Sousveillance: Inventing and Using Wearable Computing Devices to Challenge Surveillance*

Steve Mann, Electrical and Computing Engineering, University of Toronto†
Jason Nolan, Knowledge Media Design Institute, University of Toronto
Barry Wellman, Sociology, University of Toronto

June 28, 2002

Abstract

This paper explores using wearable computing devices to perform "sousveillance" (inverse surveillance) as a counter to organizational surveillance. A series of performances are used to question social norms of surveillance. A variety of wearable computing inventions generated different kinds of responses. Visible sousveillance often evoked counter-performances by front-line surveillance workers. The juxtaposition of sousveillance with surveillance generates participatory awareness of the ubiquitous presence and acceptance of surveillance in society.

1 Neighborhood "Eyes on the Street" or Organizational Surveillance?

> 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 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).

> ...felt meaningless unless they were being observed and this was the reason they all observed and took snapshots and movies of each

*We appreciate the advice and assistance of James Fung, Sharon and Corey Manders, Felix Tang, Betty Lo, Chris Aimone, Thomas Hirmer Angela Garabet, Adwait Kulkarni, Samir Parikh, Kathleen Pirrie Adams, Katherine Parrish, and Monica Prijatelj. The performances described here were supported in part by the Canada Council for the Arts.

†mann@eecg.toronto.edu: Tel.: (416) 946-3387; Fax: (416) 971-2326; www.wearcam.org

> other, for fear of experiencing the meaninglessness of their existence... staggering along in mad hope to of somehow finding someone to be observed by somewhere.... (Dürrenmatt 1988, 23).

In recent decades, public surveillance of private space has become ubiquitous. Jane Jacobs (1961), Oscar Newman (1972), and Elinor Ostrom (1990) gave this a benign spin. They claimed that people's "eyes on the street" (to use Jacobs' phrase) would prevent petty crimes and provide interpersonal social support. Jacobs' analysis has been compelling: it evokes the image of an irate housewife seeing trouble from her kitchen window, and rushing out with a frying pan to hit the troublemakers over their heads.

Although Jacobsean street-defenders may certainly exist, they have become ineffective in situations where people rarely know their neighbors. People are now often connected more through social networks and computer networks (email, etc.) rather than through local villages. Such far-flung, sparsely-knit networks are in some ways not as conducive to small groups observing and closely controlling their members' behavior.

Modern social surveillance finds its roots in the organized and asymmetric power structures of Jeremy Bentham's Panopticon (Bentham 1838 (1967)). A panopticon is a centralized arrangement for social controllers to visually observe people's behavior. Large organizations extensively surveill their employees and a public that often does not so closely surveill the organizations. Examples of private surveillance include: observing the keystrokes and web-surfing of their employees, Las Vegas casinos using field-glasses and high-powered video to record movements of their employees, and stores and factories that observe employees to stop thefts. In other situations, stores and office buildings use video to surveill patrons and visitors, and British police to observe citizens in the streets using closed circuit video systems ("CCTV") (Seabrooke and Wattis 2000; Webster and Hood 2000). They are modern panopticons, using video technologies for social control based on ubiquitous observation (Goffman 1966; Foucault 1977; Lofland 1998).

All such activity has been ***sur***veillance: organizations observing (usually acquiescent) individuals. One way to challenge and problematize both the surveillance and acquiescence that attend these technologies of control is to take the same panoptic elements and re-situate them on the individual to observe those in authority. We call this inverse panopticon "***sous***veillance"[1] from the French words for "sous" (below) and "veiller" (to watch). 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 to serious discussion of curtailing police brutality (Cannon 1999). It further intensified a movement to place video surveillance cameras in police cars. This not only documents police brutality, it protects the police

[1] Coined terms such as *sousveillance* and *coveillance* are necessary in order to situate surveillance within a broader context.

from false charges of brutality, and gives supervisors more panoptic control over the behavior of officers (see also www.copwatch.org, www.justicefiles2.org).

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 cab passengers photographing cab drivers, citizens photographing police officers, civilians photographing government officials, and residents beaming satellite shots of occupying troops onto the Internet. In many cases, these acts of sousveillance violate prohibitions, rules, or laws 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, signs prohibiting such photography are seldom present. Managers, when asked, are seldom able to show evidence of any written policy on this issue.

