Chapter 63: Learning by Being: Thirty Years of Cyborg Existemology

STEVE MANN
Department of Electrical and Computer Engineering, University of Toronto, Canada

1. INTRODUCTION

Since my childhood, a personal hobby of mine has been the functional modification of my own body, through technology. This modification often took the form of creating new sensory capabilities, as well as (what were to become eventually successful) attempts at correcting learning disabilities, such as visual memory impairment. I have had very particular experiences that speak to what it means to live within a virtual, and more importantly, a mediated (i.e., computationally modified) learning environment. I did not just experience virtual reality, mediated reality, etc., I became a cyborg, invented the technologies I needed to become a cyborg and then have spent 30 years learning and teaching about what it means to exist in a cyborg state. Originally I did this in private, but around 20 years ago I started, wearing a full computer system more openly, which resulted in my being referred to as a "cyborg" (although I do not particularly like the term because it is such a "loaded" term so heavily co-opted by science fiction). I came to best understand the term "cyborg" through a variety of discussions I had with Manfred Clynes, who coined the term. Thus I prefer to limit use the term to the Clynes sense, i.e., a synergy between human and machine that happens without conscious thought or effort (Clynes would often tell me that a person riding a bicycle was a cyborg because he or she would, after a while, forget that they were technologically modified).

As a "cyborg" (Mann, 2001) in the sense of long-term adaptation to the modified body, one encounters a new kind of existential self-determination and mastery over one's own environs (and to some degree, one's own destiny). Presently, in addition to having the internet and massive databases and video at my beck and call most of the time, I am also connected to others. While I am grocery shopping, my wife—who may be at home or in her office—sees exactly what I see and helps me pick out vegetables. She can imprint images onto my retina while she is seeing what I see. I call this collaborative mediated reality. I hope to add to the population of similarly equipped people; in the Fall of 1998, at the University of Toronto, I taught what I believe to be the world's first existemology course.

Existemology pertains to not just body modification, through technology ("cyborg primitives") but also to mind modification through long-term

J. Weiss et al. (eds.), The International Handbook of Virtual Learning Environments, 1571–1592.

adaptation. In this sense, existemology also extends into what I call the "post-cyborg" age, and thus also applies to the creation of a new state-of-mind that can persist after the technological prostheses are removed. In the sense that I found that this new state of mind could comprise an improvement, I thus encountered existemological therapy (i.e., improved condition even if the body modifications are removed or become damaged or inoperative).

The general ideas of existemology are themselves applicable to learning environments that have nothing to do with bodyborne computing. To some degree, beyond whether the technology is implanted, worn, carried, or non-existent, what can be learned is an educational paradigm that embodies an epistemology of personal choice, and the metaphysics of personal freedom, growth, and development.

2. FROM "LEARN BY DOING" TO "LEARN BY BEING": EXISTEMOLOGY AS A CONTINUATION OF CONSTRUCTIONIST LEARNING

"Love is a better master than duty"

—Albert Einstein

I begin by contextualizing my current teaching practice, and then expand upon how my "cyborg" existence led up to this current practice.

MIT is known for its Constructionist Learning, and in fact a new building is now being built at MIT, with a 42 million dollar donation, to house MIT's Constructionist Learning research effort. Constructionist Learning is, loosely speaking, "learn by doing and creating" (See, for example, http://www.jasonnolan.net/papers/doing.html).

What I mean by existemology is "learn by being" in the sense of a technologically self-modified being that encompasses long-term adaptation.

It includes a kind of "deconstructist learning" toward an emphasis on learning by involvement (learning by involvement in that which matters to the individual who is learning—learning by "being" at one with the subject matter).

This approach has worked very well for teaching personal cybernetics, wearable computing, and personal imaging, e.g., so students can learn by being at one with the very machine they are trying to learn about. But existemology can be applied to other research topics.

Existemology follows naturally in the evolution from traditional learn by rote, to building upon (De)Constructionist Learning, and onward.

I further developed existemology through a graduate level course, (course number ECE1766), beginning September 1998 (See Figure 1). In this course, I not only taught students about Personal Imaging, EyeTap, and Wearable Computer (WearComp), but I also taught them how to learn by "being at one with the machine". By becoming at one with the machine, they, in effect, became the machine. In this way, they learned by "being" the computer, and

Figure 1. Wearing my eyeglasses which embody the EyeTap technology of both image capture and image display (the special glasses look just like ordinary bifocal eyeglasses) I teach a class of about 20 students, how to become one with the machine. Here I teach how to use the standard Xybernaut wearable computer product. I also teach the students how to build their own systems, and many of the new scientific principles in the emerging field of Personal Cybernetics.

discovering the existential principle of self-empowerment and self-exploration which typically happens after a couple of months of continuous use of a WearComp system.

With more than 20WearComps, facilitated by in-kind equipment donations of various components from Xybernaut, clear-NET, WaveRider, Kodak, and various other companies, I taught my course with an emphasis on networked multimediated visual reality (loosely speaking "how to become a photographic cyborg"). This course allowed students to create their own version of reality, in their ordinary day-to-day living. What I discovered, is that students learned a great deal more, and explored a great many different avenues of pursuit, than is typically the case in a traditional "learn by lecture", or even a constructionist "learn by doing + creating" course.

