

Steve Mann

Joseph Ferenbok

University of Toronto, Canada. hydraulophone@gmail.com

University of Toronto, Canada. josephferenbok@gmail.com

Abstract

In this paper we address the increasingly complex constructs between power and the practices of *seeing, looking, and watching/sensing* in a networked culture mediated by mobile/portable/wearable computing devices and technologies. We develop and explore a nuanced understanding and ontology that examines ‘veillance’ (‘watching’) in both directions: surveillance (oversight), as well as sousveillance (‘undersight’). In this context, we look at some new possibilities for computationally mediated veillances. In particular, we unpack the new relationships of power and democracy facilitated by mobile and pervasive computing. We differentiate between the power relationships in the generalized practices of looking or gazing, which we place under the broad term ‘veillance’. Then we address the more subtle distinctions between different forms of veillance that we classify as surveillance and sousveillance, as well as McVeillance (the ratio of actual or permitted surveillance to sousveillance). We start by unpacking this understanding to develop a more specialized vocabulary to talk not just about oversight but also to about the implications of mobile technologies on ‘undersight’ (e.g. who watches the watchers, who watches the watchers of the watchers...ultimately the people at the bottom of the hierarchy). We argue that the time for sousveillance as a social tool for political action is reaching a critical mass, facilitated by a convergence of transmission, mobility and media channels for content distribution and engagement. Mobile ubiquitous computing, image capture, processing, distribution, and seamless connectivity of devices such as iPad, iPhone, Android devices, wearable computers, Digital Eye Glass, etc., allow for unprecedented ‘on the ground’ watching of everyday life. The critical mass of these ‘sousveillant’ capable devices in everyday life may make the practice of sousveillance a potentially effective political force that can now challenge and balance the hypocrisy and corruption that is otherwise inherent in a surveillance-only society (i.e. a society that has only oversight without undersight).

Introduction

Surveillance Studies has, over the last decade, become a well-known field, encompassing a large number of academic journals, conferences, and discourse (Ball and Haggerty 2005; Lyon 1994, 2001; Murakami Wood 2007). Random House Dictionary, 2013, defines surveillance as follows:

sur·veil·lance [ser·vey-luhns, -veyl-yuhns]

noun

1. a watch kept over a person, group, etc., especially over a suspect, prisoner, or the like: *The suspects were under police surveillance.*

The word ‘surveillance’ is of French origin, its etymology deriving from

- ‘**sur**’ which means ‘over’, ‘above’ or ‘**from above**’, and
- ‘**veiller**’ which means ‘**to watch**’.

Thus its literal meaning is ‘to watch from above’. Its actual usage is often broadened to include listening and other forms of monitoring or sensing (e.g. police surveillance of telephone conversations, etc.).

Mann, S. and J. Ferenbok. 2013. New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World. *Surveillance & Society* 11(1/2): 18-34.

<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author(s), 2013 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

The closest English word to the French word ‘surveillance’ is the English word ‘oversight’, although ‘oversight’ has a somewhat different and broader meaning, e.g. it can also be used to mean ‘an error or omission’. Google Translate gives the French word ‘surveillance’ when presented with the English word ‘oversight’.

In popular culture, the dystopian aspects of the power politics of surveillance often tend to overshadow the use of surveillance to achieve many necessary or useful infrastructural aspects in the ordering of modern citizens (e.g. passports and other identification systems) and societies (e.g. traffic laws) (Lyon 1994). Consider, for example, George Orwell’s *Big Brother*, and the Architect in the ‘*Matrix* trilogy’ and the like. So, in the field of Surveillance Studies the term ‘surveillance’ can be used in a way that conflates the necessary or important useful aspects with the more generalized forms of veillance and monitoring in modern societies (Norris and Armstrong 1999).

In other words, not all surveillance is ‘bad’, and not all surveillance is institutionalized and overtly regulated—actually, like most technologies, many of the surveillant technologies are value neutral until applied towards specific uses. The popular use of the term ‘surveillance’ on the one hand helps to unify and clarify a field of inquiry about the interaction between people and technologies in acts of organization, classification and monitoring. But the dominant discourse in popular culture tends to prioritize one form of veillance (surveillance in particular) over the more nuanced ‘crowd-sourced’ gaze of *sousveillance*—which tends to be more rhizomic and heterogeneous (Haggerty and Ericson 2000).

Sousveillance means ‘**watching from below**’, and its etymology derives from replacing ‘sur’ (over) with ‘sous’, which means ‘under’ or ‘below’ or ‘from below’ (as in words like ‘sous-chef’). *Sousveillance* (sometimes called ‘undersight’) has also been itself a topic of research (Mann, Nolan and Wellman 2003; Kingsley 2008; Bakir 2010).

Using the term ‘surveillance’ to address all practices of watching/gazing/looking/seeing obscures some of the power differentials and practices that are being facilitated by *sousveillance*, e.g. the democratization of broadcasting facilitated by mobile and pervasive computing and other social changes that society is currently experiencing.

Surveillance in its strict sense (i.e. ‘oversight’) does not always reduce crime—it can actually do the opposite! It has been argued (Mann and Ferenbok 2012) that surveillance may, in fact, cause or at least increase certain kinds of crime, and move crime up to corruption, or facilitate corruption within the very system it is meant to observe. With surveillance, the subject of the gaze is at a disadvantage and is often unaware of when (s)he is being watched, and thus the distribution of power is asymmetric.

The useful and beneficial, and in fact necessary infrastructure by which modern societies, i.e. ‘societies-of-strangers’ (Lyon 1994), monitor individuals to deliver rights, services, and due punishment, is regarded in this paper as ‘veillance’, which is understood to be the monitoring of modern societies through technological mediation of its citizens, members, and groups etc., both from above (i.e. those in high places watching those in low places) and from below (i.e. those in low places watching those in high places). For example, modern societies require infrastructures for governance, voting, credit, health-care, social justice, human rights, etc., and, more recently, citizen connectivity (internet, wireless communications, etc.) for mobile, portable, and wearable computing. As a counterpart to surveillance, *sousveillance* has been explored as a way of better understanding some of the social innovations being catalyzed by networked mobile, portable, and wearable computing (Mann et al. 2003). We now explore *sousveillance* and its power politics with an emphasis on *sousveillance* in the wide-sense, that is, not limited to the 20th century ‘us-versus-them’ ideas of inverse-surveillance, but also including ‘the recording of an activity by a participant in the activity’ (Mann et al. 2003).

