

Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments ¹

Steve Mann²

Electrical and Computing
Engineering
University of Toronto

Jason Nolan

Knowledge Media Design
Institute
University of Toronto

Barry Wellman

Sociology
University of Toronto

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.

Sousveillance: New Methodologies

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 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 to of somehow finding someone to be observed by somewhere. . . (Dürrenmatt 1988, 23).

Sousveillance: Surveilling the Surveillers

Public surveillance of private space has become ubiquitous. Modern social surveillance finds its roots in the organized and asymmetric power structures of Jeremy Bentham's (1838 [1967]) Panopticon, a centralized arrangement for social controllers to visually observe (usually acquiescent) people's behavior.

¹ 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, Monica Prijatelj, and Rhonna Robbins-Sponaas. The performances described here were supported in part by the Canada Council for the Arts.

² mann@eecg.toronto.edu: Tel.: (416) 946-3387; Fax: (416) 971-2326; www.wearcam.org

Contemporary western society has 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; Lefebvre 1991). This replacement of technologies and data conduits has brought new opportunities for observation, data collection, and sur/sousveillance.

All such activity has been *surveillance*: organizations observing individuals. One way to challenge and problematize both the surveillance and the acquiescence is to re-situate these technologies of control on the individual. By this means, individuals can use panoptic technologies to observe those in authority. We call this inverse panopticon “*sousveillance*” 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. Thus, reflectionism is a technique for inquiry-in-performance. It is directed (a) toward uncovering the panopticon and undercutting its primacy and privilege, and (b) relocating the relationship of the surveillance society within a more traditional commons notion of observability (Jacobs 1961; Ostrom 1990; Newman 1973). In this manner, reflectionism is related to the Theater of the Absurd (Bair 1978), and the Situationist movement in art. It is especially related to “*detournement*”: the tactic of appropriating tools of social controllers and resituating these tools in a disorienting manner as a research method (Rogers 1993; Ward 1985). Reflectionism 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). Reflectionism is *sousveillance* when it is applied to individuals using advanced technological tools to observe the organizational observer.

Sousveillance focuses on enhancing the ability of people to access and collect data about their surveillance. It differs from other empowerment solutions that seek to assuage privacy concerns by regulating surveillance (Rhodes, et al. 1999). When information and regulation are largely controlled and exchange by external agents over which the individual has little power, such regulation is as much pacifier as solution.

How will *sousveillance* play out when individuals encounter large organizations? Probably the best-known recent example of *sousveillance* is when a Los Angeles resident videotaped white police officers beating African-American Rodney King after he had been stopped for a traffic violation (Cannon 1999). Yet, *sousveillance* often violates rules stating that ordinary people should not use recording devices to record official acts.

Studying Sousveillance

In this paper, we examine how using wearable computing devices can promote personal empowerment in human technology/human interactions (Mann 1997; Fogg 1997). Key issues are the extent to which organizational surveillance can be challenged, and the ways in which organizations respond to such challenges. We describe and analyze here a set of performances that follow Harold Garfinkel’s ethnomethodological 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.

The primary goal of this paper is to explore the techniques of data collection while engaging in dialogues with workers who are at the point of contact in semi-public and commercial locations. The performers engage these front-line workers (managers, clerks, security workers, etc.) without claiming to understand hierarchical considerations or politics within their organizations. Instead, the performers instigate situations to gauge the degree to which such workers try to suppress video/photographic sousveillance in locations where it is forbidden. To do so, the performers break unstated rules of asymmetric surveillance while using newly-developed wearable computing devices. In this way, the usually *surveilled* individuals become *sousveilleurs* as they engage the workers, using devices that mirror the usual techniques these workers use.

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).