Such an approach gave rise to an epistemology of choice, in the interpretation of a computer-mediated reality that captures the essence of post-modernist deconstructionism. This "deconstructionist learning" involves not just putting things together, but also taking things apart to learn how they work. Thus an important element of a "deconstructionist education" (DeconEd) is learning the art of *reverse engineering*.

I found in my ECE1766 course, that the desire to participate was overwhelming. It was delightful to see the tremendous desire to learn, even among student "listeners" who do not get course credit.

It is unusual to find students so eager to learn that many who do not need the course credit still attend. However, in my course, this was very much the case.

It seems that a new concept in education has been discovered—a new concept in education that awakens a passionate quest for knowledge—not merely the facts presented on corporate device specifications sheets that can make us more useful to society, but also the hidden secrets of how things work, and how they were originally invented.

If science should be "unlocking (or discovering) the secrets of God", then, at least in some ways, computer science can be unlocking (or discovering) the secrets of corporations (i.e., other humans working in the corporations that produce proprietary products, etc.).

Deconstructionist learning particularly emphasizes this approach to understanding how things work, by taking them apart. This echoes my early childhood experiences of building various systems from a zero budget, through the collection of junk, garbage, and various refuse, to repurpose in new ways. Thus my life was one of creative exploration in first understanding how things work, and then using that understanding to synthesize new inventions from the components found in existing technologies, combined with the new technologies that I invented.

At the time, much of what I was doing would later seem like science fiction to others. The fact that many of my cyborg technologies of self-modification pre-dated the later "borglike" visions of science fiction, made it all the more difficult to explain these concepts to my peers, because there was not even the reference in science fiction at that time, as a basis for explanation.

In the early days, most of the discrimination that I faced was peer discrimination, rather than institutionalized discrimination by authority figures. Thus the main difficulties of my childhood were more from communal changing of clothes associated with sports, or gym class, rather than from the official machinery of airport security, which then was quite lax.

There was eventually to be a reversal, in which I found a great deal of peer acceptance, whereas the large organizations turned against my vision of the future. In particular, as time progressed, it became more socially acceptable to be a computer enthusiast, and the eventual (more recent) visions of science fiction gave a fun and creative reference. With commercial interest in my inventions, it even became fashionable to some extent, and people would often come over and talk to me, being very interested in the project. Although some of this change could be attributed to improvements in my inventions and designs, even when I re-connected to older systems I found the peer response (e.g., the general reactions from the public) to have become positive. Whereas people used to walk across the street to avoid me, or laugh at me, or be negative in other ways in the 1970s, and early 1980s, I had found peer acceptance started around 1984 (the era of new-wave androgyny where the blurring of gender lines seemed to make the blurring of human-machine lines equally acceptable). By the 1990s, the peer acceptance spread from the fringes of new-wave androgyny, the arts, and those on the creative fringes, to a more mainstream peer acceptance.

But the institutionalized acceptance diminished over time. Institutionalized discrimination began around 1985 when peer acceptance had just picked up. For example, while boarding the subway in Toronto, I was approached by concerned security guards, in the summer of 1985. The discrimination appeared to be correlated to security, and thus I found myself, as the years progressed, being terrorized by security guards, who threatened to use force to advance their political agenda of "security". It seemed that the more "security" there was, the more cyborg discrimination. This kind of annonyance intensified through the 1990s, with an unfortunate incident perpetrated by Air Canada (See for example, Paul Virilio, Crepuscular Dawn, pages 96–98).

2.1. Existential Contraband

More recently, for example, I was required to go to the US embassy to apply for a passport for my daughter (since she was born in the U.S.), but I was not allowed into the embassy because I was an electronic device, and electronic devices were considered contraband.

Thus I was simultaneously required to enter the embassy to get the passport, but not allowed to enter the embassy. In the end, the officials came out, and I swore my oath down at street level, rather than go up to the office, but this situation simply serves as an example of the absurdity of existential contraband that occurs when the body is permanently enjoined with technology.

3. WEB SURFERS' RIGHT-OF-WAY FOR BEACH ACCESS

3.1. Securityranny and Sabetyanny

Another example of institutionalized discrimination is in the realm of providing free wireless connectivity for a community of cyborgs. Back in the 1980s and 1990s this was viewed with great welcome by the official powers that be, as being a good thing. It attracted a lot of positive press coverage in the 1990s, and set forth a foundation upon which others built.

However, more recently, with new technologies that make it easier to support online access for cyborgs and for everyone, there is also a hysteria around the perceived liability issues. In the early days I had to build my own wireless equipment, and I had to help others build systems to get online on my network. I was, for example, welcomed by the New England Spectrum Management Council to establish online connectivity for my community of cyborgs in the early 1990s.

But more recently, when it is so much easier with new technologies like 802.11 wireless, the discrimination is mostly institutional. For example, officials feel that internet access should not be freely available to anyone,

because it could be used by terrorists, or copyright violators. These officials wished to impose security constraints on the network to prevent unauthenticated access.

