Surveillance & Society 1(3): 331-355
http://www.surveillance-and-society.org

Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*

Steve Mann[1], Jason Nolan[2] and Barry Wellman[3]

Abstract

This paper describes using wearable computing devices to perform "sousveillance" (inverse surveillance) as a counter to organizational surveillance. A variety of wearable computing devices generated different kinds of responses, and allowed for the collection of data in different situations. Visible sousveillance often evoked counter-performances by front-line surveillance workers. The juxtaposition of sousveillance with surveillance generates new kinds of information in a social surveillance situation.

Being Surveilled

> These days, if you feel like somebody's watching you, you might be right. One year after the Sept 11 attacks, security experts and privacy advocates say there has been a surge in the number of video cameras installed around the country [U.S.]. The electronic eyes keep an unwavering gaze on everything from the Golden Gate Bridge to the Washington Monument…. [For example,] a group of anti-surveillance activists [say]… they have seen a 40% increase in new cameras in New York's financial district since last September [2001] (Evangelista 2002).
>
> VIDEO_SURVEILLANCE and its regime of control… the banalization or popularization of global surveillance, or to put it another way, the DEMOCRATIZATION OF VOYEURISM on a planetary scale, has overexposed even our most private activities. So doing, it has exposed us

* We appreciate the advice and assistance of Kathleen Pirrie Adams, Chris Aimone, James Fung, Angela Garabet, Thomas Hirmer, Adwait Kulkarni, Betty Lo, Sharon and Corey Manders, Jennifer Marchand, Andrew Ng, Samir Parikh, Katherine Parrish, Monica Prijatelj, Uyen Quach, Rhonna Robbins-Sponaas, and Felix Tang. The performances described here were supported in part by the Canada Council for the Arts.
[1] Electrical and Computing Engineering, University of Toronto, mailto:mann@eecg.toronto.edu
website: http://www.wearcam.org
[2] Knowledge Media Design Institute, University of Toronto, mailto:jason@jasonnolan.net
website: http://www.jasonnolan.net
[3] Sociology, University of Toronto, mailto:wellman@chass.utoronto.ca
website: http://www.chass.utoronto.ca/~wellman

 ISSN: 1477-7487

> to a major iconic risk. In the best case, only marketing specialists can gauge the amplitude of this risk; in the worst, the military, investigators charged with tracking unlawful activities, political police, and automated systems for information collection… (Virilio 2002: 109).
>
> [They] felt meaningless unless they were being observed and this was the reason they all observed and took snapshots and movies of each other, for fear of experiencing the meaninglessness of their existence… staggering along in mad hope of somehow finding someone to be observed by somewhere… (Dürrenmatt 1988: 20).
>
> For decades, the notion of a "surveillance society" where every facet of our private life is monitored and recorded has sounded abstract, paranoid or far-fetched to some people. No more!… Yet too many people still do not understand the danger, do not grasp just how radical an increase in surveillance by both the government and the private sector is becoming possible … from a number of parallel developments in the worlds of technology, law and politics. (Stanley and Steinhardt 2003: iv)
>
> I feel okay with everyone picture-taking (and even everyday WebCam taking), but am uncomfortable with the video surveillance cameras that seem, these days, to be everywhere, rising over our city streets on high poles, looming over our neighbourhood stores, banks, schools and parks (Mann 1998: 140).

Sousveillance: Surveilling the Surveillers

These disparate observers are reacting to the pervasiveness of surveillance in contemporary western society (Stanley and Steinhardt 2003). Such surveillance is everywhere but often little observed. Organizations have tried to make technology mundane and invisible through its disappearance into the fabric of buildings, objects and bodies. The creation of pervasive ubiquitous technologies—such as smart floors, toilets, elevators, and light switches—means that intelligence gathering devices for ubiquitous surveillance are also becoming invisible (Mann and Niedzviecki 2001; Marx 1995; Lefebvre 1991). This re-placement of technologies and data conduits has brought new opportunities for observation, data collection, and sur/sousveillance, making public surveillance of private space increasingly ubiquitous.

All such activity has been *sur*veillance: organizations observing people. One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority. We call this inverse panopticon "*sous*veillance" from the French words for "sous" (below) and "veiller" to watch.

Sousveillance is a form of "reflectionism," a term invented by Mann (1998) for a philosophy and procedures of using technology to mirror and confront bureaucratic organizations. Reflectionism holds up the mirror and asks the question: "Do you like what you see?" If you do not, then you will know that other approaches by which we integrate society and technology must be considered. Thus, reflectionism is a technique for inquiry-in-performance that is directed:

a) toward uncovering the panopticon and undercutting its primacy and privilege;
b) relocating the relationship of the surveillance society within a more traditional commons notion of observability.

Reflectionism is especially related to "detournement": the tactic of appropriating tools of social controllers and resituating these tools in a disorienting manner (Rogers 1994). It extends the concept of detournement by using the tools against the organization, holding a mirror up to the establishment, and creating a symmetrical self-bureaucratization of the wearer (Mann 1998). In this manner, reflectionism is related to the Theater of the Absurd (Bair 1978), and the Situationist movement in art.

Reflectionism becomes sousveillance when it is applied to individuals using tools to observe the organizational observer. Sousveillance focuses on enhancing the ability of people to access and collect data about their surveillance and to neutralize surveillance. As a form of personal space protection, it resonates with Gary Marx's (2003) proposal to resist surveillance through non-compliance and interference 'moves' that block, distort, mask, refuse, and counter-surveil the collection of information.

Reflectionism differs from those solutions that seek to regulate surveillance in order to protect privacy (Rhodes, et al. 1999). Reflectionism contends that such regulation is as much pacifier as solution because in a regulatory regime, surveillance information is largely exchanged and controlled by external agents over which individuals have little power. For example, a recent regulatory proposal from the American Civil Liberties Association suggests:

> surveillance cameras … must be subject to force-of-law rules covering important details like when they will be used, how long images will be stored, and when and with whom they will be shared" (Stanley and Steinhardt 2003: 2).

By contrast, reflectionism seeks to increase the equality between surveiller and the person being surveilled (surveillee), including enabling the surveillee to surveil the surveiller.