Mobile, personal, and wearable computing devices have allowed individuals to take the personal computing revolution beyond the office, school, and home. Personal computing has enabled individuals to *feel* more empowered vis-à-vis organizations (Wellman 2001). The development of personal computers and the decades-long development of wearable technology makes possible the use of wearable computing devices by sousveilling performers. As a response to institutional and organizational surveillance of individuals, these new wearable inventions allow people to invert the gaze and watch—collect data on—the watchers. The wearable systems provide electrical connections to and from the body, as well as multimodal sensory interfaces. These allow remote communication with the body by wireless communications. EyeTap technology (www.eyetap.org) has evolved as a system for causing the eye itself to function as if it were both a camera and a display (Mann 1997, 2001; Mann and Niedzviecki 2001).

The development of wearable computing fits well with contemporary social transformations. 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). 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. 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. As a technique that situates the individual as simultaneously master and subject of the gaze, wearable computing devices offer a new tool in the usually one-sided dialogue of surveillance.

Hypotheses

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.

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 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 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 "*coveillance*," 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 One: Wearable Computer with Wearable Data Projection System

This performance takes place on a public street and 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.

When the devices are inactive, the wearer of the devices and the device itself 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.

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 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. Audience comments reveal that the technology itself is seen as a form of authority. Potentially critical audiences, shoppers, or young adults lining up for fashionable dance clubs, were favorably-to-neutrally disposed toward product displays on the device but disdained 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.

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. 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 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 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 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.

Challenging the notion of surveillance, along with role reversal (surveillance versus sousveillance), gives rise to a reversal of performer versus audience. 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 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 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.

The more highly surveilled a space is, the more objections are raised about such sousveillance, 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.

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 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 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. 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 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 Fig. 3).

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 (Mann and Niedzviecki 2001). (See Fig.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, etc. — 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, 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 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 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 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 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 Fig 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 was 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 up 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).

Summary: Performing Sousveillance

This paper has defined, described, and explored sousveillance techniques as a conceptual framework for data collection. 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 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.³

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 instance, 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 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.

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; 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

³ As Friedenbergh (1981) and Moore (1995) note, this may differentiate Canadians from Americans. It would be interesting to replicate these performances in other cultural contexts.

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 Methods in Society

The performances show how certain kinds of rule violation can assist in data collection. 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 (as the performers appear to be) 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.

The performances described here represent a method of inquiry that functions through engaging, challenging, and inverting of the power structure of surveillance. The role reversal between the surveilled individual and the act of surveillance allows for the exploration of social interactions generated by these performances. It raises questions for further inquiry; primarily issues of the collection and use of data 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 sousveillance to bear on surveillance workers whose profession it is to maintain such hierarchies of control.

Sousveillance's techniques work by inverting the techniques of surveillance that Bentham's Panopticon institutionalized. It is a conceptual model of reflective awareness that seeks to problematize social interactions and factors of contemporary life. The ubiquitous surveillance that sousveillance affords may, in the end, only serve the ends of the existing dominant power structure. Universal sousveillance may support the power structures by fostering broad accessibility of monitoring and ubiquitous data collection. Or as William Gibson comments in the movie *Cyberman* (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 society, the actions of all may, in theory, be observable, though perhaps not accountable. Although sousveillance would not eliminate unequal power in societies, it would provide the less powerful with useful tools and levers.

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.
- 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.
- Evangelista, Barry. (2002). "Surveillance Society: Don't Look Now, But You May Find You're Being Watched." *San Francisco Chronicle*, September 9. [on-line] 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*, A. Sheridan (Trans.). New York: Vintage.
- Garfinkel, H. (1967). *Studies in Ethnomethodology*. Cambridge: Polity.
- 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.
- 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. (2001). *Intelligent Image Processing*. John Wiley and Sons.
- 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.
- 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., 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.
- 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.