So I constructed an "urbeach access" metaphor, e.g., that the internet is like an urban beach, that should allow access, right-of-way. With a traditional beach, property owners are often required to provide a public right-of-way that provides beach access. Property owners who build high fences all the way around all of the property, in the name of "security", are, through this excess security, denying that right-of-way could also thus incur liability. In addition to preventing people from enjoying the beach on hot summer days, property owners who, through security excess, deny bathers access rights could risk liability, e.g., if someone suffered heat stroke because they could not exercise their lawful right of access to the beach, or a more extreme case might be if someone spilled battery acid on themselves and could not get to the beach to wash it off in the lake or ocean. This could include civil liability in which a person would have had access, but for the unlawful excess in security.

Thus we see, by way of example, that the security equation has two sides, i.e., that an organization can be liable for having too little security OR TOO MUCH security. The too-little-security side of the equation is the only one that we usually hear about, since the other side of the equation is seldom expressed.

Now to relate the analogy to our present situation: Free anonymous wireless access to the net is something that can result in personal safety. Cyborgs, or others, who might otherwise reach the 'net but are prevented from doing so, could be at risk, e.g., from a mugging or other attack that might have been prevented with 'net access.

Thus any organization that wishes to shut down one of my (or anyone else's) free wireless 'net gateways needs to be informed of the liability that their "security" measure creates. By asking them to accept liability for discontinuance of a service that people are already using, one is better prepared to keep the 'net running.

Moreover, the absurdity of someone asking me to shut down my free 'net portal, or to protect it by password, is as absurd as requiring passwords for the enjoyment of other building resources like light, heat, HVAC, and the like. Imagine a building owner who decided to license the electric light in the building by saying that people need to authenticate before receiving the light. Thus anonymous users would need to walk around in the dark, but those wearing a transponder would get a "sight license" and could see. Those without "sight licenses" (such as visiting scholars who had not yet registered) might trip and fall in the dark. They would then have a case against the building owner, and thus the building owner exposes the organization to liability by excessive photonic security.

The same might be true of HVAC, e.g., a license to receive heat, cooling, fresh air, etc., including a breathing license, and a license to exhale, as well

as to dispose of bodily waste. Those who dispose of bodily waste without a license in UriNation, are punished by the officials of urinationalism.

Thus I had little trouble in convincing many others that the airwaves should be as free as the photons and the air we breathe, and that requiring authentication for basic safety such as connectivity is absurd.

Thus the birth of "free open-air beach access".

4. "WARE" AS CONTAMINANT IN SOFT*WARE*: DECONOMICS 101

The WearComp was invented as a kind of experiment in self-determination and mastery over one's own destiny that is characteristic of modern concepts like freesource (the GNU Linux operating system that currently runs on it, etc.).

We often encounter so-called "courseware" (educational softWARE), but, as educators, we have an ethical and moral responsibility for not just what we teach, but for our choice of tools with which to teach it. A "ware" is an article of commerce. Thus the word "software" carries with it, embedded in its very etymology, the ideals of commerce. But let us consider replacing "The new economy" (which has already come to a crash—the bubble has been burst), with "The new Deconomy".

To spend a lot of time learning how to use a particular proprietary computer program, is to become trapped in a way of thinking that is an article of commerce. But there is (or should be) also room for a "deconomics"—a deconist deconstruction of economics, that allows us to have the "Soft" and not the "Ware".

That is the essence of the philosophical context of "free software", "open source", "open course", and the like, that I prefer to call "freesource". Freesource emphasizes self-determination and mastery over one's own destiny. This "personal empowerment" aspect is what I believe to be a fundamental issue in operating systems such as GNU Linux. It is this aspect that WearComp and GNU Linux both share in common, and it is for this reason that GNU Linux was selected as the operating system for my existemology project.

An important goal of freesource is that of allowing anyone the option of acquiring, and thus advancing the world's knowledge base.

This eliminates the distinction between "programmer" and "user". It also erradicates the distinction between "developer" and "end user". And it blurs the boundary between "teacher" and "learner". Finally, it also gets rid of the boundary between consumer and producer.

(For a more satirical perspective on Closed Source, see http://wearcam.org/seatsale/) In the cyborg world, such concepts are heightened, in the sense that the computer becomes part of our own "thought" process. Thus the construct known as "humanistic intelligence (HI)" (Mann, 1998) also comes into play. HI is intelligence that arises by having the human being in the feedback loop of a computational process in which the human and computer are inextricably intertwined.

HI is motivated by the philosophy of science, e.g., open peer review, and the ability to (de)construct one's own experimental space. HI provides a new synergy between humans and machines that seeks to involve the human rather than having computers emulate human thought or replace humans. Particular goals of HI are human involvement at the individual level, and providing individuals with tools to challenge society's pre-conceived notions of human–computer relationships. An emphasis in this article is on computational frameworks surrounding "visual intelligence" devices, such as video cameras interfaced to computer systems.

A fundamental problem we face in today's society, as it pertains to computers, is computer program source code disclosure. GNU Linux has emerged as one solution, together with an outlook based on science and on self-determination and individual empowerment at the personal level.

Advanced computer systems is one area where a single individual can make a tremendous contribution to the advancement of human knowledge, but is often prevented from doing so by various forms of what is alleged to be "security" but what is really a form of security excess that is dangerous to the advancement of science. Since science often leads to improved safety, it is actually therefore possible that too much security can be dangerous. A system that excludes any individual from exploring it fully, may prevent that individual from "thinking outside the box" (especially when the box is "welded shut"). Such software hegemonies can prevent some individuals from participating in the culture of computer science and the advancement of the state-of-the-art.

