Humanistic Intelligence
Steve Mann

Fig. 1 My 1970's effort at building a personal information space which culminated in this apparatus of 1980.

One of the fundamental contrasts between free democratic societies and totalitarian systems is that the totalitarian government (or other organization) relies on secrecy for the regime but high surveillance and disclosure for all other groups, whereas in the civic culture of liberal democracy, the position is approximately the reverse.
From Simon Davies (pertaining to the massive 1987 Australian campaign against a national ID card)

Introduction

Increased surveillance is often presented as a "solution" to increased crime, instead of solving the problem at its source, such as by mitigating loss of community connectedness.

Urban violence, and other forms of crime, have made it necessary, in some people's opinion, to dramatically escalate the use of measures, such as surveillance. These measures, which are brought on by large organizations, threaten the existence of a free and democratic society.

Overtly violent crimes in New York City, for example, have appeared to be less frequent, but much of this has been accomplished through the rolling back of civil liberties. Random searches, "no-knock" entry, and, most notably, increased surveillance, have ushered in a new world order of "law and order."

The recent proliferation of video surveillance cameras, interconnected with high speed computers and central databases is moving us toward a high-speed "surveillance superhighway." Cameras are used throughout entire cities (such as Liverpool and Baltimore) to monitor citizens in all public areas.

With other forms of one-sided surveillance such as fingerprinting of welfare recipients and see-through-clothing cameras for "securing buildings from employee theft" and "for police to covertly monitor crowds for weapons" (Nowhere to Hide by Joe Constance,), architects of

the "surveillance superhighway" promise us a future of reduced crime, while at the same time construct for us a future of reduced accountability for themselves.

The city has become a frightening place, and drastic "solutions" are stepped up to meet in equilibrium with the "drastic problems." A goal of my work is to challenge both sides of this equilibrium, which appear to feed on one another.

It is arguably true that organizations that use totalitarian video surveillance tend to have fewer overtly violent crimes. What I mean by totalitarian video surveillance is that the video signal is observable by only a select group, and that accountability is denied through restrictions on the collection of video by others.

A Mafia-run gambling casino might be the most extreme example of a totalitarian video surveillance environment (e.g. that the casino wants to know everything about everyone but reveal nothing about itself). In such an organization one would not expect to find any overt physical violence but there still might be occasional "disappearances" of those not favorable to the organization.

Many department stores also use video surveillance extensively, yet prohibit others from using cameras in their establishments. A goal of my work is to provide a technological framework to challenge such restrictions. A top-down panopticon-like surveillance hierarchy tends to make Jeremy Bentham's philosophy a self-fulfilling one. The sense of community that once existed, whether in the form of close-knit communities or the more modern "neighbourhood watch" (e.g. trust in other members of the community), has been replaced by absolute trust in governments, large corporations, or other unseen authorities, analogous to the unseen guard in Bentham's watchtower.

An important goal of my work is to set forth a foundation that I call "Humanistic Intelligence" (H.I.) as a basis for the existential principle of self-determination and mastery over our own destiny, as well as the humanistic notion of self-actualization.

"Humanistic Intelligence" differs from Artificial Intelligence in the sense that the goal is to "become" intelligent, through prostheses of sorts, rather than be replaced or disenfranchised by intelligent machines. Thus H.I. challenges the notion of environmental intelligence and ubiquitous surveillance. Rather than "smart rooms," "smart floors," "smart ceilings," "smart toilets," "smart light switches," etc., H.I. puts forth the notion of "smart people."

An important goal of H.I. is to take a first step toward a foremost principle of the Enlightenment, that of the dignity of the individual. This is accomplished through a prosthetic transformation of the body into a sovereign space.

Past and present works

I constructed a series of reflectionist and diffusionist (Reflectionism and Diffusionism: new tactics for deconstructing the video Surveillance Superhighway (1978—1996), by Steve Mann, 1996) performance pieces in order to challenge the notion of totalitarian surveillance, as well as challenge and appropriate the notion of higher and unquestionable authority.