How will such rule-breaking performances play out, when individuals sousveill large organizations? Key issues are the extent to which organizational surveillance can be challenged, and the ways in which organizations respond to such challenges. In this paper, we examine how wearable computing can promote personal empowerment in human-technology-human interactions (Mann 1997, Fogg 1997). We describe and analyze here a set of performances that follow Harold Garfinkel's ethnomethodological approach (1967) to breaching norms. We gain insight into unspoken norms by (a) deliberately not acquiescing to surveillance and (b) performing visible and explicit sousveillance. These behaviors break known policies. They expose hitherto discreet, implicit, and unquestioned organizational acts of surveillance (Keel 2001; Mann 2000; Mann and Niedzviecki 2001).

Our goal is to show how certain wearable computing inventions can foster sousveillance in organizational environments. As part of this enterprise, we document situations where people accept surveillance and where organizational service and security personnel usually reject, or sometimes accept, sousveillance. By violating norms about who can observe whom, these sousveillance performances make social controls explicit, challenge the unstated assumptions of surveillance and ownership of space and images, and make visible the implicit assumptions of organizational contexts. In some instances, the situations reveal how people in public spaces perceive the wearer of the wearable computer. We try to analyze the performances and try to understand how the wearing of sousveillance devices may reinforce or challenge attitudes toward surveillance and sousveillance.

2 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 (1978) 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 in the asymmetric photography/video policies of the examined establishments themselves.

The notion of ubiquitous surveillance is longstanding. Jeremy Bentham's (1838) Panopticon defined an observation system in which people could be placed under the possibility of surveillance without knowing whether or not they were actually being surveilled. Bentham proposed such an architecture for use in prisons, schools, hospitals, and workplaces.

> [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 tool in support of the governance of Industrial Revolution societies was an updating of governance techniques in pre-industrial societies. The densely-knit connections and tight boundaries of pre-industrial "door-to-door" societies fostered direct visual observation as a means of social control (Ostrom 1990; Wellman 1999, 2001). As Industrial Revolution societies developed in the early nineteenth century societies, urbanites knew only a few of their fellow residents. Societal scale had increased beyond the ability for little groups of neighbors to eye each other. There was a perceived need for industrialized social control. Hence, panopticons employed hierarchies of organizational employees to observe public spaces in prisons, factories, etc. (see also Foucault 1977). Indeed, "Panopticism was a technological invention in the order of power, comparable with the steam engine" (Foucault 1980a; Foucault 1980b: 71).

In post-Industrial society, neo-panopticons take advantage of new communication techniques. When people move in public or semi-public (e.g. commercial) locations they are liable to become unwilling and sometimes unknowing subjects of surveillance. Just the knowledge that there may be surveillance is sufficient to induce obedience to authority (Foucault 1977).

Surveillance techniques have become technologically embedded. Where people once had 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". Video cameras can be almost invisibly small, communication

networks can direct 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 them. They are subjects being monitored in two senses of the word:

- Subjects of observation on video monitors that display and preview the acquiring of their image. In that sense they are subjects of the camera (as in the "subject matter" of a photograph).
- Subjects under the potential control of the people in positions of authority who are organizational monitors of their behavior. In that sense they are like the subjects of a king, a dictator, or an authority figure or organization.

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 historic ability of 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.

3 Wearable Computing for Sousveillance

Along with the development of the personal computer there has been a growing sense that digital technology has leveled the playing field, resulting in individuals feeling more self-empowered both at home and at work (Wellman 2001). Mobile, portable, and wearable computing devices have allowed individuals to take this personal computing revolution beyond the office, school, or laboratory. 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.[2] As a response to institutional and organizational surveillance of individuals, these new sousveillance inventions allow people to invert the gaze and watch the watchers. These inventions attempt to call into question Aldous Huxley's assertion that "technological progress has hurt the Little Man and helped the Big Man" (Huxley 1958:43).

Sousveillance as personal empowerment has focused on enhancement of the ability of people to access and collect data about their surveillance (Mann and Niedzviecki 2001) rather than other suggested design solutions that seek to assuage privacy concerns by regulating surveillance. Such projects seek to develop rules and protocols to negotiate privacy (Rhodes et al. 1999). However, access to more information does not imply greater self-power. If the information is largely controlled and exchanged by external agents over which the individual has no power, then enhancements are more pacifiers than solutions.