A second fundamental problem pertains to some of the new directions in Human–Computer Interaction (HCI). These new directions are characterized by "computers everywhere", constantly monitoring our activities, and responding "intelligently". This is the "ubiquitous surveillance" or "pervasive surveillance" ("perveillance") paradigm in which keyboards and mice are replaced by cameras and microphones watching us at all times. Proponents of perveillance claim that we are being watched for our benefit, and that they are making the world a better place for us.

Computers everywhere, constantly monitoring our activities, and responding "intelligently" have the potential to make matters worse, from the closed source nature of the software, possibly excluding the individual user from knowledge not only of certain aspects of the computer upon his or her desk, but also of the principle of operation and the function of everyday things. Moreover, the implications of secrecy within the context of these intelligence gathering functions puts forth a serious threat to personal privacy, solitude, and freedom.

But the *surveillance state* locks us into a one-sided 20th century "us versus them" way of thinking. Surveillance alleges to define "good" people (the watchers), versus potentially bad people: Those "suspected" of evil (the watched).

Figure 2. Surveillance and Sousveillance: Surveillance is French for watching from above ("sur" meaning "from above" and "veiller" meaning "to watch"). Surveillance denotes the God's eye view of the proverbial "eye in the sky". Sousveillance brings the cameras from the heavens down to earth, i.e., from the lamp posts and ceilings, down to human level.

For this reason, we require the notion of "sousveillance" (inverse surveillance), from "sous" (French from under, or below), and "veiller" (French for "to watch"). Sousveillance is not merely:

- passengers photographing taxi cab drivers;
- shoppers photographing shopkeepers; and
- citizens photographing police;

but, rather, it is a construct that acknowledges the pastmodern world in which we live (See http://wearcam.org/sousveillance.htm) (See Figure 2).

In some sense, a cyborg who keeps a logfile (much like the "black box" flight recorder on an aircraft) of everything he or she expriences, is practicing the art of sousveillance. Such cyborg logfiles (also known as "cyborg logues", cyborglogs, or "glogs" for short), might also protect the individual from attackers, whether said attackers are from a higher or lower point along the "axis of evil". Thus the fact that glogs protect the wearer from human rights violations by police or other authorities, as well as attacks from muggers, etc., makes them "axis neutral", in the sense that they point everywhere, unlike surveillance from on high.

Students quickly learn about the post-modern notion of the absence of any clearly defined axis of evil. This causes them to question even the definition of "terrorism" or "terrorist" or "guerrorist". Many of the students, for example, began to compare the formal definition of "terrorist" to that of soldier, or police officer, and became confused. Thus, at the very least, "glogging", as it

is called (making cyborg logs) gave them the chance to ask questions, and to realize that life is not so clearly defined as one might have at first believed. This gave rise to yet another example of deconstructionist learning.

4.1. Computer Science versus Computer Secrecy

Science provides us with ever-changing schools of thought, opinions, ideas, and the like, while all building upon a foundation of verifiable (and sometimes evolving) truth. The foundations, laws, and theories of science, although true by assumption may at any time be called into question as new experimental results unfold. Thus when doing an experiment, we may begin by making certain assumptions, but at any time, these assumptions may be verified.

In particular, a scientific experiment is a form of investigation that leads wherever the evidence may take us. In many cases, the evidence takes us back to questioning the very assumptions and foundations we had previously taken as truth, and in some cases, instead of making a new discovery along the lines anticipated by previous scientists, we discover that another previous discovery was false or inaccurate. Sometimes these are the biggest and most important discoveries—things that are discovered by accident.

A situation in which one or more of the foundation elements are held in secret is contrary to the principles of science. Although many results in science are treated as a "black box", for operational simplicity, there is always the possibility that the evidence may want to lead us inside that box.

Imagine, for example, conducting an experiment on a chemical reaction between a proprietary solution "A", mixed with a secret powder "B", brought to a temperature of 212 degrees T. (Top secret temperature scale which you are not allowed to convert to other units). It is hard to imagine where one might publish results of such an experiment, except, perhaps, in the Journal of Irreproducible Results.

Now it is quite likely that one could make some new discoveries about the chemical reaction between A and B, without knowing what A and B are, and one might even be able to complete a doctoral dissertation and obtain a Ph.D. for the study of the reaction between A and B (assuming a large enough quantity of A and B were available).

Results in Computer Science that are based, in part, on undisclosed matters, inhibit the ability of the scientist to follow the evidence wherever it may lead. Even in a situation where the evidence does not lead inside one of the secret "black boxes", science conducted in this manner is irresponsible in the sense that another scientist in the future may wish to build upon the result, and may, in fact, conduct an experiment that leads backward, as well as forwards. Should the new scientist follow evidence that leads backward, inside one of these secret "black boxes", then the first scientist will have created a foundation contaminated by secrecy. In the interest of academic integrity, better science

would result if all the foundations upon which it were built were such as to be subject to full examination by any scientist who might, at some time in the future, wish to build upon a given scientific discovery. Thus, although many computer scientists may work at a high-level, there would be great merit in a computational foundation open to examination by others, even if the particular scientist using the computational foundation does not wish to examine it. For example, the designer of a high level numerical algorithm, who uses a computer with a fully disclosed operating system (such as Linux), does other scientists a great service, even if he or she himself or herself only uses it at the Application Program Interface (API) level and and never intends to look at its source code or that of the Linux operating system underneath it.