Figures

Figure One

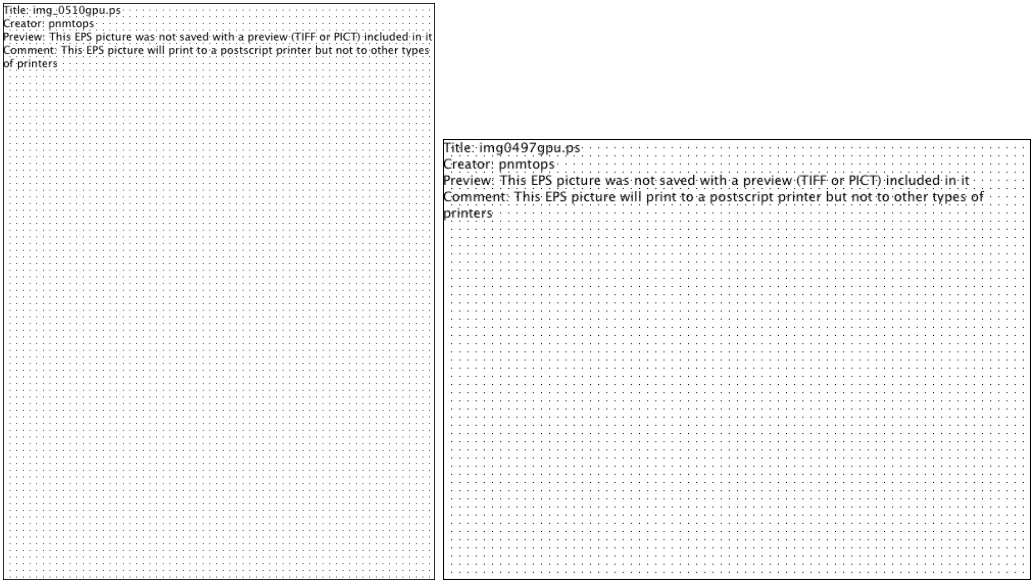


Fig. 1. (a) The wearable device contains a 1 GHz P3 CPU, rendering engine, high-power mercury vapour arc lamp data projector, within a black flame-retardant Nomex (TM) uniform custom tailored to fit the wearer. Here a person can see his own image together with other computer generated material. (b) Close-up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

Figure Two

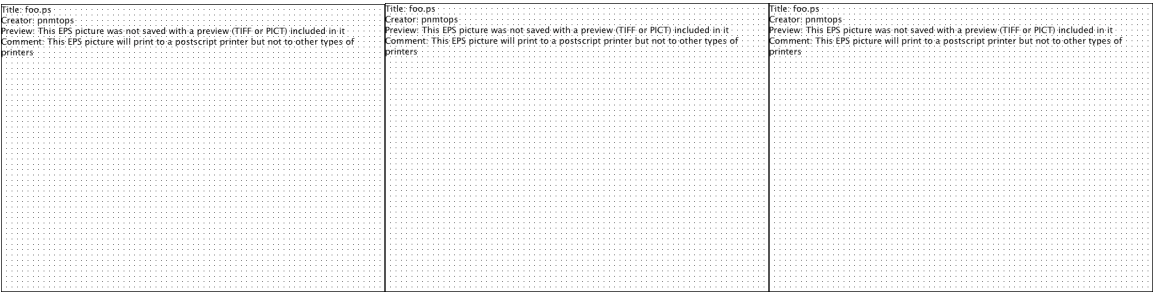


Fig. 2. (a) On the street, people would bring their children over to play in the wearable interactive video environment and performance space. (b) Large crowds gathered to see the interactive environment. (c) Even adults enjoyed playing in the interactive space.