Surveillance is widespread and well-known (Coaffee and Murakami Wood 2006; Elmer 2003; Murakami Wood 2009; Ball, Lyon, Murakami Wood, Norris and Raab 2006; Murakami Wood and Webster 2009). But when citizens point their cameras at the architects of the ‘surveillance superhighway’, or when photographers simply take pictures of bridges or buildings, they often come under attack, especially as police have placed photographers under suspicion (ACLU of Massachusetts 2012).

Police advertising campaigns promote surveillance while questioning sousveillance. Public posters and billboards in the United Kingdom read with text such as:

**THOUSANDS OF PEOPLE TAKE PHOTOS EVERY DAY.
WHAT IF ONE OF THEM SEEMS ODD?**

**... taking photos and making notes about security measures
like the location of CCTV cameras.**

If you see someone doing that, we need to know.

Let experienced officers decide what action to take.

In this sense, studying or being inquisitive about surveillance (e.g. taking pictures or notes of surveillance cameras) is itself grounds for suspicion. This comes at a time when innocent suspects have been ‘roughed up’ by police. Some have even been killed as a result of heightened suspicion and mistaken identity, such as the case of Jean Charles de Menezes, a Brazilian electrician shot to death by police in a London subway. And police seized the CCTV recordings and claimed they were blank! Now imagine if some citizens had their own cameras and had happened to capture the police shooting Menezes? Assuming the police had not also seized that recording, we might have a better sense of what happened. Surveillance has an inherent conflict-of-interest, for example, if and when it shows the surveillers doing something wrong, the data might mysteriously disappear or be altered. But with sousveillance, there is less chance that the police will have the *only* copy of a video of some incident. Therefore sousveillance is an important contemporary topic. There have been thousands of conferences, symposia, books, and articles published on the topic of sousveillance (see for example, Bakir (2010) or the university course ‘Surveillance, Sousveillance, Coveillance, and Dataveillance’ at UC Berkeley’s iSchool).

Established Norm: A History of Video Surveillance and CCTV

Much of the understandings of the institutional practices of surveillance in popular culture have been shaped by CCTV (Closed Circuit TeleVision) surveillance. This is the form of monitoring that readers of Orwell’s *1984* were introduced to with his concept of the ‘telescreen’. The history of such media-supported unidirectional viewing dates back to 1942 when German scientists first invented Closed-Circuit Television (CCTV) surveillance to monitor rocket tests from a distance (Reuter 2000). At its most basic level, a CCTV system is a camera directly connected to a video display. Connected by a continuous closed electronic circuit, the camera captures images that are then transmitted to a television display device such as a CRT (Cathode Ray Tube). In the CCTV model the information flow is uninterrupted and unidirectional. The closed path from closed-circuit (CC) camera to television (TV) screen implies an indexical relationship between the surveyed space and the image—a visual truth that hides the mediation imposed by the technology of the medium, and the viewer from the viewed. The closed-circuit system implied that the broadcast stayed located and localized as opposed to the ‘open’ television broadcast model also being developed at the time. This unidirectional information flow of CCTV was germane to both popular and Foucauldian understandings of gazing and surveillance (Foucault 1982).

The first ‘open-street’ deployment of CCTV came in 1969, when the London Metropolitan Police used two temporary cameras in Trafalgar Square to monitor Guy Fawkes Day Activities (Norris and Armstrong 1999). Police monitoring Trafalgar Square realized that the video could help more effectively deploy

officers ‘on the ground’. As a result, by the end of the 1960s this model of closed-circuit surveillance began its global dispersion, and over the next two decades CCTV systems evolved to include more than just cameras and television display devices. To facilitate multiple camera inputs and viewing options, additional devices such as switchers, controllers and recorders were integrated. CCTV networks, heavily dependent on monitoring strategies, became bimodal—the act of looking or observing from a privileged power position often became dissociated from action taken based on this act of gazing (Ferenbok and Clement 2012).

This closed-circuit television system has become the dominant metaphor for visual surveillance and surveillance has become an established form of gazing in many societies. Whether publicly funded as in the case of the UK (Norris and Armstrong 1999), or privately owned as is often the case in North America, video surveillance systems have become a standard form of asymmetric ‘gazing’ on urban streets and in publicly accessible spaces (Norris, McCahill and Wood 2004). In food courts, on public squares, in public baths (see www.poseidon-tech.com), and pointed into public streets, government and private cameras are pervasive in most urban landscapes (Norris et al. 2004). The gaze of the camera implies not only a potential observer but also a potential record upon which judicial proceedings may be based (Monahan 2006).

In more recent years, video surveillance has expanded to more ubiquitous forms (Norris et al. 2004; Ball et al. 2006). In some new cities surveillance cameras are being fitted inside every streetlight and many other light fixtures for energy management (automated occupancy sensing and lighting that adapts to the activities of the occupants) (‘Pixelview’). Moreover, video surveillance is being used in places previously off-limits or thought to be private. For example, video surveillance is being used in washrooms, change rooms, locker rooms, and the like (Fraser 2007; Monahan 2006).

As CCTV networks and their monitoring strategies became bimodal, the act of looking or observing from a privileged power position often became dissociated from actions taken based on this act of gazing. The effectiveness of the viewing and the potency of the resultant action or event determine the angle of power between the agent of the gaze and its subject. Surveillance, as a form of ‘oversight’, inherently has a sloped power relationship between the viewer and the subject of the gaze (Silverman 1984).

Wearable Computing and Augmented Reality

The utopian promise of wearable personal broadcasting began in the 1960s when video recording devices became increasingly portable. The first camera recorders were large backpacks that accompanied large camera housings, but by the 1970s single unit integrated camcorders were revolutionizing recording and broadcasting. The monopoly of studio based television began to be eroded with the rise of guerilla TV—a kind of sous-broadcasting model that allowed for ‘on-the-ground’ perspectives. Guerilla TV, made possible by portable recording, allowed the asynchronous broadcasting of counter-hegemonic spectacles.

Also beginning in the 1970s, while still a teenager, author Steve Mann created various kinds of ‘wearable computers’ for use in everyday life, envisioning the computer as a realtime seeing aid for ‘augmented reality’ (augmented, modified, and more generally mediated vision, see figure 1).

Steve Mann: Evolution of wearable computing in everyday life



Figure 1: More than 30 years of Wearable Computing and Augmented Reality in everyday life.

This ‘I/eye am/is a camera’ work blurred the boundary between ‘seeing’ and ‘photographing’, as well as the boundary between ‘remembering’ and ‘recording’. The permanently attached computer vision system that Mann originally developed as a seeing aid also makes him *existentially contraband*. Recently, for example, Mann was physically assaulted by McDonald’s employees who were acting in a vigilante capacity to enforce laws that do not even exist. This incident was described in the mainstream media as ‘the world’s first cybernetic hate crime’ and as ‘McDoGate’. McDonald’s also refused to consider the surveillance video recordings from their many surveillance cameras, and instead relied entirely on oral employee testimony in their evaluation of the incident (see <http://eyetap.blogspot.com>).