Probably the best-known recent example of sousveillance is when Los Angeles resident George Holliday videotaped police officers beating Rodney King after he had been stopped for a traffic violation. The ensuing uproar led to the trial of the officers (although not their conviction) and serious discussion of curtailing police brutality (Cannon 1999). Taping and broadcasting the police assault on Rodney King was serendipitous and fortuitous sousveillance. Yet planned acts of sousveillance can occur, although they are

rarer than organizational surveillance. Examples include: customers photographing shopkeepers; taxi passengers photographing cab drivers; citizens photographing police officers who come to their doors; civilians photographing government officials; residents beaming satellite shots of occupying troops onto the Internet. In many cases, these acts of sousveillance violate stated or prohibitions stating that ordinary people should not use recording devices to record official acts. At times, these prohibitions are stated. For example, many countries prohibit photographing military bases. More often, these prohibitions are unstated. For example, although many large stores do not want photographs taken on their premises, we have never seen a sign prohibiting such photography.

The Rise of Neo-Panopticons

Privacy is a psychological as well as a social and political requirement. For instance, people seek control over the degree of anonymity they possess in their relationships by choosing what personal information to reveal to another person based upon their relationship (Ingram 1978). Yet, the asymmetrical nature of surveillance is characteristic of an unbalanced power relationship. As Ingram suggests, the power that the police or customs officers assert when they search a person's belongings or the contents of their pockets, when the officers themselves cannot be searched, reflects a relationship firmly located in the panopticon, and is seen in the asymmetric photography/video policies of the examined establishments themselves.

However, the notion of ubiquitous surveillance is longstanding. Jeremy Bentham's (1838) Panopticon defined a system of observation in which people could be placed under the *possibility* of surveillance without knowing whether they were actually being watched. Bentham proposed such an architecture for use in prisons, schools, hospitals, and workplaces. The implications of this system are described by Foucault:

> [T]he major effect of the Panopticon [is] to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers (Foucault 1977: 201).

Bentham's ideas represented an updating of governance techniques in pre-industrial societies for Industrial Revolution societies. The densely-knit connections and tight boundaries of pre-industrial "door-to-door" communities fostered direct visual observation as a means of social control (Ostrom 1990; Wellman 1999, 2001). With the Industrial Revolution, societal scale increased beyond the ability for little groups of neighbors to eye one another. There was a perceived need for industrialized social control.

Hence, panopticons employed hierarchies of organizational employees to observe public spaces in prisons, factories, etc. Indeed, "panopticism was a technological invention in the order of power, comparable with the steam engine" (Foucault 1980b: 71; see also Foucault 1977, 1980a).

In post-Industrial societies, new communication techniques are exploited by neo-panopticons. In public or semi-public (e.g. commercial) locations individuals are liable to become unwilling and sometimes unknowing subjects of surveillance, and the knowledge that they may be under surveillance may be sufficient to induce obedience to authority (Foucault 1977). Recall the television show, *The Prisoner* (McGoohan and Tomblin 1967) set in an ostensibly bright and cheery village under constant video surveillance. The pastoralism on the surface is enforced by a panopticon.

Since that comparatively ancient time, surveillance techniques have increasingly become embedded in technology. Where people once watched people with their naked eyes, computer-aided machines now do remote sensing of behavior. Automatic messages inform callers to organizational "call centers" that their conversations are being monitored to "improve customer service". Surveillance cameras are spreading rapidly through public space. "A survey of surveillance cameras in Manhattan, for example, found that it is impossible to walk around the city without being recorded nearly every step of the way" (Stanley and Steinhardt 2003: 2). Video cameras can be almost invisibly small, communication networks, directing surveillance images to monitors (both people and screens) located elsewhere, and information technology can use facial recognition software to identify likely suspects. Those subject to neo-panopticons do not have direct visual and aural contact with those who are observing. Yet, they may be thrust into private jails that big retail chains maintain to hold observed deviants (Elliott 2003).

They are subjects being monitored in two senses of the word. First, they are subjects of observation on video monitors displaying and previewing the acquisition of their image. In this sense, they are subjects of the camera (as in the "subject matter" of a photograph). Second, subjects are under the potential control of people in positions of authority who are organizational monitors of their behavior. They are like the subjects of a king, a dictator, authority figure, or organizational institution. And the situation created *by* technology mediated surveillance creates an imbalance in terms of who can undertake these forms of surveillance.

There is a digital divide in the unequal access to these technologies by the general public. The proliferation of environmental intelligence, in the form of cameras and microphones observing public spaces, challenges the traditional ability of an individual being able to identify and watch the watchers. The collection of data in public places, with the camera as the dominant form of data input device, is coupled with the integration of surveillance with statistical monitoring and security applications. The passive gathering of intelligence represents a challenge to privacy in public places that has been largely accepted (Mann 2000; Webster and Hood 2000).

Even before the personal computer revolution, other efforts were made to attach computing technology to the body (Mann 1997, Mann and Niedzviecki 2001). Systems were developed to provide electrical connections to and from the body, as well as multimodal sensory interfaces. These allowed remote control of the body by wireless communications. EyeTap (www.eyetap.org) technology also evolved as a system for causing the eye itself to function as if it were both a camera and a display (Mann and Niedzviecki 2001). This allowed the devices to modify visual perception, thus setting the stage for an interface to the body that challenged the notion of free-agency and locality of reference.

Wearable Computing for Sousveillance

Digital technology can build on personal computing to make individuals feel more self-empowered at home, in the community, at school and at work. Mobile, personal, and wearable computing devices allow people to take the personal computing revolution with them. Sousveilling individuals now can invert an organization's gaze and watch the watchers by collecting data on them.

The development of wearable computing fits well with contemporary social transformations. While surveillance is a manifestation of the industrial and post-industrial eras of large hierarchical organizations that have efficiently employed technologies in neo-panopticons of social control, there is now a turn from such organizations to "networked societies" (Wellman 1999, 2001; Castells 2000). Rather than being embedded in single communities or work groups, individuals switch among multiple, partial communities, and work teams. They move about, both socially and physically. Where centralized mainframe computers served the needs of large hierarchical organizations, personal computers better fit the needs of people in networked organizations and communities who move with some autonomy among geographically and socially dispersed work teams, friends and activities. Yet personal computers are still rooted to desktops at the office and tabletops at home. They are still wired into computer networks. Wearable, wireless computers better fit the needs of people to be physically mobile as they move between interactions with workmates and community members. As the developed world transforms from small-group to person-to-person interactions, they are a powerful tool for personal empowerment.