More active forms of sousveillance confront surveillance by using wearable computing to surveill 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). 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 provides a transformation from surveillance techniques into sousveillance techniques in order to watch the watchers.

We report in this paper on a series of performances that attempt to hold a sousveillance mirror up to society in the tradition of Theater of the Absurd (Bair 1978). Uncertainty surrounds these performances, as no one is ever sure of the outcome of the interaction between device, wearer and participants. Design factors can influence interaction: the wearing of technology can be seen as either acceptably empowering or unacceptably threatening, depending on the type of technology, location, and how it is presented/represented (Dryer, et al. 1999). For example, people who use more 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).

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. 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

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

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, and (b) break unstated rules of asymmetric surveillance using new wearable computing inventions (Mann and Niedzviecki 2001).

The collecting of digital images, the taking of 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.) using devices that mirror those used by these social controllers.

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 question socially controlling surveillance. 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 North American city. Hundreds of people actively participated in or directly observed each performance.

We hypothesize:

- In conditions of interactions among ordinary citizens being photographed or otherwise having their image recorded by other apparently ordinary citizens, those being photographed often 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 hierarchical peers can see the both the recording and the presentation of the images, is neither "surveillance" nor "sousveillance". We term such observation that is side-to-side in an organizational hierarchy "***co***veillance, an example of which includes one citizen watching another citizen.

- 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 (such as EXISTech Corp.) monitoring another large corporation (such as the establishment where the performance takes place).

4 Performance One: Wearable Computer with Wearable Data Projection System

One of the performances that takes place on a public street involves a wearable computer with a wearable high power mercury vapor arc lamp and data projector, all running from a backpack-based 120 volt battery (see Figures 1 and 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 in 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.

While setting up and getting ready with the devices inactive, the wearer of the apparatus and the device are not foci of attention. When the display is not on, and investigators are not doing anything in particular, passers-by come up 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.[3]

The nature of the displayed material greatly 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 also its wearer as a marketing tool. This fits within an often expected and accepted use of public space. Experience gained from this type

[3] "EXISTech" (existech.com) is short for "Existential Technologies Corporation", a company name inspired by Kafka's *The Trial*. It is an organization federally incorporated in Canada, and also registered in the United States trademark office by Mann to aid in the authenticity of the performances. All forms, business cards, letterhead, etc, show Hong Kong as EXISTech's head office. This location was selected for remoteness to make it less convenient for people to communicate with EXISTech by telephone, so that people would be more likely to communicate in writing.

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. Audience comments reveal that the technology itself is seen as a form of authority. The most potentially critical audiences, such as avid members of a consumerist society, or people lining up for fashionable dance clubs, were favorably-to-neutrally disposed toward product displays on the device but expressed disdain for artistic or satirical displays.

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 kind of advertisement* in which live images were captured, and rendered into computer-generated ads which include the subjects as models. Although one might have expected people to object to their images being used in a marketing system, there were few objections.

5 Performance Two: Projected Data with Input from a Hidden Camera

This performance makes the source from where the projected images originate less visible than in Performance One. Using 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 solitude" are mixed with video from the concealed night vision camera system (See Fig 1.).

This system gives rise to a roving interactive performance space where the roles of artist versus spectator, as well as architecture versus occupant, were challenged and inverted, as shown in Fig. 2.

A common reaction to Performance Two is that people try to find the hidden camera. They appear captivated (and sometimes amused, or obsessed) 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. Among the most visceral of responses are when people see their own picture incorporated into the display. For example, when images are captured of people and then turned into a computer-generated advertisement, people pay much more attention to the

(a) (b)

Figure 1: (a) The wearable apparatus contains a 1 GHz P3 CPU, rendering engine, high-power mercury vapour arc lamp data projector, within a black flame-retardant Nomex (TM) 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.

(a) (b) (c)

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 see the interactive environment. (c) Even adults enjoyed playing in the interactive space.

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.

Challenging the notion of surveillance, along with role reversal (surveillance versus sousveillance), gives rise to a reversal of performer versus audience. Passers-by became 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 play with or walk away from the situation and not participate mitigates the invasiveness of the sur/sous/coveillance.