Changing forms of Veillance

Wearable computing and personal broadcasting change the rules of the game. Among other things, they provide individuals with a record, an external memory aid, independent ‘proof’. What life-blogging and wearable computing represent are the tip of a much larger social change that will change the power relationships caught-up in acts of mediated gazing. Within the complex socio-technical milieu of the modern state, ‘veillance’, or the acts of gazing, can be further unpacked into ‘surveillance’ and ‘sousveillance’. Both these forms of ‘veillance’ involve the relationships of power between the subject and the agent. Following its etymology, surveillance and ‘oversight’ may be thought of as approximate reciprocals of *souveillance* and ‘undersight’, in situations where they both represent a power relationship between an observer and the observed. In this sense, *sousveillance* may be described as ‘watchful vigilance from below’. But surveillance and *sousveillance* go beyond a 20th century ‘us versus them’ argument and need to be understood in the broader intellectual landscape. The nature of surveillance itself has been irrevocably changed by digitization, networking and ubiquitous computing. Surveillance has pushed well beyond Foucault’s vision of its prison context. Surveillance has both diversified in the kinds of looking and the kinds of power relationships it involves, and it has become abstracted to the level of symbols, or binary codes, aggregated and reconstituted at will, by those who control it.

Whereas surveillance and oversight once literally meant to watch from above, increasingly the word ‘surveillance’ (and the word ‘oversight’, its literal English translation) has taken on a broader meaning in both the ‘over’ and the ‘sight’ parts:

- The ‘sight’, ‘veiller’ is now being used more broadly than only visual sensing. Surveillance now also refers to audio monitoring, pressure-sensing (e.g. ‘smart’ floor tiles, etc.), and, more generally, any kind of data collection, etc., not just video data collection;
- The ‘above’, ‘sur’ is becoming decoupled from its literal meaning of being in physically high places, such as a high mountaintop lookout, as suggested by Sun Tzu in the *Art of War*. Surveillance is now thought of in a more metaphorical context, such as hierarchically being ‘in

high places' (e.g. police keeping watch over citizens, shopkeepers keeping watch over their shoppers, etc.), regardless of whether or not the police, shopkeepers, etc., are literally at a high vantage point. For example, the computationally intensive surveillance infrastructure depicted in such television shows as *Person of Interest* often in fact accumulates in a data vault deep in a basement or sub-basement computer room, or a deep underground data vault, rather than at the top of a high mountain, although its network of cameras often do watch us from above.

Thus a police officer recording your telephone conversations from the basement of a police headquarters is still doing 'surveillance' even if they are down in a basement with their eyes closed, listening intently on their earphones. And a presidential oversight committee eavesdropping on that police officer, unbeknownst to the officer, is yet another form of surveillance == meta-surveillance (i.e. a form of surveillance of the surveillance that is not necessarily sousveillance).

The data, information, knowledge, and wisdom we generate online and offline are increasingly the subjects of inspection, analysis, and aggregation by those in high places (governments, corporations, and other large organizations). Surveillance has become more of a matter of collecting and analyzing information rather than merely 'looking down at people'. Also the very act of looking, 'veillance', has become abstracted into algorithms and databases hidden behind the data-shadows we leave behind. We are no longer 'looked-at' from a hilltop or a high turret; we are now inspected years after our lives have changed, by images, etc., captured into government and corporate databases. Data from our present and past can be searched, 'looked-at', by authorities and corporations across the boundaries of time and space, e.g. from distant cities, or at times in the distant future. And the 'looking' does not stop here: increasingly, algorithms are being taught to look ahead, to anticipate our potential actions. What has remained constant though is the relationship of power between the gaze of power and its subject, and that power favours the institutionalized agent, or agency, be it government or corporate or hybrid entities—'governments' and 'corporations'.

Surveillance and Power

Along with the changing forms of looking involved in the mediated production of meaning (veillance) are changing systems of power. Surveillant systems have been often discussed in relation to Foucault's panopticon systems that promote internalized discipline through acts of looking. Foucault's panopticon (Foucault 1995) is a power metaphor for the distribution of institutional power that works through the fear of being watched. The challenge of the modern state, as Foucault identifies, is to keep track of and discipline large numbers of people. To 'watch' many individuals Foucault's system 'localizes' people into cells to make them into quantifiable institutional bodies—what Foucault calls docile bodies: individuals that have been 'localized' into the system. A National ID system may thus be understood as a way of disciplining individuals into localized identities to create 'known' docile bodies. The knowledge produced by the gaze of the state 'looking-at' its citizens becomes a form of power. Bodies are be linked (metaphorically localized) through institutional mechanisms to a specific file or record (a.k.a. identity). These systems are often based and dependent on asymmetries of gazing.

In Foucault's panopticon, the watcher sees the body of prisoner, but is not him or herself seen (Elmer 2003; Foucault 1995). A panoptic system is based on asymmetric gazing between guards and prisoners—agents of the institution generally write, maintain, store and interpret the record or identity, and the subject of the gaze, from whom the system is generally kept opaque. So, the guards (metaphorical authoritarians), use their ability to 'see-but-not-be-seen' to observe and discipline people. This model suggests that we as citizens generally observe the rules of the authority in power because we fear repercussions: the punishment. This Foucault terms as internalized discipline. For this surveillance mechanism to monitor mass populations in an effective manner there is a tension between the forms of localization (from literal to metaphorical imprisonment) and its resource implications for oversight. In modern democracies, for the

most part, the gaze of surveillance and the threat of being caught encourage most citizens to obey, to become docile bodies.

Among Foucault's arguments throughout *Discipline and Punish* (1995) is that the institutionally disciplined body (the 'docile body') that has been integrated into a panoptic system of surveillance and internalized discipline becomes 'useful' and administered at a relatively low cost. Foucault argues that 19th and 20th century institutions are able to 'govern' mass populations by localizing bodies into individual cells that can then be used to promote discipline through asymmetric observation. The threat of punishment, e.g. the threat of the gallows, then becomes the motivation for internalized discipline.