4.2. Obvious or Obfuscated

Imagine a clock that was designed so that when the cover was lifted off, all the gears would fly out in different directions, so that it would be more difficult for a young child to open up his or her parents' clock and determine how it works. Alternatively, imagine the clock was loaded with explosives, so that it would completely self-destruct upon opening.

Assuming a child survived such a bad experience, it is still doubtful that devices made in this manner would be good for society, in particular, for the growth and development of young engineers and scientists with a natural curiosity about the world around them.

As the boundary between software and hardware blurs, devices are becoming more and more difficult to understand. This difficulty arises in part, as a result of deliberate obfuscation on the part of product manufacturers. More and more devices contain general-purpose microprocessors, so that their function depends on software. Specificity of function is achieved through specificity of software rather than specificity of physical form. By manufacturing everyday devices in which there is provided only executable code, without source code, manufacturers have provided a first level of obfuscation. Further more, additional obfuscation tools are often used in order to make the executable task image more difficult to understand. These tools include strippers that remove object link names, etc., and even tools for building encrypted executables which contain dynamic decryption function that generates a narrow sliding window of unencrypted executable, so that only a small fragment of the executable is decrypted at any given time. In this way, not only is the end user deprived of source code, but the executable code itself is encrypted, making it difficult or impossible to look at the code even at the machine code level.

Moreover, devices such as Complex Programmable Logic Devices (CPLDs), such as the Alterra 7000 series, often have provisions to permanently destroy the data and address lines leading into a device, so that a single chip device can operate as a finite-state machine yet conceal even its

machine-level contents from examination. (An excellent tutorial on FPGAs and CPLDs may be found in(Brown & Rose, 1996)). Devices such as Clipper chips go a step further by incorporating fluorine atoms, so that if the user attempts to put the device into a milling machine, to mill off layer-by-layer for examination under an electron microscope, the device will self-destruct in a drastic manner that destroys structure. Thus the Clipper phones could contain a "trojan horse", or some other kind of "back door", and we might never be able to determine whether or not this is the case. This is yet another example of deliberate obfuscation of the operational principles of everyday things.

Thus we have a growing number of general-purpose devices whose function or purpose depends on software, downloaded code or microcode. Because this code is intellectually encrypted, so is the purpose and function of the device. In this way, manufacturers may provide us with a stated function or purpose, but the actual function or purpose may differ, or may include extra features, of which we are not aware.

5. EQUIVEILLANCE: THE NEED TO STRIKE A BALANCE IN THE EQUILIBRIUM BETWEEN SURVEILLANCE AND SOUSVEILLANCE

Of primary importance, students learned that the world is not so one-sided as they first believed, and in fact the "sur" and "sous" form a kind of "yin" and "yang". When we have only one, we are in a life-out-of-balance.

Never is this lack of balance so evident as in the proliferation of devices we call "environmental technologies".

There are a number of researchers who have been proposing new computer user-interfaces based on environmental sensors. Buxton, who did much of the early pioneering research into intelligent environments (smart rooms, etc.), was inspired by automatic flush urinals, (as described, for example, in U.S. Pat. 4309781, 5170514, etc.), and formulated, designed, and built a HCI system called the "Reactive Room" (Cooperstock & Buxton, 1995; Cooperstock et al., 1997). This system consisted of various sensors, including optical sensors (such as video cameras), and processing, so that the room would respond to the user's movement and activity.

Increasingly we are witnessing the emergence of "intelligent highways", "smart rooms", "smart floors", "smart ceilings", "smart toilets", "smart elevators", "smart light switches", etc. However, a typical attribute of these "smart spaces" is that they were architected by someone other than the occupant. Thus the end user of the space often does not have a full disclosure of the operational characteristics of the sensory apparatus and the flow of intelligence data from the sensory apparatus.

In addition to the intellectual encryption described in the previous section, where manufacturers could make it difficult, or perhaps impossible for the end user to disassemble such sensory units in order to determine their actual

function, there is also the growth of hidden intelligence, in which the user may not even be aware of the sensory apparatus. For example, U.S. Pat. 4309781 (for a urinal flushing device) describes:

> . . . sensor . . . hidden from view and thus discourage tampering with the sensor . . . when the body moves away from the viewing area. . . . located such that an adult user of average height will not see it. . . . sensing means, will be behind other components. . . . positioned below the solenoid to allow light in and out. But the solenoid acts in the nature of a hood or canopy to shield the sensing means from the normal line of sight of most users . . . Thus most users will not be aware of the sensing means. This will aid in discouraging tampering with the sensing means. A possible alternate arrangement would be to place the sensing means below and behind the inlet pipe.

U.S. Pat. 4998673 describes a viewing window concealed inside the nozzle of a shower head, where a fiber optics system is disclosed as a means of making the sensor remote, concealment to prevent users from being aware of its presence. U.S. Pat.5199639 describes a more advanced system where the beam pattern of the nozzle is adapted to one or more characteristics of the user, while U.S. Pat. 3576277 discloses a similar system based on an array of sensing elements.

