011. "Insurers and Social Media: Insurers' use of social networks impinges on privacy rights." The Lawyers Weekly. March 25. http://www.lawyersweekly.ca/index.php?section=article&volume=30&number=43&article=2. Accessed May 10, 2011.

Natapoff, Alexandra. 2009. Snitching: Criminal Informants and the Erosion of American Justice. New York: New York University Press.

Nye, David. 2006. Technology Matters: Questions to Live With. Cambridge, MA: The MIT Press.

O'Connor, Mary Quinn. 2011. "Social-Networking Tools Help Find Missing Children." FoxNews.com. March 30. http://www.foxnews.com/scitech/2011/03/30/social-networking-tools-help-missing-children/. Accessed May 10, 2011.

Pearlman, Leah. 2007. "Facebook Ads." The Facebook Blog. November 6. http://blog.facebook.com/blog.php?post=6972252130. Accessed May 10, 2011.

Popken, Ben. 2011. "Facebook is Number One Tool for Divorce Lawyers." The Consumerist. May 18. http://consumerist.com/2011/05/facebook-is-number-one-tool-for-divorce-lawyers.html. Accessed May 28th, 2011.

Poster, Mark. 2004. "Consumption and digital commodities in the everyday." Cultural Studies. 18(2): 409-23.

Protalinski, Emil. 2011. "Teenager tries to hire a hitman via Facebook, fails." ZDNet. February 15. http://www.zdnet.com/blog/facebook/teenager-tries-to-hire-a-hitman-via-facebook-fails/129?tag=mantle_skin;content. Accessed May 10, 2011.

Shirky, Clay. 2008. Here Comes Everybody: The Power of Organizing Without Organizations. New York: The Penguin Press.

SNL. 2010. Saturday Night Live. Season 36, Episode 10. First aired December 18. NBC.

Vogelstein, Fred. 2009. "Great Wall of Facebook: The Social Network's Plan to Dominate the Internet – and Keep Google Out." Wired.com. July 17. http://www.wired.com/techbiz/it/magazine/17-07/ff_facebookwall. Accessed May 10, 2011.

Wills, David and Stuart Reeves. 2009. "Facebook as a political weapon: Information in social networks." British Politics. 4(2): 265-81.

Zetter, Kim. 2010. "Undercover Feds on Social Networking Sites Raise Questions." Wired.com, March 16. http://www.wired.com/threatlevel/2010/03/undercover-feds-on-facebook/. Accessed May 10, 2011.

Zuckerberg, Mark. 2007. "Thoughts on Beacon." The Facebook Blog. December 5. http://blog.facebook.com/blog.php?post=7584397130. Accessed May 10, 2011.

----. 2010. "Building the Social Web Together." The Facebook Blog. April 21. http://blog.facebook.com/blog.php?post=383404517130. Accessed May 10, 2011.