Foucault's metaphor of the citizen as 'prisoner' in an institutional (identity) panopticon 'without walls' has revolutionized understandings and the analysis of 'power' in modern societies through their systems of organization and centralized control, and have allowed Surveillance Studies scholars to move beyond (Murakami Wood 2009). Before the days of video surveillance cameras, gallows and gibbets figured strongly in symbolic oversight. Upon entering London, England, from the West entrance, one would need to pass around the massive Tyburn Gallows (on which 24 prisoners could be hanged simultaneously) located right in the middle of the roadway. Public hangings drew massive crowds, and many towns had gallows in prominent positions in the village square or out in front of the court house. The French word for 'the gallows' is 'la potence', which derives from the Latin word 'potentia' meaning 'power'. Foucault wrote about how society was transformed from corporeal punishment (e.g. gallows) to observation and surveillance. In this sense, surveillance has replaced by, or at least been derived from, the gallows.

But we do not live in virtual prisons, at least not ones without some form of agency. And new media, in particular personalized broadcasting, and more specifically networked, wearable computers capable of broadcasting and sharing virally what we see have significant implications for the power dynamics within society. Imagine that prisoners in Foucault's panopticon could look back—imagine they could see their guards and be able to record their interactions. In the *Matrix* movie, where human-beings are reduced to a shared delusional state and serve as batteries to their mechanical overlords, copperheads cannot look back! In Orwell's *1984*, people can't see who is behind the telescreen. But the power of mobilized media that is always on, always able to broadcast, always able to access a network of followers or friends or circles, changes these broader notions of surveillance and oppression. We are entering an age where people can and will not only look back, but in doing so potentially drive social and political change. No one can tell you what the matrix is, but once you've seen it, you are immediately embroiled in the power politics of Sousveillance.

Thus wearing a camera does not necessarily mean we're 'shooting back' against surveillance. We might actually be in favour of both forms of veillance, especially in times of danger or high risk. This is where blogging, Eye Glass (EyeTap), Google Glass ('Project Glass' 2012), practical philosophy and socially responsible design intersect. What was once a fringe of inventors and early adopters is now increasingly, with projects like Digital Eye Glass (EyeTap) and Project Glass, part of the everyday. With mobile and pervasive computing quickly becoming part of our reality, the possibility for sousveillance—that is undersight of political and corporate entities, the 'watchers'—becomes increasingly possible. It is this change, the shift towards mainstream that makes it particularly apropos to rethink the politics of sousveillance. The politics of sousveillance are themselves divisible into those that deal with the channels, media and technology of sousveillance that intern influence power and its efficacy. The efficacy and power of sousveillance is in part influenced by the design of media technologies that channel the message. This relationship between mediated and distributed undersight, technology, communication and the privileging of some political agendas over others happens at the system design stage.

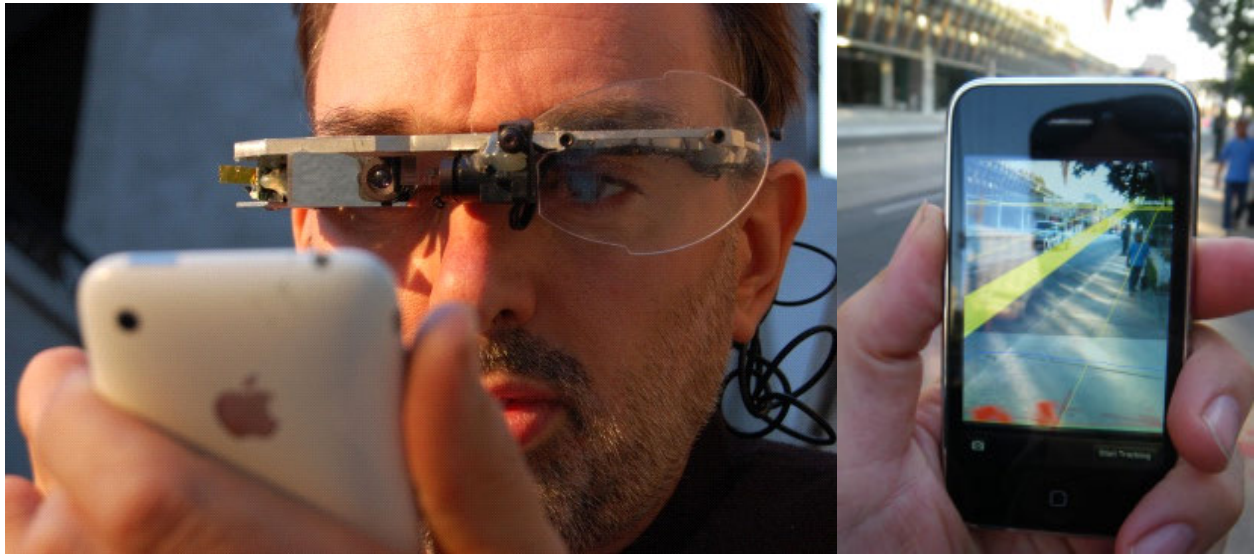


Figure 2: (left) Steve Mann's EyeTap eyeglass and (right) display as it appeared on iPhone in early 2008.
http://www.glogger.mobi/users/mann/image/2009_07_13_21_33_41.jpg

Sousveillance changes the relationships between the asymmetric paradigm for social control that Foucault discussed as the formational characteristics of modern societies—what he termed the panoptic gaze (Foucault 1995). Adding sousveillance to the mix makes the shaping of society more of a continual dialogue between prisoners and guards, politicians and citizens, bureaucrats and people (figure 2). Sousveillance differs critically from surveillance in the relationship of power between the observing gaze and its subject (see figure 3). This relationship implies that there is power in the act of looking back, but it also makes clear that looking back is ‘uphill’, and that even if an individual cannot ‘see’ his guard the looking back provides a kind of back channel, a social check-and-balance to potentially serve as a mechanism for helping to regulate the scope and socio-political boundaries of institutional surveillance practices. Where the viewer is in a position of power over the subject, this is considered surveillance, but where the viewer is in a lower position of power, this is considered sousveillance. Sousveillance represents a ‘gazing’ from below. The viewer is by definition at a lower power potential than the subject of the gaze.

Just as the efficacy of surveillance relies on ‘la potence’ (potency, e.g. ‘the gallows’), the efficacy of sousveillance requires a different kind of ‘potency’ or reciprocal concept, i.e. another force to make the undersight an effective social mechanism for political action and change. We name this force ‘swollag’ (‘gallows’ spelled backwards). This other equalizing force, swollag, although it can be political or economic, is considered here as a socio-technical assemblage of new media and social networks. The coalescing of power through new



Figure 3: Power Relationship between sur- & sous-veillance.

media and its distribution through social networking represents the mechanism for potentially effective oversight. In this power triangle, if the viewer's incline is small, then the efficacy ('swollag') required for effective oversight is relatively little. However, if the inclination is steep, the swollag required for effective change through sousveillance is much greater. The practice of viewing from below when coupled with political action becomes a balancing force that helps—in democratic societies—move the overall 'state' towards a kind of veillance (monitoring) equilibrium, what we refer to as *equiveillance*. Sousveillance may lead to revolutions and uprisings, and could be for example argued to have arisen in the modern state at the very onset of the French Revolution. The storming of the Bastille was itself the flashpoint where distributed power from below was brought to bear on the existing social structure of order and control—the prison (which at the time only housed seven prisoners and had 144 guards). However, it is really since the proliferation of video recording and transmitting, and ubiquitous computing that a major swell in the practices of and effectiveness of sousveillance have become noticeable—and worthy of further study and analysis.