Here I describe experiments and performances that I have conducted and purposely taken to the extreme in order to (a) illustrate a point and (b) experience reactions and observations first hand. It is not likely that the average reader would go to these extremes but some more subtle

variations of these experiments and performances may still be used to provide similar insight or reactions.

My Manager: Externalization of the locus of control

By "externalization of the locus of control," I am referring to the phenomenon you experience when, for example, you're standing at a department store customer service counter. The clerk has the power of various support media, and might, for example, defer his or her judgment (or pretend to defer his or her judgment) to an external entity such as a telephone (ostensibly that of another entity at the other end of the communications channel), a computer screen, or other form of media to which you do not share the privilege of access. In this sense, the clerk may, if desired, absolve himself/herself from responsibility for his/her own actions.

Centralized computing, in particular, has ushered in a new era of this form of externalization. A department store clerk may tell us, perhaps untruthfully, that "I cannot process your return; the computer won't let me." Often the clerk does have the ability to fulfill the request, but chooses voluntarily to be subject to (or to appear to be subject to) a higher and unquestionable authority. Thus the customer is placed in an inferior position of not knowing whether the clerk is acting on his/her own will, or the will of a higher authority that is not subject to question by you, the customer.

This tactic is often the practice of used-car sales representatives who might, for example, say, "I'd really like to give you the car for $2,000, but let me check with my manager," and then disappear into a back room for a few minutes, have a cup of coffee, all alone, and then emerge to declare "My manager won't let me sell it to you for that low . . ."

One of my performance pieces, entitled My Manager was a reflectionist performance piece in which I attempted to provide myself with the same kind of support infrastructure. This was achieved through construction of various forms of a personal information space comprising a computer in a backpack, connected to a display situated over one or both eyes[1] with a radio teletype interface to a remote "manager."

In this way, I carried with me, in my clothing, a support infrastructure that made it ambiguous as to whether my thoughts and such were my own, or those of a remote entity.

My apparatus differed significantly from a two-way voice radio, where it is clearly apparent to anyone else when the unit is being used. Later, the laptop computers that evolved in the 1980s still failed to provide the ambiguity and uncertainty of my earlier apparatus.

My Manager was my attempt to return to the Enlightenment, and declare the sovereignty of the individual, through the illusion of its subversion. In the spirit of the situationist tradition, I have created a detournement of my own subversion.

Painful Disconnect

In a further embodiment of the My Manager performance, a remote agent of my choosing may also provide remote control of my body, in the Stelarc sense, so that I can further subvert myself to an authority that acts in my own interest yet is inaccessible to, and unquestionable by, others.

I may also choose to be given an "electrical corrective signal" (through a high-voltage step-up transformer connected to my garment-based computer) should I become disconnected from the Internet. Thus, if I am asked to step into an elevator or the like, I can honestly reply that this would inflict great pain on me.

In that sense someone who forced me to enter an environment in which I might lose radio contact with potential outside accountability would be committing an act which is equivalent to torture.

As torture is viewed as a human rights violation, the goal of this performance piece is to suggest that disconnectivity, against one's will, should also be viewed as a human rights violation.

Painful Disconnect makes real the notion that denial of the right to self-surveillance by friends and family is equivalent to possible torture or other mistreatment.

Necessification

Because of the long-term adaptation process which I have undergone in the use of this apparatus (e.g. that I have worn it for many years), I have come to rely on it to see properly, and thus in some sense, it has become a visual prosthetic device (Eudaemonic Eye,).

Further toward making it absolutely essential that I wear the device, it also serves as a personal status monitor, e.g. a health monitor of sorts, and therefore, in some sense, asking me to remove it is a first step toward not only placing me in danger of tripping or falling (e.g. injury) but also asking me to put my life in danger through the absence of a health monitor that might otherwise bring medical aid should my heart show early signs of incipient malfunction or the like.

The Personal Safety Device

H.I. provides a further framework for personal safety by acting as a protective and defensive agent. For example, I am able to announce my location to one or more people of my choosing, either automatically through a GPS-ready radioteletype interface, or through a direct input device (e.g. a series of pushbutton switches integrated into my belt or clothing).