These relationships become more complex when wearing the apparatus 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 barrier.

The more highly surveilled a space is the more objections are raised about this sousveillance performance, regardless of whether the displayed subject matter is satirical (anti-corporate) or advertising (pro-corporate). In one sense, when the displayed subject matter is clearly corporate, sousveillance masquerades as coveillance (e.g. one corporation such as EXISTech Corp. invading the space of another corporation such as a shopping mall). But in this context of escalated coveillance (e.g. one company watching another) coveillance is not more tolerated by the surveillers than sousveillance would be.

6 Performance Three: Making the Camera Obvious

Two cameras are used with the high intensity wearable projection computer system, including the concealed infrared night vision camera of Performance Two, and an additional head-mounted digital camera of the ordinary hand-held consumer variety. 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 to most people like a very traditional camera so that its function is obvious. 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. The device represents the average individual's conception of what a camera should look like.

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 as well as live video) are displayed side-by side. The flash serves as an annunciator, to indicate clearly that a picture is being taken every 19 seconds (the update rate of the color 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" 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 apparatus.

2. The apparatus 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 apparatus. 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:

1. The wearer is bound by contractual obligation to take pictures. The wearer's livelihood depends on doing this.

2. The wearer simply is unable to remove or stop the device from taking pictures (e.g. because it is permanently attached to the body, cannot be turned off, etc.).

When "malfunctions" occur, the same types of social controllers–shopkeepers, customer service personnel, security officials, etc.–accept the fact that the wearer is 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 wearer explains that he is not in control of the device and does not know when the device takes pictures, then the majority of surveillance personnel do not object to wearable devices. Surveillance personnel may initially object to the photography; however 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 some external authority, and thus mirroring the usual response patterns observed in surveillance personnel, the act of taking pictures is

(a) (b) (c)

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". (b) Confrontation with officials at an upscale jewelry store. (c) A favorable reaction was obtained from department store security staff who thought the device was a good invention.

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 Fig. 3).

7 Performance 4: 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 (See Figure 4) (Mann and Niedzviecki 2001). 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 apparatus 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.

8 Performance Five: Conspicuously Concealed Cameras

Whereas previous performances encountered resistance from certain surveillance establishments such as pawnbrokers, jewelry stores, mafia run gambling casinos, etc., the goal of Performance Five is to create an ambiguous situation in which data-gathering wearable computer systems 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, as shown in Fig 4. This figure shows a line of products, along with a corporate brochure that was created to present the artifacts in the context of purchased goods. Store employee objecting to the wearing of such apparatus would also by implication be objecting to EXISTech Corporation's 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 other customer service personnel in other shops.

9 Conspicuously Concealed Cameras with Wearable Flat-Panel Displays

Some of the performance apparatus 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 Fig 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

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.

cameras are prohibited.

When the performers wear a flat-panel screen or a data projector on their bodies, they show images of themselves (and their stores) to the social controllers–from clerks to 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 controllers, it is the wearable sousveillance devices that 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 mechanism (Mann and Niedzviecki 2001).

9.0.1 Invisibility suit

An element of the sociological inquiry was a questioning of visibility and transparency. In one performance, a backworn wearable flat panel display was arranged to show a view from a frontworn camera. When asked what this apparatus was, the performer simply said that it was an "invisibility suit" (See Fig 5.) Obviously this notion is nonsense, in the sense that the device certainly doesn't give invisibility (in fact it attracts all the more attention). However, it was found that by presenting the camera as art (e.g. as in Magritte's 1936 painting of a painting showing reality), it was somehow justified. Presenting the camera as a form of theatre, helped to legitimize it, as an externality, although with less success than the legitimization that was provided by an external corporate requirement to wear the camera.

In some performances, the wearer offered to cover the data display with paper so that it will no longer bother the customer service personnel. 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).

10 Sousveillance and Reflectionism

10.1 Performing 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 location of interaction is busy downtown streets. The goal is to learn how people respond to the wearable computer. The mechanisms of interaction are conversation with

(a)

(b)

(c)

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 backworn display shows output from a frontworn camera, so that people can "see right through" the wearer. Thus the 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 very silly answer, namely that the apparatus 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. Firstly such a crazy idea as an invisibility suit makes it hard for the agent of surveillance to reason with the wearer. Secondly, 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.