Where the 'sur' in 'surveillance' embodies the metaphoric advantages of the perspective of a high vantage point, and of gravity, sousveillance faces these same conditions as obstetrical to overcome. The strategies by which sousveillance is able to challenge the dominant perspectives, and overcome the pull of corruption through established inertia, are the politics of *sousveillance*. Can 'looking from below' (sousveillance) provide the missing element that oversight alone cannot? Can oversight remedy the power asymmetries of surveillance in democratic societies?

Power Politics of Sousveillance

Foucault's prisoner metaphor is no longer sufficient to describe power relationships mediated by mobile computing and ubiquitous computing enabled by new media. As much as we are subjects of institutional gazes, we are increasingly gazing back at institutions using technology, new media and distributed 'cloud' politics. More akin to the telegraph than to radio or television, new media is not only a channel for unidirectional broadcasting, but incorporates the capacity for feedback and the mechanism for organization and action.

We are not making the claim that sousveillance has not existed in some form throughout the history of human society. But what has changed most recently is the way in which oversight has been affected by technology, through transmission and distribution by new media. New media has enabled a secondary gaze that moves along the power and veillance axis in different directions than surveillance practices. Sousveillance acts as a balancing force in a mediated society. Sousveillance does not exactly or necessarily counteract surveillance, but co-exists with surveillance within a social system that then provides a kind of feedback loop for different forms of looking—potentially creating a balancing force for 'veillance'.

New Media as the Message of Sousveillance

Arguably, sousveillance is more dependent on technology than surveillance—it's harder to 'push back' uphill. Technology is one mechanism that can help mediate the asymmetries of power between a viewer and the subject. In the case of surveillance, technology, as in the case of Foucault's panopticon, can intensify the power of the viewer over the subject. In the case of sousveillance, technology facilitates the observations of the watchers and the ability to mobilize power against a subject at a higher 'institutionalized' position within the system. Although not absolutely necessary for the act of sousveillance, pervasive digital mobile technologies can make sousveillance more effective through transmission and distribution of the archive. Technology extends along the range of veillance by facilitating capabilities, necessary not only to see (and record) the subject, but also to mobilize political force against the power incline.

Technology can play a significant role in sousveillance precisely because looking from below is both practically and metaphorically at a disadvantage (if un-mediated by technology: glasses, telescope, etc.). In this case portable computing has not proved enough. In the early days of the world-wide-web, scholars jumped at the gnostic and democratic potentials of portable computing. As with other technologies, once the initial optimism and excitement begins to wane, people realize that computing and transmission was not itself enough to provide the critical mass necessary to create a cascade of large scale institutional change. In recent years however, mobile networked devices have been combined with social networks that can trigger political disruption and change. Coupling portability, capture, storage and distribution, portable media has allowed us to bring along content, but mobile media (portable media with dedicated internet infrastructures) provides significant opportunities for individuals not only to capture records of abuse of power or corruption, but also to quickly distribute and communicate it to others for political action. For example, a PSD (Personal Safety Device) that simply transmits and records data at a remote location protects it from being destroyed by an attacker or perpetrator, regardless of whether the perpetrator is a low-level street thug, or a corrupt police officer, of possibly high rank.

Case Study in Sousveillance: Lifeglogging

The application of distributed power of individuals and masses has been increasingly mediated through the 20th and 21st centuries. One particular area of sousveillance is lifecasting, also known as cyborglogging, glogging, lifeglogging, lifelogging, or the like. The first person to do lifecasting, i.e. stream continuous live first-person video from a wearable camera, was the co-author, Steve Mann, with his ‘Wearable Wireless Webcam’. Mann’s experiments with wearable computing and streaming video began in the early 1980s in Canada, and the early 1990s at MIT. Starting in 1994, Mann continuously transmitted his everyday life 24 hours a day, seven days a week, and his site grew in popularity to become Cool Site of the Day in 1995. Using a wearable camera and wearable display, he invited others to both see what he was looking at, over the web, as well as send him live feeds or messages in real time. In 1998 Mann started a community of lifecasters which has grown to more than 100,000 members.

Following Mann’s example, a number of other early pioneers joined the ranks of lifecasting. Jennifer Ringley’s JenniCam (1996–2004) attracted mass media attention, as noted by Cnet: ‘JenniCam, beginning in 1996, was the first really successful “lifecasting” attempt’. Ringley appeared on talk shows and magazines covers, and her pioneering effort was followed by collegeboyslive.tv and MagicsWebpage.tv (1998). That same year, the streaming of live video from the University of Toronto became a social networking phenomenon. Also, Lisa Batey and HereAndNow.net started streaming 24/7 in 1999, continuing into 2001. And, ‘We Live In Public’ was a 24/7 internet conceptual art experiment created by Josh Harris in December 1999. With a format similar to TV’s *Big Brother*, Harris placed tapped telephones, microphones and 32 robotic cameras in the home he shared with his girlfriend, Tanya Corrin. Viewers talked to Harris and Corrin in the site’s chatroom. Zac Adams’ *CollegeBoysLive* (1998–present) became the first live reality site featuring a group of unrelated gay guys living in a house together. *CollegeBoysLive* chose random people to live in the house and have their lives broadcast 24/7.

These artistic, political and entertainment uses of new media and social networking to establish communities around the streaming of regular lives has significant implications for oversight and the overall power relationships of gazing. Whereas radio and television generally provided curated and produced materials from centralized broadcasters, lifecasting gathered and broadcast ubiquitous information from below. With 24/7 streaming ‘incidental’ observations, events are captured as part of the continuous channel of information. Events captured by ordinary people then become an unofficial official record of events that may be used to challenge to authoritative history. What’s more is that these incidental vignettes of life become more ‘real’ than the ‘reels’ of truth produced by centralized media channels. Although lifecasting potentially includes forms of oversight, as is the case with much of

surveillance, most of the content is every day and banal. Lifecasting does nevertheless demonstrate the potential of mobile and pervasive media for marginal narratives and ‘news’.