Various sensory apparatus I have incorporated into clothing measure both me and my environment. These sensors include a 24.360 GHz radar set, a 10.250GHz radar set, video cameras, microphones, infrared vision system, as well as a variety of sensors that measure quantities upon my own body, such as my heart rate (ECG), footstep rate (transducers in my shoes), etc. Intelligent signal processing may be used to construct an automated personal safety system. The inputs from the various sensors form a feature vector that may be processed by the circuits I've built into my clothing (e.g. 133MHz 586 processor running under the Linux 2.0 operating system, along with various special purpose DSP hardware, TMS320 series processors, etc.).

As an example of how intelligent signal processing can be used as a protective entity, consider what happens when one is approached by an assailant wielding a sawn-off shotgun and demanding cash. In such a situation, the victim's heart rate is apt to increase but with an inexplicable decrease in footstep rate (owing to the assailant's request that the victim stop and hand over a wallet or the like).

Consider a quotient of heart rate divided by footstep rate. One could easily imagine how this quotient, taken over a certain time window, could provide a rough indication of distress. In actual fact, I've been developing more advanced intelligent signal processing algorithms, which include, for example, situational awareness.

Electric Feel Sensing: Synthetic Synesthesia of Sixth and Seventh Senses

Another example of intelligent signal processing comprises a radar system which I have built into my clothing, to provide me with the ability to "feel" if someone sneaks up behind me. The radar system establishes a far-field electromagnetic wave pattern whose demodulated Doppler output is processed and used to drive vibrotactile transducers connected to my body. In this way, when someone sneaks up behind me, I can feel them "pressing" against my body, even though they are still some distance away. The closer they get, the stronger I feel them "pressing" against my body. At 20 or 30 meters, the feeling is very faint, while at 10 meters, the feeling is stronger, and as they approach within stabbing distance, the feeling is much stronger, to the point of being difficult to ignore.

This kind of user-interface is intuitive, because it is mapped in a manner that establishes a one-to-one correspondence with me and my environment. When someone sneaks up behind me from the left, for example, I can feel them "pressing" against the left side of my back, and likewise to the right.

Systems of this nature provide me with additional senses (such as radar, sonar, etc.) beyond the normal five senses. However, to be perceptible, I map the additional senses onto the usual five senses, a mapping that I call "synthetic synesthesia."

Furthermore, the mapping need not be one-to-one. For example, I often map the radar system into more than one of my five senses. One such mapping I tend to favor uses the radar to also switch in a rear-looking video camera.

Intelligent signal processing may, in fact, be used to select the degree to which the rear-looking camera is mixed in, rather than merely switching it in. For example, I designed a radar system having both the in-phase and the quadrature components. Thus the signals may be processed to determine whether objects are moving toward me or away from me. Objects moving toward me from behind are of particular interest, because most objects that are behind me (such as the ground, parked cars, stationary objects) are moving away from me in a relative sense.

The portion of the Doppler spectrum corresponding to objects approaching me may be integrated to arrive at a saliency index. This saliency index is similar to the previosly described heartrate/steprate quotient in the sense that both of these saliency indices attempt to indicate to me or my processing agent the degree of attention that should be paid to some other instrument of situational awareness.

In the case of the radar system, the saliency index may be used to control a video mixer that controls the degree to which my attention is focused on my rear-looking camera. The image from the rear-looking camera is presented to my eye upside-down and backwards (e.g. the camera is mounted upside-down and a circuit is used to flip each raster of video from left to right), so that it appears to me as though the rays of light from behind me are passing through the back of my head, through my retina, and then through the optical center of my eye. This provides a system which obeys the true laws of projective geometry, and redefines the eye as

a device that captures a pencil of light rays from a single point in space, and merely projects this pencil of rays onto a single image plane. I view this image plane upon the miniature computer screen I have built into my eyeglasses.

With the radar's visual saliency index in the control loop, the rays of light from behind me may be modulated in brightness, to correspond with the amount of attention that the processing agent believes that they merit.

SafetyNet

Once a distress signal is detected (by intelligent signal-processing agents or manually by myself), a communications channel may be opened to friends and relatives who have been previously entered on my personal safety list. This communications channel includes live video and other environmental information, which is transmitted and recorded at remote locations in various countries around the world, so that it cannot be destroyed by a potential assailant.