We describe here an attempt to use newly invented forms of wearable computing (Mann 1997, Mann 2001a) to empower individuals in at least some aspects of their encounters with organizations[4]. These inventions call into question Aldous Huxley's assertion that "technological progress has hurt the Little Man and helped the Big Man" (Huxley 1958:43). We examine how using wearable computing devices can promote personal empowerment in human technology/human interactions (Mann 1997; Fogg 1997). Two key issues are the extent to which organizational surveillance can be challenged, and the

[4] Steve Mann invented the apparatus, designed the performances, and did the performances together with his students as described in http://www.eyetap.org and http://www.wearcam.org/adwear/index.htm

ways in which organizations respond to such challenges. We describe and analyze here a set of performances that follow Harold Garfinkel's ethnomethodolgical approach to breaching norms (1967). We gain insight into these norms by: (a) deliberately not acquiescing in surveillance, and (b) performing visible and explicit sousveillance. By breaking organizational policies, these performances expose hitherto discreet, implicit, and unquestioned acts of organizational surveillance.

More active forms of sousveillance confront surveillance by using wearable computing to surveil the surveillers reflectively, bringing into question the very act of surveillance itself. Because of the mobility of the modern individual, this act is best accomplished by mobile, wearable computers. In the mobile society of the early twenty-first century, Western societies move among milieus. Their personal environments travel with them in the unstable environment of ostensibly neutral public spaces such as streets, sidewalks, shopping malls, etc. (Lefebvre 1991; Wellman 2001). In such milieus, individuals are largely responsible for their own security and integrity. Wearable computing devices afford possibilities for mobile individuals to take their own sousveillance with them. Given this frequent sociophysical mobility, it makes sense to invent forms of wearable computing to situate research devices on the bodies of the surveilled (customer, taxicab passenger, citizen, etc.). The act of holding a mirror up to society, or the social environment, allows for a transformation of surveillance techniques into sousveillance techniques in order to watch the watchers.

The goal of the performances reported here is less to understand the nature of surveillance than to engage in dialogues with front-line officials and customer service personnel at the point-of-contact in semi-public and commercial locations. With Gary Marx, we are interested in how "the relationship between the data collector and the subject may condition evaluations, as may the place" (1998: 176). We attempt, as a systems analyst might, to engage our points of contact (managers, clerks, security workers, etc.) without claiming to understand complicated internal hierarchical considerations or politics within large bureaucratic, sometimes multinational, organizations. Instead, the performers instigate situations in order to:

(a) gauge the degree to which customer service personnel will try to suppress photography in locations where it is forbidden;
(b) (break unstated rules of asymmetric surveillance using new wearable computing inventions (Mann and Niedzviecki 2001).

The collecting of digital images, via photographs or videos, is usually prohibited by store personnel because of stated policy, explicit norms, or unconscious norms that are only realized when they are breached. The surveilled become sousveillers who engage social controllers (customs officials, shopkeepers, customer service personnel, security guards, etc.) by using devices that mirror those used by these social controllers.

Uncertainty surrounds these performances; no one is ever sure of the outcome of the interaction between device, wearer, and participants. Design factors can influence performances: the wearing of technology can be seen by participants as either

empowering or threatening, depending on the type of technology, location, and how it is presented and represented. For example, people who use familiar mobile devices, such as laptop computers and personal digital assistants, are perceived as more socially desirable than those with less familiar devices, such as wearable computers and hands-free mobile phones (Dryer, et al. 1999).

Research Expectations

We present accounts of five performances held in 2001 that were designed to allow ordinary people to use sousveillance-enabling wearable computing devices. Each performance responds to different situations in which sousveillance techniques can be used to explore surveillance situations. The performances range from situations in which passers-by are shown how they may passively become the subjects of observation (Performances One and Two), to situations in which sousveillance, using covert and overt wearable computing devices, engages organizational surveillance (Performances Three, Four, and Five). The performances were held in streets, shops, restaurants, shopping malls, and department stores in a major shopping district of a large English-Canadian city. Hundreds of people actively participated in or directly observed each performance. In thinking about these performances, we developed expectations about what our research might find:

- In conditions of interactions among ordinary citizens being photographed or otherwise having their image recorded by other apparently ordinary citizens, those being photographed generally will not object when they can see both the image and the image capture device *(Performance One)* in the context of a performance space. This condition, where peers can see both the recording and the presentation of the images, is neither "surveillance" nor "sousveillance." We term such observation that is side-to-side "*co*veillance," an example of which could include one citizen watching another.
- In conditions of interactions among ordinary people, those being coveilled generally will not object when they can see images being recorded from a concealed image capture device onto a wearable display device as part of a performance space *(Performance Two)*.
- Organizations engaged in surveillance generally will object to people engaging in obvious sousveillance in their establishments *(Performances Two* and *Three*).
- Surveillers will object more to the social act of challenging their authority through sousveillance than to the actual existence of sousveillance *(Performances Three* and *Four)*. Unlike coveillance, making the sousveillance image visible in the context of a mere performance piece will not necessarily make sousveillance more acceptable to the surveillers. The social act of challenging surveillance through sousveillance will itself often be challenged more than the mere gathering of images, whether gathered openly or covertly.
- The objections that surveillers have with sousveillance can often be overcome by promoting the sousveillance to a high-level coveillance. Such high-level coveillance consists of essentially one large corporation monitoring another large

corporation, such as the establishment where the performance takes place *(Performance Five*).

Performance One: Wearable Computer with Wearable Data Projection System

This performance takes place on a public street and involves a wearable computer, high power mercury vapor arc lamp and data projector, running from a backpack-based 120 volt battery (see Figure 1 and Figure 2). The projector is aimed at the ground, with an image projected right side-up to people facing the wearer. At this stage, the wearer of the device walks through the crowded downtown streets of a major metropolitan city on busy evenings. This performance is designed to gauge the reactions of ordinary citizens towards the device itself, unaccompanied by any explicit breach of any actual or implicit rules or regulations.

When the devices are inactive the wearer of the devices and the device itself are not foci of attention, although passers-by approach to the computer wearer and ask questions unrelated to the project. For example, some ask for directions to nearby places (as if, perhaps, the wearer might have access to online data). Once the set-up is complete, the display stimulus consists of the dynamic video of passers-by combined with the text caption "www.existech.com" projected on the ground.