Until recently most people didn’t care much about this work, or how it might shape society. But recently (in the last 12 years), Steve Mann has been called ‘the father of AR’ and ‘the father of wearable computing’ (first at the IEEE International Solid-State Circuits Conference, February 2000), which is now a \$241 billion industry. Now many people use smartphones for AR (Augmented Reality), or simply to help failing eyesight by photographing and magnifying something, or perhaps to translate a foreign restaurant menu into their own language using an optical character recognition app. But a new way of seeing is not without social issues. Penny Sheldon, a travel agent from Boise, Id., was physically assaulted by McDonald’s staff in Paris, France, (the same place Mann was assaulted by McDonald’s staff) because she photographed their menu.

As AR and personal technologies enter the mainstream, we are at a pivotal era where the questions we are asking require answers! For example, Google is making an eyeglass product that resembles Mann’s ‘Eye Glass’ (‘EyeTap’) in both form and function, and we have heard that Google has contacted McDonald’s Head of Security to learn from Mann’s experience. Photography, whether used as a seeing aid, for AR, or just to understand the world around us, is being prohibited by overzealous security forces who at the same time are installing surveillance cameras all around us. Thus we coin the term ‘McVeillance’ to denote the ratio between surveillance and sousveillance, or the ratio of permissibility of surveillance to sousveillance. McVeillance is the opposite of equiveillance (equality of surveillance and sousveillance and their equal acceptance in a society).

In more recent years wearable computing technology has been integrated seamlessly into social networking sites, with more than 100,000 users (e.g. www.glogger.mobi)—an example appears in figure 2. More recently, others such as Nokia, Apple, Microsoft, Hewlett Packard, and Google, are commercializing similar wearable computing devices (see for example figure 4).



Figure 4: Glass (left), ‘Digital Eye Glass’, (right) Google’s ‘Project Glass’ [16] (image adapted from Antonio Zugaldia’s picture on Wikimedia Commons).

The significance here is not just of augmented reality, but the potential transformative scale of such an idea being backed by large corporations. Beyond just integrating programs like Google Streetview and e-mail or even augmented reality or mediated reality into the daily lives of a few early adopters, the wearable computing field may help integrate mobile computing into our daily sense-making and wayfinding. Wearable Computing represents a step towards ubiquitous information by way of bi-directional streaming and computer-aided sense making. But it also potentially represents a movement

towards ubiquitous personal image, audio and video capture and sharing. In addition to accessing and consuming, these kinds of technologies can turn every wearer into an information production factory—a sousveillance-capable post-cyborgian human. This form of open-circuit life streaming, among other things, inverts the dynamics of institutional practices of looking such as CCTV (closed-circuit television) and organizational video surveillance.

The Politics of Sousveillance

What was once a fringe of inventers and early adopters is now increasingly, with Wearable Computing and Augmented Reality, part of the everyday. With mobile and pervasive computing quickly becoming part of our reality, the possibility for sousveillance, that is undersight of political and corporate entities, the ‘watchers’, becomes increasingly possible. It seems then particularly apropos to rethink the politics of sousveillance. This paper is the beginning of this project.

The politics of sousveillance are themselves divisible into those that deal with the channels, media and technology of sousveillance and those that deal with the power of its efficacy. Three cases to consider:

1. Veillance and power are of equal forces;
2. Veillance is greater than power;
3. Power is greater than veillance.

In the first case, where the mechanism of undersight and the power required to enact change are approximately equal, a kind of *equiveillance* (a balance of forces between oversight and undersight) is achieved. In this case, both the acts of looking from below and the power mechanism necessary to enact change from below are in a state of balance with surveillance from above. That is to say, the society has an effective feedback mechanism where undersight is an effective tool of monitoring the overseers. Although difficult to quantify, it may be said that the mechanisms or forces of surveillance and sousveillance form a democratic homeostasis (figure 3).

The Gaze: Veillance & Power

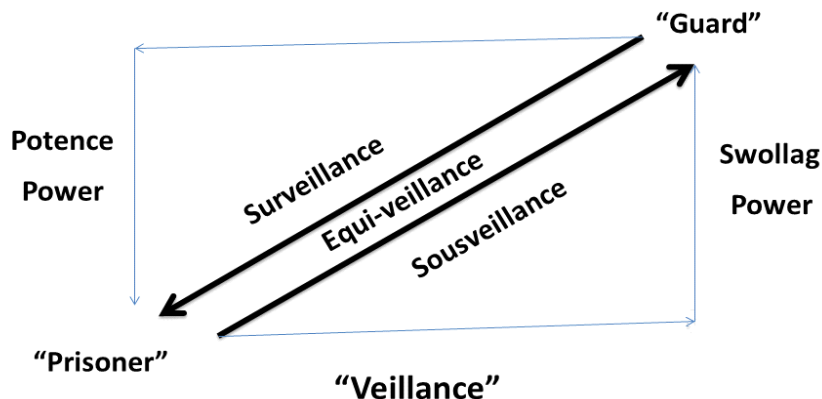


Figure 5: Power Relationships in forms of Veillance

In the second case (figure 5) the powers of sensing and ‘seeing’ what the over-seers are up to is extensive. Since very little power is needed here to challenge the power incline and the mechanism of sensing or oversight are extensive, the society, in this case, can be said to be a transparent one. A transparent society then becomes one where veillance infrastructures are extensive and the power requirements to enact change from below are marginal. This type of system would likely protect whistle-blowers, encourage public fora and debate, and implement participatory projects and innovations to the system. Even the powers of oversight in this configuration are likely to be seen from below and subject to evaluation.

Gentle Slope for Sousveillance

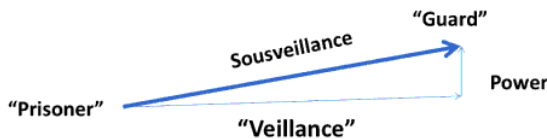


Figure 6: Gentle Slope of Sousveillance

Steep Slope of Sousveillance



Figure 7: Steep Slope of Sousveillance

In the final case (figure 6), the mechanisms and strategies of veillance are limited and restricted. Where the axis of power is a significantly larger vector than the mechanism of sousveillance, significant mobilization is needed to enact change. Here the channels of sousveillance require significant political, ideological and even coercive force to enact change. The slope between the viewer and its institutional agent is so steep that seeing, witnessing, recording and even distributing images and video of corruption and wrongdoing is not likely enough to motivate political action. In this case, other strategies are required. For example, in 2012 when the US government proposed legislation to ‘snoop’ on internet users and providers, GoDaddy.com a major ISP came out in support of the legislation. Despite many client requests from below, it wasn’t until an organized movement of people to leave the provider, and an exodus of over 20,000 clients (including Wikipedia) in several days, that GoDaddy.com reversed its support for the legislation.