Figure Three

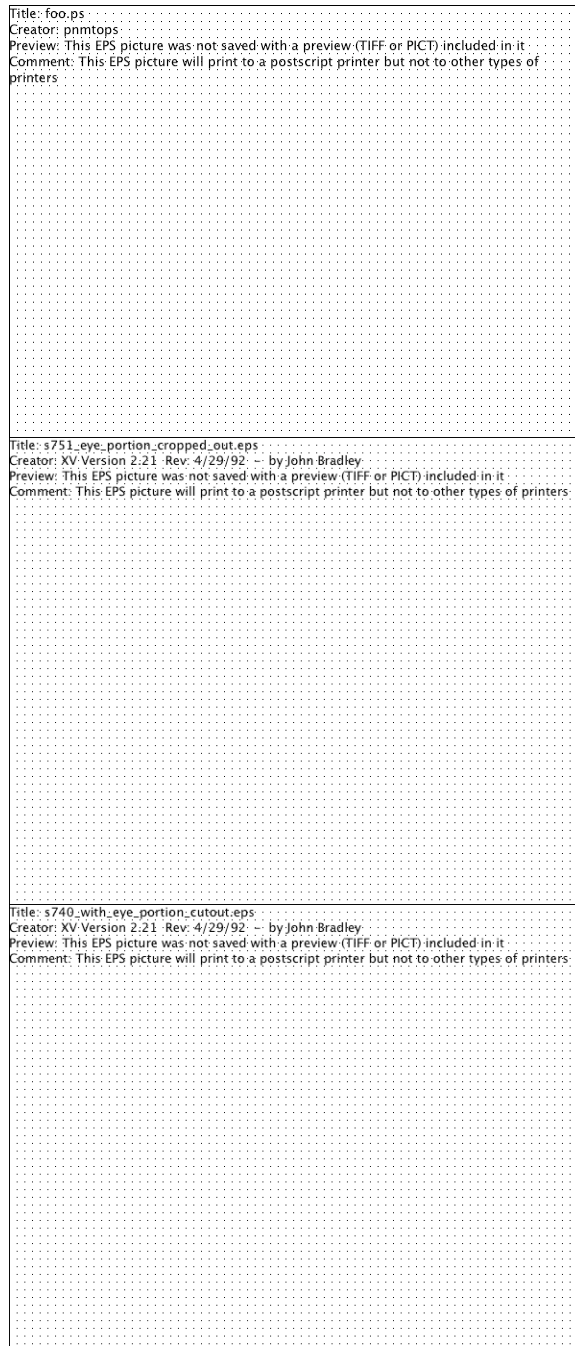


Fig. 3. (a) Projected text: "Cameras reduce crime; for your protection your image shall be recorded and transmitted to the EXISTech.com image and face recognition facility."