The nature of the displayed material affects attitudes toward and perceptions of the device itself. For example, when the text displayed on the ground contains a ".com" URL, many people associate the device with a corporation. They approach the wearer of the devices, asking questions such as "what are you selling today?" The commercial nature of the web address contextualizes the device and its wearer as a marketing tool. This fits within an often expected and accepted use of public space. Experience gained from this type of performance suggests that the level of tolerance and acceptability towards the device and wearer relates to how it is contextualized within the existing knowledge and experience of people who encounter it. If the device appears to be sanctioned by a corporation or some other credible external authority, the level of acceptance is high, and the technology itself is seen as a form of authority. Potentially critical audiences, such as shoppers, or young adults lining up for fashionable dance clubs, were favorably disposed toward product displays on the device but negative towards artistic or satirical displays.

In short, when the performance is done in public spaces and appears to be organizationally related, acceptance by the public appears high. Surprisingly, people approved of the new form of advertisement in which live images were captured and rendered into computer-generated ads that included the subjects as models. People rarely object to their images being used in marketing.

Performance Two: Projected Data with Input from a Hidden Camera

This performance makes the source of the projected images originate less visible than in Performance One. The use of the same highly visible projection, but with a hidden camera, sets up a disconcerting discrepancy in expectations between the technology used to capture an image and the projection of that image. A concealed infrared night vision camera is used to capture live video of passers-by. In the simplest form, the live video output of the hidden camera is displayed directly to the data projector. The effect of the hidden video camera remains obvious by virtue of the intense beam of the data projector and the arrangement of the projection.

In other forms of this performance, text, graphics, and other content containing images from the hidden camera are integrated on-the-fly and rendered to the data projector for the audience. Provocative text messages such as "ADVERTISING IS THEFT of personal solitude" are mixed with video from the concealed night vision camera system (see Figure 1).

A common reaction is that people try to find the hidden camera. They appear captivated (and sometimes amused) by its apparent physical absence despite its obvious functionality. Various text, graphics, and other subject matter—mixed in with live data and displayed by the wearable data projector—evoke diverse responses. The most visceral of responses are when people see their own picture incorporated into the display. For example, when images of people are captured and then turned into a computer-generated advertisement, people pay much more attention to the advertisements in which they are the subjects than they do to other, similar, video material. People immediately recognize the appropriation of their image by a concealed, and therefore disconcerting, means.

The system gives rise to a roving interactive performance space where the roles of performer versus spectator, as well as architecture versus occupant, are challenged and inverted (see Figure 2). Passers-by become street performers and artists on the wearable stage that reflects their images to them. The stage itself, ordinarily thought of as a piece of architecture, has become a piece of clothing. Of course, the ability to choose to participate mitigates the invasiveness of the situation.

These relationships, however, become more complex when wearing the device into spaces such as shopping malls that are semi-public rather than fully public. The potential for confrontation between the wearer and security personnel increases by moving into the more highly surveilled spaces of malls and stores while wearing the hidden camera and the projector. The device also loses much of its playfulness as it moves across this invisible border. Therefore, the more highly surveilled a space is, the more objections are raised about such sousveillance, regardless of whether the content displayed is satirical or advertising in nature.

Performance Three: Making the Camera Obvious

Two cameras are used with the high intensity wearable projection computer devices, including the concealed infrared night vision camera of Performance Two, and an additional digital camera of the ordinary consumer variety that has been head-mounted. The purpose of using the additional camera is to make the act of taking a picture obvious. The additional camera chosen, a Kodak DC 260, looks like a traditional camera. It has a loud click sound (synthesized by its built in speaker, so that it sounds like a film camera) and a built-in electronic flash that calls attention to itself whenever it takes a picture.

When people turn to see what caused the flash, they see their pictures projected on the ground. To make the image capture more obvious, both pictures (freeze-frame stills and live video) are displayed side-by side. The flash serves as an annunciator, clearly indicating that a picture is being taken every 19 seconds (the update rate of the still camera). Text such as "CAMERAS REDUCE CRIME. . ." is used in the projection, together with the still and video displays.

During Performance Three, social controllers often object to the taking of pictures because of organizational policies against sousveillance. However, the situation changes when the camera wearer attributes the acts of photographic data collection to external circumstances or to the camera wearer's apparent lack of control over picture taking. Various externalizers are used in the performance:

1. The wearable computer system is completely hands-free. The wearer has no controls, no keypads, no mice, no buttons to push, and no other form of control over the device.
2. The device is automated or controlled externally so that it continues to take pictures while the wearer is explaining to the surveiller that it is beyond his control.
3. The wearer appears unable to remove the device. For example, the wearer can explain to the surveiller that the device is held on by screws for security purposes. In this case, a skull frame with dermaplants and comfort bands are screwed to the eyeglass frames so that the wearer cannot remove the device. Other variations on externalization themes include deliberately modifying the camera ahead of time so that it "malfunctions" and gets stuck in the "on" position.

In addition to these physical externalities, the wearers create social externalities that suggest that they are required to wear the device due to various external obligations such as that the wearer is bound by contractual obligation to take pictures or that the wearer's livelihood depends on doing this. When "malfunctions" occur, the same types of social controllers—shopkeepers, customer service personnel, security officials, etc.—accept the fact that the wearers are taking pictures in their establishments.

The greater the appearance that the sousveiller has personal control over the device, the less acceptable the act of sousveillance becomes. For example, the level of tolerance and acceptability for taking pictures varies according to the degree of a "will not/may

not/cannot" externality continuum. If the wearers explain that they are not in control of the devices and do not know when the devices take pictures, then the majority of surveillance personnel do not object to wearable devices. Surveillance personnel may initially object to the photography, but, if the wearers of recording devices can show that they are not in control of the technology they are wearing, surveillance personnel are often mollified.

In other situations, if the sousveillance wearer is, or appears to be, "just following orders" of an external authority, and thus mirroring the usual response patterns observed in surveillance personnel, the act of taking pictures is tolerated. Such externalization was made famous as the "Eichmann defense" by Hannah Arendt (1963). The performers use a wearable camera—whose use is made obvious by a flash and a loud click for each picture that is followed by a display of the picture. This produces a negative reaction when used without any attribution to external sousveillance authority. But this negative reaction disappears when the picture-taker concomitantly uses a headset with microphone and says loudly to a remote "boss": "They seem to be objecting to having their pictures taken." The sousveillance wearer's apparent compliance with a credible external authority reduces objections made by surveillance personnel in a manner similar to Milgram's (1974) discoveries of obedience to authority (see Figure 3).