The channels of sousveillance are increasingly becoming less visible and potentially ubiquitous. This is itself problematic and exciting. In the infancy of portable computing it was easy to see when and if someone was taking an image or a video with a cell phone or portable camera. Often agents of surveillance will react poorly to mobile recording equipment, citing the potential criminal uses of the recordings. For example, banks are reluctant to share images of people acquired by their surveillance systems, in part because they claim that the images they capture might then be used to figure out a way of avoiding their cameras or avoiding optimal camera angles. Mann and Ferenbok (2012) have described instances where grocers prohibit cell phones and cameras on their premises while at the same time selling items with hyper-codes that require and promote online and augmented interactions (i.e. the process of consumption actually requires the very cell phones and cameras that are being prohibited). The absurdity of this juxtaposition demonstrates the anecdotal reticence on the part of individuals acting as ‘panoptic’ guards to themselves being watched and subjected to surveillance.

It could be that they fear accountability, or it could simply be that guards don't like to be guarded by others who they consider to be from a lower 'rung' of the social 'ladder'. For example, police, as in the G20 summit in Toronto, did not respond well to being photographed in public while they were supposedly working for the public. Is it that somehow these authoritarians understand that sousveillance represents not only a challenge to its institutional gaze, but also a reminder of the limits of the power of surveillance?

The ability to record (i.e. to 'make record(s)') of, an individual's viewpoint (likely directly from the ocular nerve in future iterations), represents an interesting change to the conception of secrecy, privacy, and 'publicity', in the context of our daily lives. We will be surveilled but will also be able to sousveill both in real-time and backwards in time ('retroactive record') through our personal and or public profiles. Wearable computing not only enables us to see the world augmented and mediated by technology, but it also allows what we are seeing to be broadcast and recorded for others.

Wearable Computing and augmented reality (AR) technologies make human-computer interaction seamless and invisible. This means that historically specific prohibitions will likely vanish into the margins, heralding a time where individuals can continuously capture and share visual and experiential sensing information. Social networking sites or hubs like Twitter, Facebook, and Youtube then become potential distribution channels for individual broadcasting that can mobilize distributed power into networks of social action and political change, as can be argued was the case with 'Officer Bubbles' who was brought to charges because of a viral video and eventually was forced to reveal names of other officers abusing their powers during the G20 summit in Toronto (*Huffington Post* 2012).

The looking back of individuals onto the practices of institutions will by necessity change the way institutional and state surveillance systems are organized, implemented and managed. An individual who accuses a police officer of brutality will, in our immediate sousveillant future, have made a record of the event—a recording that will likely be stored and shared almost instantaneously. This of course does not guarantee that institutional changes will move towards more open and transparent practices, and it seems that at the cusp of these social upheavals.

Sousveillance and Technology

Arguably, sousveillance is more dependent on technology than surveillance—it's harder to 'push back' uphill. Mobile and pervasive media technologies are *one* mechanism that can help mediate the asymmetries of power between a viewer and the subject. In the case of surveillance, technology, as in the case of Foucault's panopticon, can intensify the power of the viewer over the subject. In the case of sousveillance, technology facilitates the observations of the watchers and the ability to mobilize power against a subject at a higher 'institutionalized' position within the system. Although not absolutely necessary for the act of sousveillance, pervasive digital mobile technologies can make sousveillance more effective through transmission and distribution of the archive. Technology extends along the range of veillance by facilitating capabilities, necessary not only to see (and record) the subject, but also to mobilize political force against the power incline.

Technology and its flexible and open design can play a significant role in sousveillance precisely because looking from below is both practically and metaphorically at a disadvantage (if un-mediated by technology, such as glasses, telescope, etc.). In this case portable computing has not proved enough. In the early days of the world-wide-web, scholars jumped at the gnostic and democratic potentials of portable computing. As with other technologies, once the initial optimism and excitement begins to wane, people realize that computing and transmission was not itself enough to provide the critical mass necessary to create a cascade of large scale institutional change. In recent years, however, mobile networked devices have been combined with social networks that can trigger political disruption and change. Coupling portability, capture, storage and distribution, portable media has allowed us to bring along content, but

mobile media (portable media with dedicated internet infrastructures) provide significant opportunities for individuals not only to capture records of abuse of power or corruption, but also to quickly distribute and communicate it to others for political action. For example, a PSD (Personal Safety Device) that simply transmits and records data at a remote location protects it from being destroyed by an attacker or perpetrator, regardless of whether the perpetrator is a low-level street thug, or a corrupt police officer, of possibly high rank. With media, we become sousveillance-enabled individuals able to contribute to a broader social responsibility of oversight. However, where the storage and custodianship of the information streamed becomes the property of a corporation, whether sousveillance-enabled individuals contribute to oversight or become co-opted into complicit drones in corporate and larger government surveillance networks, remains to be seen.

Established Norms and Oversight

‘Recording’ or any kind of mediated oversight has traditionally been feared by institutional agents, and as we transition to a mass-streaming society, oversight will continue to instil fear among proponents of the one-sided but obsolete surveillance-only society. The idea of being filmed and broadcast has until recently remained a socially undesirable process. In actuality, the very foundations of North American Privacy legislation stem from the acknowledgement of the right to be left alone from photographic observation (Warren and Brandeis 1890)—the intrusion of media into the lives of others. Surprisingly this fear is not just limited to the corrupt or criminal. Concerns have been raised about the ability of professionals to carry out their duties while under constant scrutiny. Police have been particularly vocal in this debate—going to the lengths in some US states to try to stop public recordings of police officers carrying out their duties. In Boston, a lawyer witnessing police indiscretion was arrested for taking pictures in a public space. Upon the successful legal challenge to the arrest of Mr. Glik (ACLU of Massachusetts 2012) and the police conduct in the matter, the city of Boston has promised to introduce sensitivity training to make police aware that they are not beyond the reach of sousveillance in public spaces.

In the city of Toronto another kind of reaction to sousveillance occurred in 2010. After several incidents of transit workers being ridiculed for, among other behaviours, sleeping on the job and texting while driving, the union came out strongly against the sousveillance of their employees on the job (CBC News 2012) and another texting while driving (CNet 2012). Agents of the transit system became sensitive towards public scrutiny, and belligerent at the sight of media hardware. However, the political potency of this type of oversight can potentially improve otherwise opaque public services. Portable media technologies that help facilitate and support the exchange of individual perspectives and experiences can help support a greater dialogue in society between the watchers and the prisoners watching the watchers. This dialogue is significant because it points to an overall restructuring of society that moves beyond the Foucauldian asymmetric triangle into a networked framework that accounts for monitoring both by institutional agents and individual citizens within a particular system (Murakami Wood 2009). This shift from understanding society as strictly an oversight system, versus one that has potential to be multi-channelled, suggests both the importance of social responsibility of systems design and the importance of socially responsible design for the shaping of the democratic infrastructures of society.