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 the sousveillance wearer has a more official context, such that the performance might more properly be regarded as surveillance rather than coveillance, citizens surprisingly become more tolerant of the performance, when one might expect the opposite should be true.

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 a prop ensures that everyone in the vicinity knows that pictures are being taken. In this instance, the devices evoke responses from store employees, and various mechanisms of skillful 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 like casinos, jewelry stores, and department stores in which more surveillance cameras are present. Lesser 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 setting in which the images were taken. By this means, the experience of surveillance is reflected back to the surveiller. 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 take a position of graciously accepting the sousveillance when the sousveillance is apparently sanctioned by another external authority. This degree of acceptance also 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 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 becomes acceptable to authority figures most of the time.

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).

With Performance Five, focus switches to a playful repositioning of surveil-

lance 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 tool and consumer product.

10.2 Sousveillance in Society

The performances show how certain kinds of rule violation can be deliberately used to engender a new kind of balance. All hypotheses are supported. 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. As hypothesized, 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.

Acts of sousveillance redirect an establishment's mechanisms and technologies of surveillance back on the establishment. Gaze is inverted. This challenge to authority is both technological and social. 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. 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.

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. It becomes impossible to isolate and identify a specific responsible entity, as responsibility defuses into generalized deferrals to the way things are.

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.

10.3 Reflectionism as Inquiry and Practice

"Reflectionism" is a term invented by Mann (1998a) for a series of concepts that center around the idea of challenging bureaucracy by holding a mirror up to society, creating a symmetrical corporate infrastructure for a self-bureaucratized individual. Reflectionism usually involves constructing a wearable form of bureaucracy and sousveillance that attempts to mirror exactly that of the establishment where the apparatus is worn (e.g. wearable domes that match the decor of the establishment, wearable signage, self-demotion to subservience of a remote but uncompromising manager). Reflectionism challenges the often illusory taken-for-granted notions of ubiquity, location, physical place and cyberspace, by taking them up in the context of transgression, privacy, and technology (Lefebvre 1991; Newman 2000). As contemporary western society has tried to make technology mundane and invisible through its disappearance into the fabric of buildings, consumed objects and lives, the creation of pervasive ubiquitous technologies, smart floors, toilets, elevators, and light switches, means that intelligence gathering devices, "ubiquitous surveillance", are becoming equally

invisible (Mann and Niedzviecki 2001). This re-placement of technologies, and the concomitant data conduits, has brought new opportunities for observation, data collection, and surveillance.

Reflectionism is related to the Situationist movement in art, in particular the aspect of as "detournement": the tactic of appropriating tools of social controllers and resituating these tools in a disorienting manner (Rogers 1993; Ward 1985). Reflectionism extends the concept of detournement by using the tools against the oppressor, holding a mirror up to the establishment, and creating a symmetrical self-bureaucratization of the wearer (Mann 1998a). Surveillance is inverted through such mimesis into a form of performance that partakes of the nemesis, a divine justice, or "payment... duly made" in having the tables turned, and the power structure inverted (Graves 1955: 126-7). The mimetic symmetry that is created is meant to stimulate self-reflection that makes the situation problematic for all parties involved.

The dialogue reflectionism initiates by computer-mediated communication is a tool of performance-based inquiry that rapidly escalates the engagement and the associated discourse to the highest level of authority willing to engage in the immediate situation. In reflectionist situations, one might expect a manager to come running out to see what is going on, and become personally engaged in the dialog. Employees responsible for security suddenly become available for immediate discussion. This is research in action, confronting agents directly and attempting to engage them in dialogue that is otherwise difficult to initiate because the high level managers are not usually available to ordinary people.

Reflectionism is a program of inquiry-in-performance. It is directed (a) toward uncovering the panopticon and undercutting its primacy and privilege, and (b) to relocating the relationship of the surveillance society within a more traditional commons notion of observablity. (Jacobs 1961; Ostrom 1990). Credible self and mutual monitoring in self-governing communities is a possible outcome when surveillance is deinstitutionalized. Thus, wearable computing affords the technological possibility of privacy as a common pool of resources over which no group has sole say or sway.

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 single parent families are scattered about at various activities. Most friends and relatives live in other parts of the city, continent or globe (Wellman 1999). Many coworkers are not collocated in the same spaces, and most shopkeepers do not know their customers personally.