Performance Four: Sousveillers Presenting Pictures of a Surveilling Site to the Surveillers

The same kind of surveillance domes used by establishments can be used in wearable computing performances (Mann and Niedzviecki 2001). (see Figure 4) These performances use wine-dark hemispheres similar to the seemingly opaque domes commonly found on the ceilings of stores. The fact that the domes may or may not contain cameras creates an important design element for the wearer because it is possible to arrange the situation such that the wearer does not know if the device contains a camera. If questioned about the wearable domes, the wearer is able to reply that they are unsure what the dome contains.

Video recordings used in Performance Four had been previously made by entering the shops with hidden cameras and asking various surveillance personnel what the domes on the ceilings of their shops were. In one case, customer service personnel explained that the domes on their ceiling were temperature sensors. In another situation, a record store owner asserted that the store's dark ceiling domes were light fixtures. By using flat panel displays to play back the recording to the customer service personnel, their surveillance is reflected back to them as sousveillance.

In practice, surveillance personnel's appeal to authority can be countered by the sousveillers appealing to conflicting authorities. To be most effective, the sousveilling camera/projector wearer needs to be operating under social control policies in the same way that the surveillance worker or official is operating under company policies about surveillance. In this way, the wearer and the employee acknowledge each other's state of

subordination to policies that require them to photograph each other. While the wearer and the employee engage in what would normally be a hostile act of photographing each other, they can be collegially human to one another and discuss the weather, sports, and working conditions.

Performance Five: Conspicuously Concealed Cameras

Whereas previous performances encountered resistance from certain surveillance establishments such as pawnbrokers, jewelry stores, and gambling casinos, the goal of Performance Five is to create ambiguous situations in which wearable data-gathering devices are conspicuously concealed (Mann and Guerra 2001). In this example, "blatantly covert" domes are used, together with a high quality brochure that corporatizes and commercializes the tools of sousveillance. Figure 4 shows a line of products, along with a corporate brochure that was created to present the artifacts in the context of purchased goods. Store employees objecting to the wearing of such device would also, by implication, be objecting to products of the consumerist society they are supposed to be upholding.

The wearable computers with domes evoke dialogue that varies as the size of the dome varies. For example, in one performance, a series of people entered an establishment wearing progressively larger domes until a complaint was raised. In some performances, performers play back video recordings of the same customer service personnel or of customer service personnel in other shops.

Conspicuously Concealed Cameras with Wearable Flat-Panel Displays

Some of the performance device also incorporates various large flat-panel display screens, worn on the body, that display live video from a concealed camera or from video recorded from a previous trip to the same shop (see Figure 5). The ambiguity surrounding when the video was recorded allows the wearer to explore the issues of recording and displaying video images in locations where cameras are prohibited.

When the performers wear a flat-panel screen or a data projector on their bodies, they show images of themselves to the people and managers who work there. These visible displays can evoke social control without any need for comments from the wearer of the camera and display. By remaining mute until addressed by store employees, the wearable sousveillance devices become the object of attention and not the sousveilling person wearing them. Indeed, the probability of interaction increases with an increase in the overtness of the sousveillance camera/data collection device (Mann and Niedzviecki 2001).

Invisibility Suit

An element of the inquiry was the questioning of visibility and transparency. In one performance, a flat panel display worn on the performer's back was arranged to show the view from a camera worn on the front. When asked what this device was, the performer simply said that it was an "invisibility suit" (see Figure 5). Obviously this notion is

nonsensical in the sense that the device certainly does not give invisibility In fact, it attracts all the more attention. Presenting the camera as a form of theatre helped to legitimize it as an externality, although with less success than the legitimization that provided by an external corporate requirement to wear the camera.

In some performances, when staff object to the video displays, the performers offer to cover the displays with sheets of paper so that the images would no longer be visible. This situation creates a distinction between the conflated issues of:

(a) privacy/no personal data being collected (which is violated by input devices such as cameras) versus
(b) solitude/no intrusion on personal space (which is violated by output devices such as video displays).

This separates the issue of privacy (the right to be free of the effects of measuring instruments such as cameras) from the issue of solitude (the right to be free of the effects of output devices such as video displays).

Performing Sousveillance

Although theorists and outside observers may perceive sousveillance to be empowering, what are the perceptions and experiences of those actually performing it. Jennifer Marchand reported to us after performing sousveillance:

> It felt refreshing, mostly the impressions being made on those under plain old surveillance. People got to say to themselves, 'Wait a minute, if I wanted to take a camera into the store, they would hassle me like that too?' thank God, I am glad that I experienced the image of freedom we are presented with (especially inside of places like malls).
> Everyone around us saw employees hide in huddles discussing the strategies of attack. We heard them tell us it was for our own good, we all made way for the rushing guards to greet us with concerns for our safety. They tell you it is for your own good and then refuse to tell you why. Then they laugh at you as if you were a silly peasant who needs to get back in line before you hurt yourself. It felt a little bit like monkey in the middle: I guess I'd be the monkey between the managers and the guards.
> There needed to be more people. It was hard. But exhilarating. People were absolutely shocked, appalled, amused, entertained, confused, intimidate, but we ourselves felt refreshed to be able to show people that there is a lot being hidden from us.
> Surveillance is a silly game of make-believe, like we can pretend we are not involved in the game (as the audience), but in fact we are the other team. Sousveillance is honest and factual, where the audience is aware of their part because we all become the audience. It's too factual to be a game.

Summarizing Sousveillance

This paper defines, describes, and explores sousveillance as both a conceptual framework for and as a performance of various techniques of self-empowerment in opposition to modern technologies of surveillance. The goal is to reveal and call into question the asymmetrical nature of surveillance through a series of performances. Each performance builds on the previous experience to articulate the necessity of sousveillance to restore balance to an otherwise one-sided surveillance society.