Rather than notify police or other authorities, which could result in a high degree of false alarms, the system notifies members of my SafetyNet — a network of friends and relatives looking out for each other's safety. This approach to personal safety may be combined with a high degree of constant connectivity with others such as a radioteletype UNIX "talk" window open at all times, video conferencing from a first-person perspective (e.g. from a wearable video camera) open at all times, etc.

Such a form of personal safety device may also protect one from police brutality and various other forms of human rights violations.

Subversion of Panopticon with Wearable Wireless Webcam

Ordinary cameras have become much smaller now, thanks to the miniaturization afforded by modern technology. However, they still share a common attribute with their predecessors, namely that it is immediately apparent to anyone when the camera is being used, because one must bring it up to one's eye, and look through it, etc., and this usage pattern is likely to put an assailant or the like into an angry mode of thought. For example, in a situation involving police brutality, police may attempt to forbid photography or the like, or may attempt to intimidate those engaged in the practice of documenting an atrocity.

Another weakness of current camera technology is that the storage of images or video is local, so that those committing the atrocity may seize the storage media (film, videocassette, flash memory, floppy disk, or the like), claiming that they need it for "evidence," when in fact their wish might be that it be destroyed.

I established a "personal imaging" (Wearable Computing: A First Step Toward Personal Imaging, IEEE Computer, Vol 30, No. 2,) framework for obtaining video from a first-person perspective. This video is part of my personal information space, and therefore accessible to others via a wireless link to the Internet. This means that anyone with access to the Internet can view the images, and thereby take an active role in making sure that there are multiple copies of the images in various countries around the world, so that an assailant, or a violator of human rights, could not destroy the images. Even by placing me under duress, the images could not be destroyed, because I have chosen to not know how many copies of each picture or video sequence there are, or in which countries they are mirrored, archived, and backed up.

A principle of totalitarian video surveillance is that only the guards have access to the privileged vantage point afforded by video cameras. An important goal of my performance piece was to make the situation approximately the reverse, that is, my "personal imaging" system was a first step toward subverting totalitarian surveillance by making some video (at least mine) available to everyone.

I later constructed larger communities of individuals wearing cameras in order to make multiple image streams available to large numbers of individuals.

Recently, with the advent of the World Wide Web, I have simply turned my apparatus into a "WebCam," resulting in a further simplification of its use, and a further subversion of Panopticon.

My camera (WearCam, short for wearable camera) is situated in such a way that it is not possible for an assailant to determine whether or not an image is being captured at any given time. This is accomplished through having the camera worn in an always-active mode, so that it in fact functions as a visual prosthetic of sorts.

Maybe Camera

Fig. 2 A Firing Squad comprised of various individuals wearing Maybe Cameras. Here, even though I built these units, do not know which ones contain cameras with transmitters, transmitting to the World Wide Web.

I may also choose that the remote accountability afforded by my SafetyNet be of origin unknown to me, so that if I am asked "Are you recording me?", I might be able to say that I honestly do not know. This denial of accountability, for taking pictures in establishments where photography is prohibited, was explored through a performance piece called Firing Squad.

For Firing Squad, I constructed a number of "Maybe Cameras."

Furthermore, when challenged by representatives of the surveillance superhighway, we simply declared: these are uniforms — standard issue from Our Manager — which we are required to wear while running errands on company time.

Fig. 3 Close up view of one of the shirtbased realizations of *Maybe Camera*

A "Maybe Camera" is constructed by first cutting out a number of small (e.g. 8 cm by 13 cm) pieces of very dark plexiglass (e.g. with transmissivity in the 3%—15% range) and then placing a miniature camera and transmitter on one or two of these units, and dummy circuitboards and dummy lenses on the others. All units are fitted with leads to a 9 volt battery snap, regardless as to whether they are real units or dummy units. 11 units are then sealed in black epoxy, and allowed to set. A series of holes is drilled around the outside of each one, so that it can be sewn onto a shirt after making a small hole to insert the 9 volt battery snap so that it hangs inside the shirt. Prior to sewing the units onto the shirts, it is preferable to silkscreen the shirts with the words "For YOUR protection, a video record of you and your establishment may be transmitted and recorded at remote locations. ALL CRIMINAL ACTS PROSECUTED!!!".