Surveillance is a manifestation of the industrial and post-industrial eras of large hierarchical organizations, efficiently employing technologies in neopanopticons of social control. Contemporary societies are best characterized as "networked societies" (Wellman 1999). Yet, rather than being embedded in single communities or work groups, individuals switch among multiple, partial communities and work teams. In such milieus, individuals are largely responsible for their own security and integrity. They are more likely to need sousveil-

lance and coveillance, for they lack the protection of the village/community or hierarchical organization. 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.

Bell, D. and Kennedy, B.M. (Eds.). (2000). *The Cybercultures Reader*. London: Routledge.

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.

Dryer, D.C., Eisbach, C., and Ark, W.S. (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*. J. Agee (Trans.). London: Jonathan Cape.

Fogg, B.J. (1997). Captology: "The Study of Computers as Persuasive Technologies." In *Extended Abstracts of CHI '97*. Atlanta GA: ACM Press (129).

Fogg, B.J. (1998). "Persuasive Computers - Perspectives and Research Directions." *Proceedings of CHI '98*. Los Angeles CA: ACM Press (225-232).

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

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

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

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

Gaver, W. and Dunne, A. (1999). Projected Realities - Conceptual Design for Cultural Effect. In *Proceedings of CHI '99*. Pittsburgh: ACM Press (600-607).

Goffman, E. (1966). *Behavior in Public Places: Notes on the Social Organization of Gatherings*. New York: Free Press.

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

Huxley, A. (1958). *Brave New World Revisited*. New York: Harper. (p. 43)

Ingham, R. (1978). Privacy and Psychology. In *Privacy*, J. B. Young (Ed.). Chichester: Wiley (35-57).

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

Keel, R. (2001). "Ethnomethodological Perspective (on Crime and Deviance)." *Encyclopedia of Criminology and Deviance*, C. Bryant (Ed.). New York: Taylor and Francis (148-153).

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

Lofland, L.H. (1998). *The Public Realm : Exploring the City's Quintessential Social Territory.* Hawthorne, N.Y: Aldine de Gruyter.

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

Mann, S. (1998a). "'Reflectionism' and 'Diffusionism': New Tactics for Deconstructing the Video Surveillance Superhighway." *Leonardo* 31(2): 93-102.

Mann, S. (1998b). "Humanistic Intelligence/Humanistic Computing: 'WearComp' as a new framework for intelligent signal processing." *Proceedings of the IEEE* 86(11): 2123-2151+cover. [also on-line] at: http://wearcam.org/procieee.htm

Mann, S. (2000a). "Comparametric Equations with Practical Applications in Quantigraphic Image Processing." *IEEE Transactions on Image Processing* 9(8): 1389-1406. [also on-line] at: http://wearcam.org/comparam.htm

Mann, S. (2000b). "Computer Architectures for Protection of Personal Informatic Property: Putting Pirates, Pigs, and Rapists in Perspective." *First Monday* 5(7) [on-line] at: http://www.firstmonday.dk/issues/issue5_7/mann/

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

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

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

Milgram, S. (1977). *The Individual in a Social World* . London: Addison-Wesley.

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.

Pentland, A. and Choudhury, T. (2000). "Face Recognition for Smart Environments." *Computer*, 33(2): 50-55.

Rhodes, B.J., Nelson, M., and Weaver, J. (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. (1993). "Disrupted Borders: An Intervention." In *Definitions of Boundaries*, S. Gupta (Ed.). London: Rivers Oram.

Seabrook, T. and Wattis, L. (2001). "The Techno-Flaneur: Tele-Erotic Re-Presentation of Women's Life Spaces." In *Community Informatics: Shaping Computer-Mediated Social Relations*, L. Keeble and B.D. Loader (Eds.). London: Routledge (240-259).

Spears, R. and Lea, M. (1994). "Panacea or Panopticon? The Hidden Power." In *Computer- Mediated Communication Research*, 21(4): 427-459.

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

Ward, T. (1985). The Situationists Reconsidered in *Cultures in Contention*, D. Kahn. And D. Neumaier (Eds.). Seattle: The Real Comet.

Webster, C.W. and Hood, J. (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 *Networks in the Global Village*, B. Wellman (Ed.). 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.