In Performance One, the wearable computer is a visible device that cannot be mistaken for a fashion accessory or casual consumer item. The goal is to learn how people respond to the wearable computer. The mechanisms of interaction are conversation with the wearer of the device, the collection of visual data of people moving in the local environment, and the presentation of processed visual images through a projection device using the sidewalk as a screen. When sousveillance device wearers have more official contexts, such that the performances might more properly be regarded as surveillance rather than coveillance, citizens become more tolerant of the performances. They defer to authority.[5]

Performance Two differs from Performance One by hiding the camera so that people do not know where the images are coming from. Yet, the highly visible projection of the manipulated video feed ensures that everyone knows they are being watched. For many, the idea of surveillance is lost in the playful novelty of the interactions with the wearer of the projection device.

Performance Three involves taking multiple cameras into the semi-public locations of shopping malls. Not only are the wearable computers visible, but the use of props ensures that everyone in the vicinity knows that pictures are being taken. In this case, the devices evoke responses from store employees, and various techniques of resistance are applied to continue collecting and projecting visual data. The degree of objection to sousveillance varies with the amount of surveillance present. The greater objections to sousveillance take place in establishments such as casinos, jewelry stores, and department stores in which more surveillance cameras are present. Fewer objections take place in department stores where fewer surveillance cameras are present.

In Performance Four, images taken earlier by hidden cameras are shown to customer service personnel in the same settings in which the images were taken. By this means, the experience of surveillance is reflected back to the surveillers. When a plausible reason for sousveillance is evident, surveillers often choose to ignore sousveillance. Moreover, when sousveillers are challenged by surveillance authorities, the authorities often accept the sousveillance as is, apparently sanctioned by other external authorities. This degree of acceptance varies in proportion to the degree of externalization, giving rise to a "will not/may not/cannot" hierarchy. Thus when the sousveiller refuses (will not) to stop taking

[5] As Friedenberg (1981) and Moore (1995) note, this may differentiate Canadians from Americans. It would be interesting to replicate these performances in other cultural contexts.

pictures, the situation escalates, whereas when the wearer is contractually required to take pictures (may not) the situation remains neutral, and when the wearer is unable to stop taking pictures (cannot) the situation usually becomes acceptable to authority figures.

This may be successfully done through self-demotion (Mann 2001b) of the wearer (e.g. having the wearer be or seem to be required to wear the device as part of a company uniform while running errands on company time). The success of such self-demotion in having surveillers tolerate being photographed depends inversely on the degree of free-will exercised by the wearer, along a continuum from "will not" (wearer refuses to stop taking pictures) to "may not" (wearer required to take pictures) to "cannot" (wearer unable to take off uniform or eyeglasses are affixed with a security bracket or dermaplants that the wearer cannot remove or that require medical/surgical intervention to remove).

Sousveillance challenges the systems and technologies of surveillance that are both human and technological. Often, customer service workers are positioned as "just following orders" from management, or as acting in the best interests of management. Managers of department stores sometimes "demote" themselves by pretending to be sales staff. In this role of "clerk," they assert: "You must have permission from the manager to take pictures here," hoping not to be revealed as the very person in that position of responsibility. This deferral to authority can continue up a hierarchy where management claims the surveillance cameras were installed by a directive from head office. In turn, head offices have claimed that the insurance companies require the cameras. This deferral to authority can continue up a hierarchy where management claims the surveillance cameras were installed by a directive from head office. It becomes impossible to isolate and identify a specific responsible entity; responsibility defuses into generalized deferrals to the way things are.

With Performance Five, focus switches to a playful repositioning of surveillance technologies on the body as fashion features. The dark plastic surveillance domes that hide cameras are now worn as fashion accessories, perhaps concealing their own recording devices. Or projection devices are worn like jewelry, blurring the distinction between surveillance device and consumer product.

Conclusions: Sousveillance in Society

The performances show how certain kinds of rule violation can be deliberately used to engender a new kind of balance. They show public acceptance of being videoed as an act of surveillance in public places. When such data collection is done by ordinary people, such as the performers, to other ordinary people, it is often accepted. However, when data projectors show surveillance officials the data that has been collected about them, there is less acceptance. Organizational personnel responsible for surveillance generally do not accept sousveillance from the "ordinary people" performers, even when data displays reveal what the sousveillers are recording. The only instances of acceptance are in

Performance Four, when surveiller and sousveiller can find common ground in both doing "coveillance" work for symmetrically distant organizations.

Surveillance cameras threaten autonomy. Shrouding cameras behind a bureaucracy results in somewhat grudging acceptance of their existence in order to participate in public activities (shopping, accessing government services, traveling, etc.). By having this permanent record of the situation beyond the transaction, social control is enhanced. Acts of sousveillance redirect an establishment's mechanisms and technologies of surveillance back on the establishment. There is an explicit "in your face" attitude in the inversion of surveillance techniques that draws from the women's rights movement, aspects of the civil rights movement, and radical environmentalism. Thus sousveillance is situated in the larger context of democratic social responsibility.

The performances described here engage, challenge and invert the power structure of networked surveillance. The role reversal between the surveilled individual and the act of surveillance allows for the exploration of the social interactions that are generated by these performances. It raises questions for further inquiry; primarily issues of collective- and self-empowerment within the panopticon of social surveillance and the governance of public and semi-public places (Foucault 1977; Ostrom 1990). As well, the performances show how the public can bring the technologies of surveillance to bear on surveillance workers whose profession it is to maintain such hierarchies of control.

Sousveillance disrupts the power relationship of surveillance when it restores a traditional balance that the institutionalization of Bentham's Panopticon itself disrupted. It is a conceptual model of reflective awareness that seeks to problematize social interactions and factors of contemporary life. It is a model, with its root in previous emancipatory movements, with the goal of social engagement and dialogue.

The social aspect of self-empowerment suggests that sousveillance is an act of liberation, of staking our public territory, and a leveling of the surveillance playing field. Yet, the ubiquitous total surveillance that sousveillance now affords is an ultimate act of acquiescence on the part of the individual. Universal surveillance/sousveillance may, in the end, only serve the ends of the existing dominant power structure. Universal sur/sousveillance may support the power structures by fostering broad accessibility of monitoring and ubiquitous data collection. Or as William Gibson comments in the feature length motion picture film CYBERMAN (http://wearcam.org/cyberman.htm) “You're surveilling the surveillance. And if everyone were surveilling the surveillance, the surveillance would be neutralized. It would be unnecessary.”

In such a coveillance society, the actions of all may, in theory, be observable and accountable to all. The issue, however, is not about how much surveillance and sousveillance is present in a situation, but how it generates an awareness of the disempowering nature of surveillance, its overwhelming presence in western societies, and the complacency of all participants towards this presence.