Means of creating viewing windows to observe the occupants of a space while, at the same time, making it difficult for the occupants to know if and when they are observed, are proposed in U.S. Pat. 4225881 and U.S. Pat. 5726706.

In addition to concealing the sensory apparatus, a goal of many visual observation systems is to serve the needs of the system architect rather than the occupants. For example, U.S. Pat. 5202666 discloses a system for monitoring employees within a restroom environment, in order to enforce hygiene (washing of hands after use of toilet).

Other forms of "intelligence", such as "intelligent highways" often have additional uses, beyond those purported by those installing the systems. For example, traffic monitoring cameras were used to round-up, detain, and execute peaceful protesters in China's Tiananmen Square.

U.S. Pat. 4614968 discloses a system where a video camera is used to detect smoke by virtue of the fact that smoke reduces the contrast of a fixed pattern opposite the video camera. However, the patent also notes that the camera can be also used for other functions such as visual surveillance of an area, since only one segment or line of the camera is needed for smoke detection. Again, the camera may thus be justified for one use, and additional uses, not disclosed to occupants of the space, may then evolve. U.S. Pat. 5061977 and 4924416 disclose the use of video cameras to monitor crowds and automatically control lighting, in response to the absorption of light by the crowds. While this form

of environmental intelligence is purportedly for the benefit of the occupants (to provide them with improved lighting), there are obvious other uses.

U.S. Pat. 5387768 discloses the use of visual inspection of users in and around an automated elevator. Again, these provide simple examples of environmental intelligence, in which there are other uses, such as security and surveillance. Although even those other uses (security and surveillance) are purportedly for the benefits of the occupants, and it is often even argued that concealing operational aspects of the system from the occupants is also for their benefit, it is an object of this paper to challenge these assumptions and to provide an alternate form of intelligence.

When the operational characteristics, function, data flow, and even the very existence of sensory apparatus is concealed from the end user, such as behind the grille of a smoke detector, environmental intelligence does not necessarily represent the best form of human–machine relationship for all concerned. Even when the sensors are visible, there must be the constant question as to whether or not the interests of the occupant are identical to those who control the intelligence-gathering infrastructure.

The need for personal space, free from monitoring, has also been recognized (Goffman, 1959) as essential to a healthy life. As more and more personal space is stolen from us, we may need to architect an alternative space of our own.

5.1. Solution to the Software Problem in Education

The first solution to these problems is a framework called Completely Open Source, Headers, Engineering, and Research (COSHER).

Before investing considerable time in learning how to use new software, and in developing works in that new software, which may then become "locked into" a particular file format, we ask ourselves a very simple question: Is the software in question COSHER?

What this means is that there has been no deliberate attempt at obfuscation of the underlying principles of operation of this software, or in preventing us from freely distributing the intellectual foundations upon which we might invest many years of our lives. Deliberate attempts at obfuscation include such practices as elimination of source code and stripping of executable task images.

By using COSHER software, we are making a statement that we prefer Computer Science over Computer Secrecy. Science supports the basic principles of peer review, and a continued development and advancement of software principles, and principles that we build on top of the software.

Moreover, the time we invest in both learning the software, as well as creating works in the software, will be less likely to go to waste if we have

a copy of the complete source code of the software. In this manner, should the software ever become discontinued or unsupported, we will be able to become our own software support group and migrate the software forward to new architectures as our old computers become obsolete. If it is COSHER, chances are we will be less likely to lose the many hours or many years we invest in producing works within the software.

Furthermore, if we make new discoveries that are built on a foundation of COSHER software, they are easier to distribute.

In science, it is important that others be able to reproduce our results. Imagine what it would be like if we had built our results on top of DOS 3.1. Others would have to either rewrite our software to exactly reproduce our results, or find an old version of DOS 3.1. Since this is proprietary software, we are not at liberty to freely distribute it with our research, but it is also no long available for purchase. However, if we had built our work on COSHER software, such as Linux 1.13, we can include a full distribution of Linux 1.3 in an archive, together with our results. Many years in the future, a scientist wishing to reproduce our results could then obtain a virtual machine (emulator for our specific architecture which will no doubt be obsolete by then) and install the COSHER operating system (Linux 1.13) that came with our archive, and then compile and run our programs.

5.2. Examples of COSHER Software

The Linux operating system is a good example of a COSHER operating system. GNU software is also COSHER. There are many COSHER software packages, including GIMP (Gnu Image Manipulation Program), and the Video Orbits software package, described in http://wearcam.org/orbits/index.html.

5.3. Solution to Environmental Intelligence Gathering

A proposed solution: HI for the re-configured self.

HI is a computational framework for individual personal empowerment. This framework is based on my “WearComp” invention—an apparatus for (embodiment of) realization of HI.

This framework involves the architecting of a new kind of personal space. An embodiment of the “WearComp” invention is an apparatus that is owned, operated, and controlled by the occupant of that space. In some sense, the apparatus of this invention is like a building, built for one occupant, and collapsed down around that one occupant. This computational framework for HI, called “WearComp”, and will now be described.

Figure 3. Evolution of the apparatus of the 'WearComp' invention from the 1970s to the present-day version built in ordinary-looking eyeglasses.