Figure Four

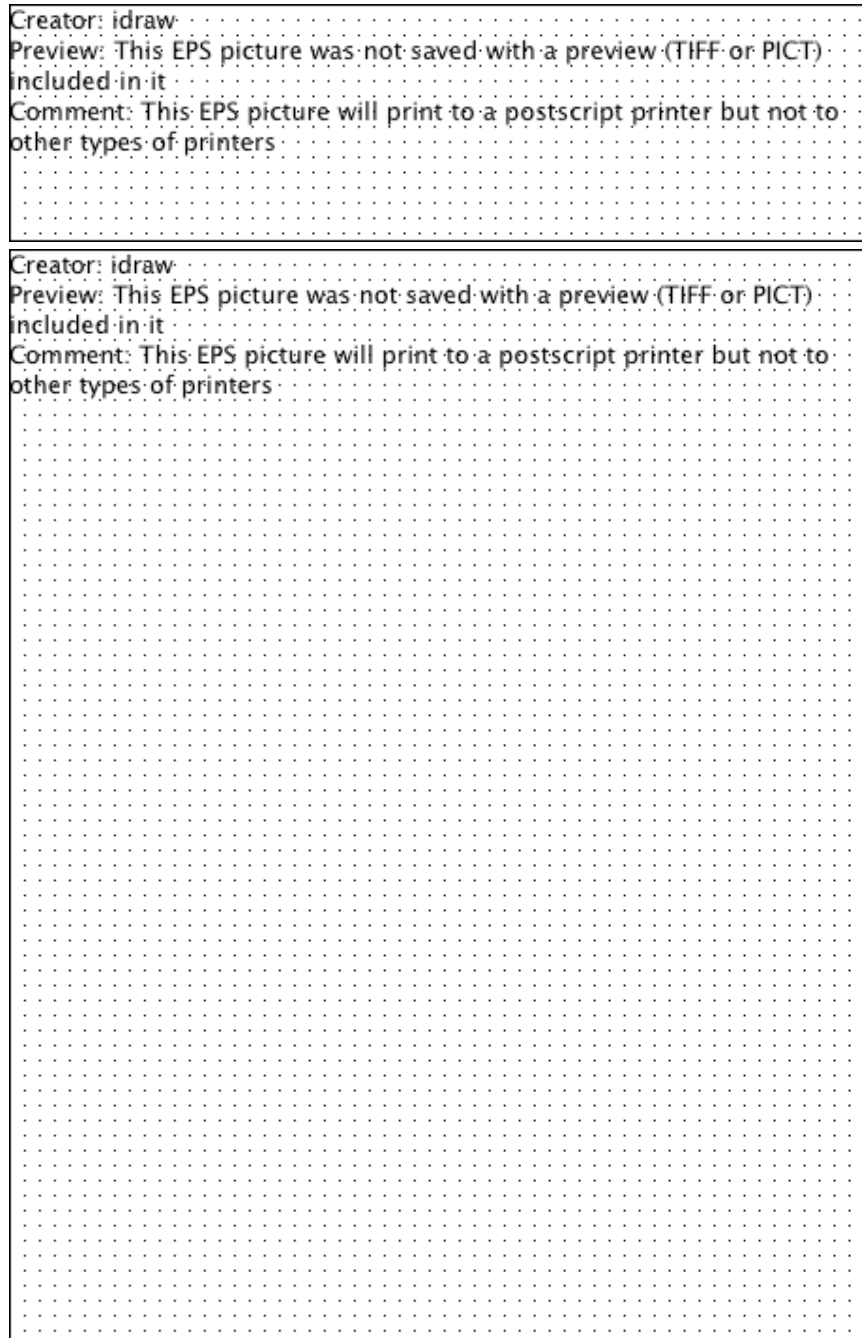
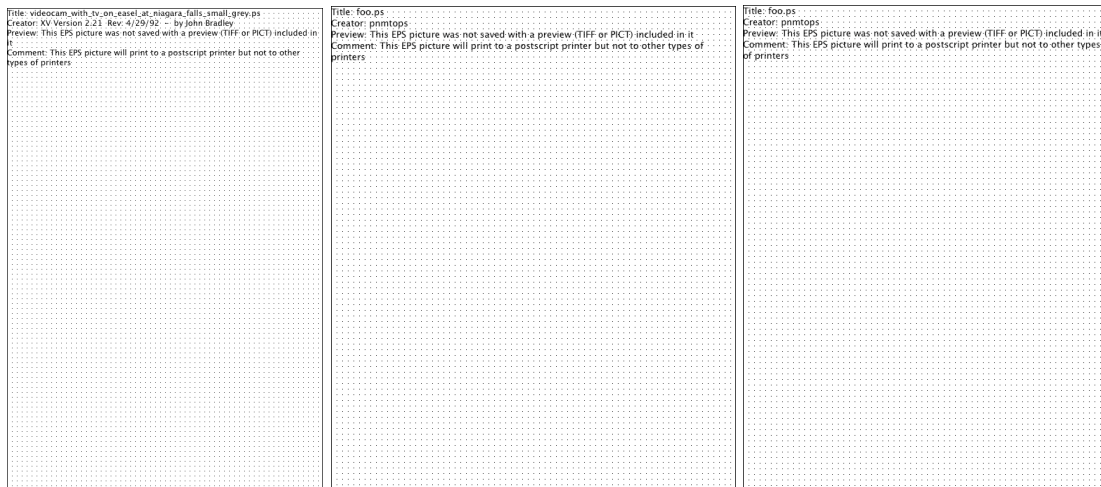


Fig. 4. EXISTech's corporate brochure was created to present the artifacts of sousveillance in the context of high fashion, as high cost purchased goods. This contextualizes sousveillance products and services as legitimate elements of conspicuous consumption in our consumerist society.

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.