Despite police espousal of "neighborhood watch" programs, few of us live in a world where watching one's neighbors is a practical mode of social control. Such close local observation is mostly found in pre-industrial societies, their remnants in rural and urban villages, and in specialized situations (Ostrom 1990). Urban houses are often vacant while families are scattered about at various activities. Most friends and relatives live in other parts of the city, continent or globe. Many coworkers are not collocated in the same spaces, and most shopkeepers do not know their customers personally.

In contemporary networked societies, individuals switch among multiple, partial communities and work teams rather than being embedded in single communities or workgroups (Wellman 1999). Yet, surveillance is a manifestation of the industrial and post-industrial eras of large hierarchical organizations efficiently employing technologies in neo-panopticons of social control. But in networked societies, people are more likely to want sousveillance and coveillance, for they lack the protection of the village/community or hierarchical organization. Newly developed technology allows them to surveil the surveillers. In affording all people to be simultaneously master and subject of the gaze, wearable computing devices offer a new voice in the usually one-sided dialogue of surveillance. They suggest a way towards a self-empowering sousveillance for people as they traverse their multiple and complex networks.

References

Arendt, H. (1963). *Eichmann in Jerusalem: A Report on the Banality of Evil*. New York: Viking.

Bair, D. (1978). *Samuel Beckett: A Biography*. New York. Simon and Schuster.

Bentham, J. (1968). *The Collected Works*. London: Athlone Press.

Cannon, L. (1999). *Official Negligence: How Rodney King and the Riots Changed Los Angeles and the LAPD*. Boulder, CO: Westview.

Castells, M. (2000) *The Rise of the Network Society*, Revised Ed. Oxford: Blackwell.

Dryer, D.C., C. Eisbach, and W.S. Ark (1999) At what cost pervasive? A social computing view of mobile systems. *IBM Systems Journal*, 38(4): 652-676.

Dürrenmatt, F. (1988). *The Assignment, Or, On the Observing of the Observer of the Observers*, trans. J. Agee. London: Jonathan Cape.

Elliott, A. (2003) In stores, private handcuffs for sticky fingers. *New York Times*, June 17: A1.

Evangelista, B (2002). Surveillance society: don't look now, but you may find you're being watched. *San Francisco Chronicle*, September 9.

At: http://www.sfgate.com

Fogg, B.J. (1997) Captology: 'the study of computers as persuasive technologies'. In *Extended Abstracts of CHI '97*. Atlanta GA: ACM Press, 129.

Foucault, M. (1977). *Discipline and Punish*, trans. A. Sheridan. New York: Vintage.

Foucault, M. (1980a) Prison talk. In *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, ed. C. Gordon. New York: Pantheon, 37-54.

Foucault, M. (1980b) Questions of geography. In *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, ed. C. Gordon. New York: Pantheon, 61-77.

Friedenberg, E. (1980) *Deference to Authority: The Case of Canada*. New York: M.E. Sharpe.

Garfinkel, H. (1967) *Studies in Ethnomethodology*. Cambridge: Polity.

Graves, R. (1955) Nemesis. In *The Greek Myths:1*. Harmondsworth: Penguin.

Ingham, R. (1978) *Privacy and Psychology*. New York: John Wiley & Sons.

Huxley, A. (1958) *Brave New World Revisited*. New York: Harper.

Jacobs, J. (1961) *The Death and Life of Great American Cities*. New York: Random House.

Keel, R. (2001) Ethnomethodological perspective (on crime and deviance). In C. Bryant (ed.) *Encyclopedia of Criminology and Deviance*. New York: Taylor and Francis, 148-153.

Lefebvre, H. (1991) *The Production of Space*, trans. D. Nicholson-Smith. Oxford: Blackwell.

Mann, S. (1997) Wearable computing: A first step toward personal imaging. *IEEE Computer*, 30(2): 25-32.

Mann, S. (1998) 'Reflectionism' and 'diffusionism': new tactics for deconstructing the video surveillance superhighway. *Leonardo*, 31(2): 93-102.

Mann, S. (2001a) *Intelligent Image Processing*. New York: John Wiley and Sons.

Mann, S. (2001b) Can humans being clerks make clerks be human? - exploring the fundamental difference between UbiComp and WearComp. *Informationstechnik and Technische Informatik* 42(2): 97-106.

Mann, S. and H. Niedzviecki (2001) *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*. Toronto: Random House Doubleday.

Mann, S. and R. Guerra (2001) The Witnessential Net. In *Proceedings of the IEEE International Symposium on Wearable Computing, Switzerland: October 8-9*, 47-54.

Marx, G. (1995) The engineering of social control: the search for the silver bullet. In J. Hagan and R. Peterson (eds.) *Crimes and Inequality,* Stanford: Stanford University Press, 225-235.

Mary, G. (1998) An ethics for the new surveillance. *The Information Society* 14 (3): 171-85.

Marx, G. (2003 in press) A Tack in the shoe: neutralizing and resisting the new surveillance. *Journal of Social Issues* 59(1).

McGoohan, P. and D. Tomblin (1967) *The Prisoner*. [television series.] London: Everyman Films and ITC.

Milgram, S. (1974) *Obedience to Authority.* London: Tavistock.

Moore, M. (1995) *Canadian Bacon*. Writer and director. John Candy, star.

Newman, O. (1972) *Defensible Space*. New York: Macmillan.

Ostrom, E. (1990) *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge: Cambridge University Press.

Rhodes, B.J., M. Nelson and J. Weaver (1999) Wearable computing meets ubiquitous computing: reaping the best of both worlds. In *Proceedings of The Third International Symposium on Wearable Computers*. San Francisco, 141-149.

Rogers, T.W. (1994) Detournement for fun and (political) profit. *Ctheory* At: http://ctheory.net/text_file.asp?pick=242

Stanley, J. and B. Steinhardt (2003) Bigger monster, weaker chains: the growth of an American surveillance society. Washington: Technology and Liberty Program, American Civil Liberties Union.

Virilio, P. (2002) *The Visual Crash*. Cambridge, MA.: MIT Press.

Webster, C.W. and J. Hood (2000) Surveillance in the community: community development through the use of Closed Circuit Television. Presented at *Community Informatics*. Middlesbrough, UK: University of Teesside.

Wellman, B. (1999) The network community. In B. Wellman (ed.) *Networks in the Global Village*. Boulder, CO: Westview, 1-48.