Conclusion: Sousveillance with swollag

For sousveillance to have efficacy, it must comprise either a large network of large numbers of low-grade participants, working with little or no effort or ability (‘power’), or a smaller communities of more active ‘sousveillance officers’ like at the ‘The Office of Community Sousveillance’ in Nottingham City Centre, England. Sousveillance, by its nature, tends to be distributed, so its efficacy (‘swollag’) would naturally be enhanced by widespread adoption, where its swollag is distributed through a large network, rather than smaller groups from the ‘likes’ of hacktivism.

Much of the world's intellectual property battleground, as well as AR product manufacture, is based in the United States. And the United Kingdom is often said to be the surveillance capital of the world. Asia is also becoming a surveillance society. But early adopters of sousveillance technologies have the opportunity (and moral and ethical duty!) to position themselves at the forefront of this research, inquiry, and be the voice-of-reason in a world otherwise dominated by the one-sided gaze of surveillance. The ability to share and upload visual documents as records is changing who watches the watchers. In a media driven democratic state, everyone is subject to observation ('veillance'), even the observers themselves. The relationships of power (and swollag) between the individual viewer and the institutional viewer become a combination of the technological mechanisms of sense making (the veillance axis) and the relationships of power supporting the mechanisms of over- and oversight. Moreover, the political potency of this type of oversight can potentially improve otherwise opaque public services.

References

- ACLU of Massachusetts. 2012. City of Boston pays \$170,000 to settle landmark case involving man arrested for recording policy with cell phone, March 31, 2012. Retrieved from http://aclum.org/news_3.27.12
- Bakir, V. 2010. *Sousveillance, media and strategic political communication: Iraq, USA, UK*. Continuum International Publishing Group.
- Ball, K.S. and K.D. Haggerty. 2005. Editorial: Doing Surveillance Studies. *Surveillance & Society* 3(2/3): 129-138.
- Ball, K.S., D. Lyon, D. Murakami Wood, C. Norris and C. Raab. 2006. *A Report on the Surveillance Society : For the Information Commissioner by the Surveillance Studies Network*. Wilmslow, UK: Office of the Information Commissioner.
- CBC News. 2010. TTC to investigate 'sleeping' fare collector, Jan 22, 2010. Available at <http://www.cbc.ca/news/canada/toronto/story/2010/01/22/snoozing-ttc.html>
- CNews. 2012. Subway driver caught texting. (2012, Apr 22). Retrieved from <http://cnews.canoe.ca/CNEWS/Canada/2012/04/22/19664456.html>
- Coaffee, J. and Murakami Wood, D. 2006. Security is coming home: rethinking scale and constructing resilience in the global urban response to terrorist risk. *International Relations*, 20(4): 503-517.
- Dennis, K. 2008. Viewpoint: Keeping a close watch—the rise of self-surveillance and the threat of digital exposure. *Sociological Review* 56(3): 347-357.
- Elmer, G. 2003. A diagram of panoptic surveillance. *New Media & Society* 5(2): 231-247.
- Ferenbok, J. and A. Clement. 2012. Hidden Changes: from CCTV to 'Smart' video surveillance. In: *Eyes Everywhere: The Global Growth of Camera Surveillance*, eds A. Doyle, R. Lippert and D. Lyon. London: Routledge.
- Foucault, M. 1982. The Subject and Power. *Critical Inquiry* 8(4): 777-795.
- Foucault, M. 1995. *Discipline and Punish: The birth of the prison* (A. Sheridan, Trans. 2nd ed.). New York: Vintage Books.
- Fraser, D.T.S. 2007. Alberta Commissioner upholds camera in locker rooms at health club. Retrieved from <http://blog.privacylawyer.ca/2007/03/albertacommissioner-upholds-cameras-in.html>
- Haggerty, K.D. and R.V. Ericson. 2000. The surveillant assemblage. *British Journal of Sociology* 51(4): 605-622.
- Huffington Post. 2012. Toronto Police Commanders Face G20 Charges. (2012, May 17). Retrieved from http://www.huffingtonpost.ca/2012/05/17/toronto-g20-charges_n_1525309.html
- Lyon, D. 1994. *The Electronic Eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.
- Lyon, D. 2001. *Surveillance Society*. Buckingham: Open University Press.
- Mann, S. and J. Ferenbok. 2012. *Ski Googles and Streetview Sousveillance: The politic of police, piercings, and prosthetics in the era of post-Cyborgian Primitives*. Paper presented at the The Fifth Biannual Surveillance & Society Conference, 'Watch This Space: Surveillance Futures'. April 2012, Sheffield. http://wearcam.org/sousveillance_and_society.htm
- Mann, S., J. Nolan and B. Wellman. 2003. Sousveillance: Inventing and Using Wearable Computing Devices. *Surveillance & Society* 1(3): 331-355.
- Monahan, T., ed. 2006. *Surveillance and security: Technological politics and power in everyday life*. New York: Routledge.
- Murakami Wood, D. 2007. Beyond the Panopticon? Foucault and surveillance studies. In: *Space, Knowledge and Power: Foucault and Geography*, eds J. Crampton and S. Elden, 245-263. Aldershot: Ashgate.
- Murakami Wood, D. 2009. The Surveillance Society 'Questions of History, Place and Culture. *European Journal of Criminology* 6(2): 179-194.
- Murakami Wood, D. and C.W.R. Webster. 2009. Living in Surveillance Societies: The normalization of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research* 5(2): 259-273.
- Norris, C. and G. Armstrong. 1999. *The Maximum Surveillance Society: the Rise of CCTV*. Berg: Oxford.
- Norris, C., M. McCahill and Wood, D. 2004. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publically accessible space. *Surveillance & Society* 2(2/3): 110-135.
- Pixelview. *Lighting Science*. Retrieved August 15, 2007, from <http://www.lsgc.com/pixelview/>
- Project Glass. 2012. Retrieved from <https://plus.google.com/u/0/111626127367496192147/posts>

- Reuter, C. 2000. *The V2 and the German, Russian and American Rocket Program*. New York: S.R. Research and Publishing.
- Silverman, K. 1984. *The subject of semiotics*. New York: Oxford University Press.
- Warren, S.D. and L.D. Brandeis. 1890. Right to Privacy. *Harvard Law Review* 4(5).