5.4. WearComp as a Basis for HI

I invented WearComp in Canada in the 1970s, as a photographic tool for the visual arts (Mann, 1997a), in particular, something I called "Mediated Reality" (altered perception of visual reality). The goal of Mediated Reality, unlike related concepts like virtual (or augmented) reality, was to reconfigure (augment, deliberately diminish, or otherwise alter) the perception of reality in order to attain a heightened sense of awareness of how ordinary everyday objects respond to light.

HI is a new form of HCI comprising a computer that is subsumed into the personal space of the user (e.g., the computer may be worn, hence the term "user" and "wearer" of the computer may be used interchangeably), controlled by the wearer, and has both operational and interactional constancy, e.g., is always on and always ready and accessible (Mann, 1997b).

The WearComp invention described in IEEE Computer, Vol. 30, No. 2: http://wearcomp.org/ieeecomputer.htm (an historical account was given in IEEE ISWC-97, Oct.'97, and is also online at: http://wearcomp.org/historical/index.html) forms the basis for HI. The evolution of the apparatus of this invention is depicted in Figure 3.

5.5. Definition of WearComp

A WearComp is a computer that is subsumed into the personal space of the user, controlled by the user, and has both operational and interactional constancy, i.e., is always on and always accessible.

Most notably, it is a device that is always with the user, and into which the user can always enter commands and execute a set of such entered commands, and in which the user can do so while walking around or doing other activities.

The most salient aspect of computers, in general, (whether wearable or not) is their *reconfigurability* and their *generality*, e.g., that their function can be made to vary widely, depending on the instructions provided for program execution.

With the WearComp, this is no exception, e.g., the WearComp is more than just a wristwatch or regular eyeglasses: It has the full functionality of a computer system but in addition to being a fully featured computer, it is also inextricably intertwined with the wearer.

This is what sets the WearComp apart from other wearable devices such as wristwatches, regular eyeglasses, wearable radios, etc. Unlike these other wearable devices that are not programmable (reconfigurable), the WearComp is as reconfigurable as the familiar desktop or mainframe computer.

The formal definition of wearable computing defined in terms of its three basic modes of operation and its six fundamental attributes is provided elsewhere in the literature (Mann, 1998).

5.6. WearComp as Universal Interface to Reality

Such a computational framework allows one to subsume all of the personal electronics devices that one might normally carry, such as:

- cellular phone;
- pager;
- wrist watch;
- heart monitor;
- camera;
- video camera

into a single device. Obviously, since it is a fully featured computer, it is possible to respond to e-mail, plan events on a calendar, type a report, or the like, while walking, standing in line at the bank, or the like. In this way WearComp anticipated the later arrival of the so-called "laptop computer", but has advantages over the laptop computer in the sense that it can be used while walking around doing other things. However, the real power of WearComp is in its ability to serve as a basis for Personal Imaging and HI.

5.7. Personal Safety Device: Cyborg Logs for Sousveillance

WearComp not only subsumes the function of the laptop computer, but goes beyond it.

Another area in which WearComp provides a truly new form of user-interface not found on laptop computers and PDAs is in its constancy of user-interface, and constancy of operation. This characteristic perhaps becomes most evident in its use as a personal safety/security camera. Imagine, perhaps as you walk down some quiet street late at night, an assailant wielding a sawn-off shotgun, demanding cash from you. You would not likely

have time or opportunity to pull out a camcorder to record the experience, but since the eyeglasses are worn constantly, you would have captured the experience.

5.8. Camera of the Future

Less extreme examples of WearComp as a new user-interface include the ability to construct a personal documentary video without conscious thought or effort. For example, in a fully-mediated reality, all light entering the eyes, in effect, passes through the computer, and may therefore be recorded (and possibly transmitted to remote locations). Wearable Wireless Webcam (Jones, 1995) was one example of a personal documentary video recorded using a reality mediator.

In the future, we may well have the capability to capture and recall our own personal experiences, and to have photo albums generated automatically for us. We will never miss baby's first steps, because we will have a retroactive record feature that lets us, for example, "begin recording from 5 minutes ago". Photo albums, in addition to being generated automatically, may also be exhibited while they are being generated. Rather than sending postcards to friends and relatives, or showing them an album after you come back from vacation, you may just put on your sunglasses and have the album sent to them automatically, as was done with the Wearable Wireless Webcam experiment in which video was transmitted, and still images were also automatically selected from the video.

5.9. Personal Intelligence Arms Race

While there will no doubt be more environmental intelligence than personal intelligence, there is at least the hope that there might be an end to the drastic imbalance between personal intelligence and environmental intelligence. The individual making a purchase in a department store may have several cameras pointing at him to make sure that if he removed merchandise without payment that there would be evidence that he did not pay for the item. However, in the future, he will have a means of collecting evidence that he did pay for the item, or a recorded statement of a clerk about the refund policy. More extreme examples, such as the case of Latasha Harlins[1] also come to mind.

In this sense, the camera-based reality-mediator becomes an equalizer much like the Colt45 in the Wild West. When there is a standoff, it does not matter whether one person has a big gun and the other has a small gun, so long as there is enough ammunition for mutually assured destruction.

In the WearCam case, it is simply a matter of mutually assured accountability.