Wellman, B. (2001) Physical place and cyberspace: the rise of personalized networks. *International Journal of Urban and Regional Research*, 25(2): 227-252.

Figures

Figure 1.
(a) The wearable device contains a 1 GHz P3 CPU, rendering engine, high-power mercury vapour arc lamp data projector, within a black flame-retardant Nomex uniform custom tailored to fit the wearer. Here a person can see his own image together with other computer generated material.
(b) Close-up view showing the output of the high intensity data projection system.

Back to text.

Figure 2.
(a) On the street, people would bring their children over to play in the wearable interactive video environment and performance space.
(b) Large crowds gathered to s ee the interactive environment.
(c) Even adults enjoyed playing in the interactive space.

Back to text.

Figure 3.
(a) Projected text: "Cameras reduce crime; for your protection your image shall be recorded and transmitted to the EXISTech.com image and face recognition facility." Back to text.

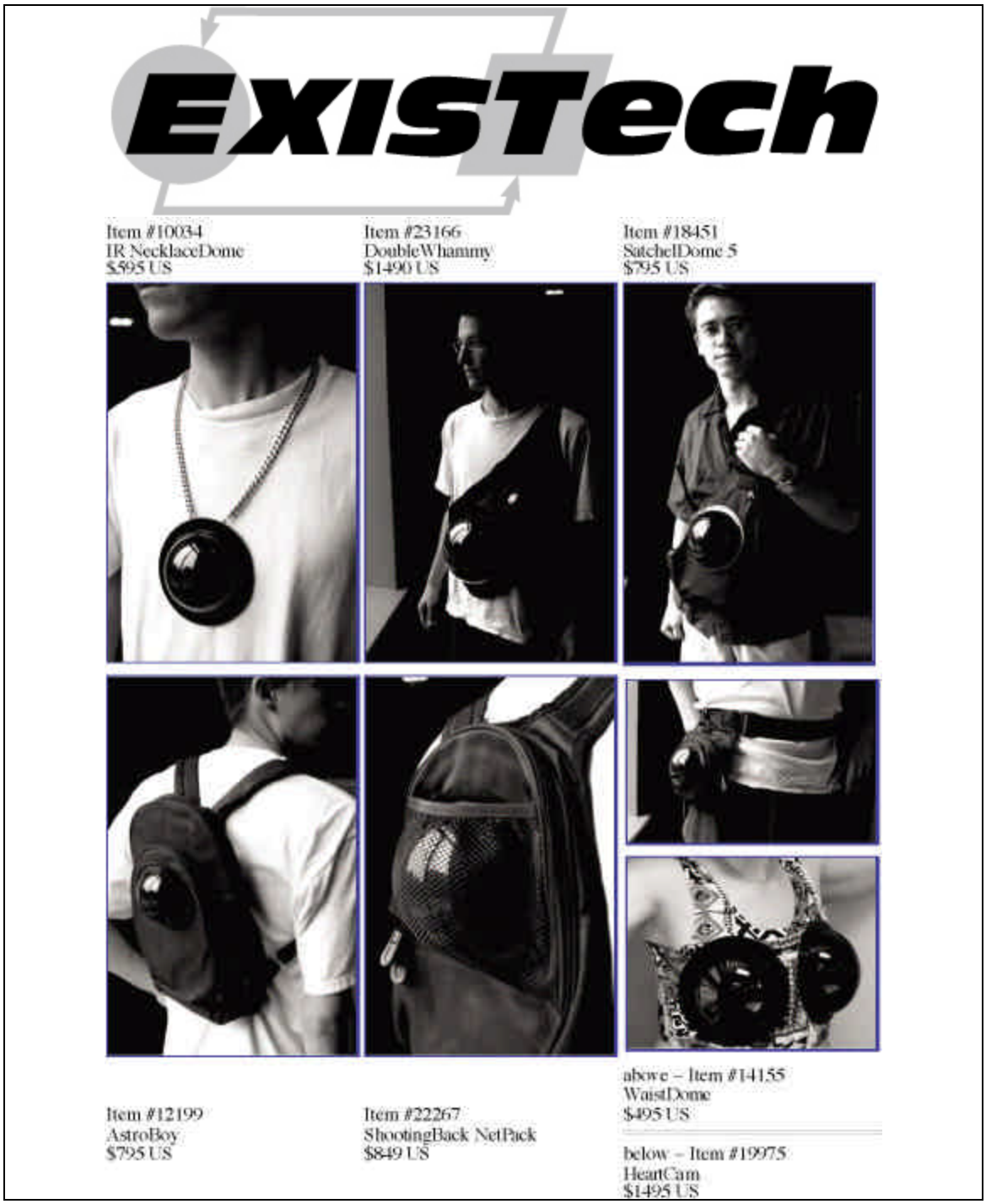

Figure 4.
EXISTech's corporate brochure was created to present the artifacts of sousveillance in the context of high fashion, as high cost purchased goods. This contextualizes sousveillance products and services as legitimate elements of conspicuous consumption in our consumerist society.

Back to text.

Figure 5
(a) Illusory transparency of television. A television mounted to an easel and placed it at the base of one of the most commonly photographed subjects, Niagara Falls, illustrates the principle of illusory transparency with a video camera connected to the television and positioned it such as to show the subject matter behind the television in exact image registration with what one would see if the television were not present (*a la* Magritte).
(b) Invisibility suit: Street Theatre of the Absurd. A large 1024x768 flat panel display incorporated into a wearable computer system. The screen is sideways (portrait orientation) to maximize screen size on the body. The back-worn display shows output from a front-worn camera, so that people can "see right through" the wearer. Thus the wearer's back is a window, showing what is in front of the wearer. Therefore when asked by agents of surveillance what this special clothing is, the wearer responds with a silly answer, namely that the device is an "invisibility suit to provide privacy and protection from their surveillance cameras." Such a silly answer externalizes the locus of control of the wearable camera. First, a silly idea such as an invisibility suit makes it hard for the agent of surveillance to reason with the wearer. Second, the wearer argues that the motivation for wearing the camera is to provide protection from being seen by surveillance cameras. Thus, the surveillance agent's objection to the sousveillance camera becomes an objection to his own surveillance camera.
(c) Sousveillance under surveillance: The invisibility suit worn under a department store's ceiling domes.
Back to text.