Second Brain as Personal Diary without Contempt of Court

In many ways, I regard my rig, together with its personal information space, as a second brain — as a true prosthetic device.

Thus, even in situations in which I do make a conscious decision to record an image or video of some activity, I may wish that this recording be entered into a personal diary of sorts which is only accessible to "me." (The definition of "me" may include that which falls within my newly defined corporeal boundary, which might include, for example, other members of my SafetyNet.)

People have often felt uneasy entrusting to my second brain certain personal pieces of information, fearing that even if I made my best efforts to keep this information in confidence, it could be compromised through a subpoena.

Even if I were to protect it with ordinary encryption, its security may still be compromised through the process of torture or other forms of duress.

In the same way that our first brain is protected by the Constitution (the Fifth) from contempt of court for refusing to answer (self-incriminate), I desired to establish a means of protecting the "second brain" from self-incrimination.

My solution was to encrypt it with a key that I do not know myself. Thus I may encrypt materials with public keys of other members of my SafetyNet. In this way, my SafetyNet could recognize when I am under duress, and thus my inability to access my second brain would not be seen in contempt of whatever duress I might be placed under.

Life through the Screen: A Window to the Future

Many important questions were raised by these performance pieces and the new inventions upon which they were realized.

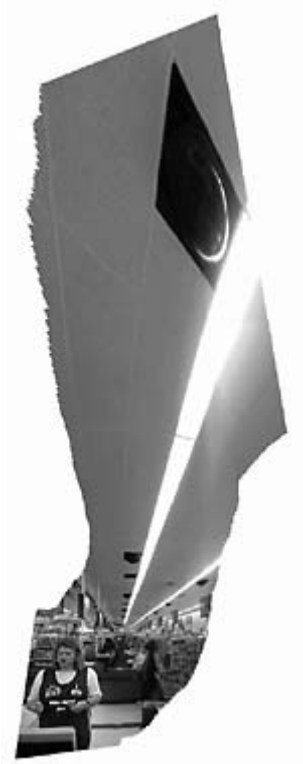
For example, My Manager provided a form of personal empowerment brought forth by the ability to take a solid stance and defer any questioning of my will to a (possibly fictitious) higher and unquestionable authority, just as representatives of establishments often do. However, there is also the danger that this could be abused, for example, as a means of controlling or enslaving people.

In particular, the exploration of the remotely controlled body raises not only the question of possible enslavement by a higher authority that is not actually acting in the best interest of the individual wearing the apparatus of control, but also some serious questions about the locus of responsibility for one's acts. As we move toward a future of networked personal information spaces, we will need to think carefully about how these worlds are constructed.

The goal of humanistic intelligence, that of providing the individual with an increased degree of self-determination and mastery over his or her own destiny, will have to compete against the goals of utilitarianism, and the desire merely to increase workplace productivity and make people more useful to society.

Will we see a future of "cyborgs," as "puppets" on a virtual string, imprisoned in their workcells, carrying out the orders of an omnipotent boss, or will we see a healthy community of free self-actualized citizens looking out for each other's safety and well-being?

This is the question that we must carefully consider as our "corporeal boundary" will no longer end at the flesh, but, rather, will extend and diffuse into the ether.



© Steve Mann, Boston, Mass.

© Steve Mann, Boston, Mass.

Notes

1. I referred to this invention as a "personal computer," though, in recent years, that term has come to mean a desktop computer.
Thus my apparatus has, over the years, been called a "humanistic computer," "existential computer," "eudaemonic computer," "wearable computer," or the like.

I owe much to those around me, who have influenced my thinking: Rosalind Picard, Hiroshi Ishii, Krzysztof Wodiczko, William Mitchell, Obed Torres, Thad Starner, Olivier Faugeras, Kent Nickerson, Simon Haykin, and many others. I would also like to thank Chris Dodge for reading this essay and making some important suggestions.