6. BECOMING A PHOTOBORG

Among other things, the cyborg apparatus of the invention functions as a two-way Wearable Wireless Webcam, in which the wearer can allow others to see exactly what he or she is seeing, over the World Wide Web. Moreover, the wearer can also allow others to alter his or her perception of visual reality as a means of communication. While the traditional videophone shows us a picture of the user, Wearable Wireless Webcam shows us what the user is looking at. Within most social circles, such as among friends and relatives, we already know what the other people look like, so we do not need to see a picture of these people. Instead, it is far more meaningful for us to "become" these people, e.g., to put ourselves in their shoes and see the world from their point of view.

6.1. Eye Am a Camera

One outcome of the apparatus of the invention, is a photographic mindset. In effect, the eye itself becomes a camera, and, while sending everyday experiences to the World Wide Web, students can develop a cinematographic awareness. The students have the opportunity to wear the apparatus continuously, so that a photographic awareness develops over time, as opposed to the traditional notion of only looking through the camera viewfinder while shooting or preparing to shoot.

By giving students the ability to wear the devices over an extended time period, they are able to internalize the mapping from 3d to 2d and the laws of projective geometry.

Students each have the opportunity to make a movie, viewed in real time by their friends and relatives. In this way, without even being aware of the learning process, the students have learned far more about cinematography than if they had taken traditional "learn by doing" photo and film courses. By becoming a camera, the student truly learns what a camera is. The "learn by being" approach far surpasses the traditional "learn by doing" approach. The successful photoborg (photographic cyborg) learns to shoot high quality documentary video without conscious thought or effort. After time, the camera functions as a true extension of the mind and body.

7. EYETAP: TAPPING INTO THE MIND'S EYE

The tremendous success of this project, to date, suggests a next step in the evolution of the PhotoBorg. EyeTap technology is an apparatus that intercepts light passing through the center of projection of at least one eye of the wearer of the apparatus. The intercepted light is converted into a numerical

representation, modified by the computer, and then converted back into a light representation in the EyeTap device. The device causes the eye itself to, in effect, become the camera.

When the eye itself, in effect, functions as a camera, and the retina itself, in effect, functions as a display, there is a new possibility for a connected collective HI.

Although I have working prototypes of the EyeTap technology, in order to perfect the EyeTap system for manufacture, there still remain some issues, such as to miniaturize the apparatus so that it will fit entirely within ordinary eyeglasses, including the computational portion that is presently built into an undershirt so that it can be concealed under the wearer's outer shirt.

8. BREAKING THE BOUNDARY BETWEEN EDUCATION AND THE REST OF LIFE

I believe that one of the most enlightening discoveries arising from the "community of cyborgs" was that students took a personal interest in computing, once they had a "space" (mediated cyberspace) of their own. In particular, it appeared that when a student had a feeling of having his or her own computer, the usage of the computer entered into ordinary facets of day-to-day living, such as keeping in touch while walking around in normal life, or in applying computing to other endeavours, and in building new and interesting devices to connect to the computer that go beyond what is expected of the classroom or lab setting.

The difference between how the students regard these truly personal computers and how they might regard normal university computers is somewhat captured by the difference between ordinary clothing and prison uniforms. Where students had previously dutifully done their lab work, somewhat "dragging their feet", they now approached the subject with a passionate element of love of the subject matter, rather than duty to memorize the course material for the final exam. The "learn by being" approach meant that students assimilated the material into their ordinary day-to-day life. Exist Edbroke down the usual barrier between study and non-study, e.g., the artificial barrier that usually exists between "work" and "play" and the rest of life.

9. EXISTED WITHOUT BEING A CYBORG

At the nexus of research and teaching, we have found a new approach, originally developed as a "school for cyborgs" but immediately applicable to many facets of education that have nothing to do with body-borne (wearable or implantable) computing devices.

As an example, these methods were applied to my ECE385 course, *Introduction to microprocessors*. Firstly, this involved the use of low cost personal computers. In the deconist tradition, students were encouraged to find an old

computer in a dumpster, or to purchase an old computer for approximately $10 (or certainly not more than $100). Instead of using the expensive computers in the lab, which were chained down, bolted down, and hooked up to an alarm, the students then brought their own computers into the lab. These being of low (or zero) cost, the students were taught to overcome fear in opening the computers up and hacking the internals.

Because the systems were the students' own computers, and not University property, a certain existential element prevailed, as well. For example, the students would bring the computers home with them, and apply what they learned in class. And students often innovated, and created, in a true free-spirited fashion.

Thus ExistEd was successful in a variety of other venues, outside the cyborg arena. This method was also applied in the author's ECE431 course (Digital Signal Processing) and ECE496 course (Design). Results were very successful. Provided below are some student quotes from the official anonymous Course Evaluation forms:

10. CONCLUSION

Rather than conclude, I will attempt to also extrapolate into the future. Results are deconclusive, and thus meant to raise important questions about how we might drastically modify the way we teach, in order to teach the "stuff that matters to the student". In particular, by focusing on development of the student, as a human being, in the feedback loop of the learning process, we arrive at a new framework for teaching, in which the student takes personal interest in the subject matter, as it pertains to his or her own daily life. For example, sousveillance was presented as a form of action research (i.e., research that affects social change by conducting inquiry), that includes inverse surveillance. This led the students to create their own existential understanding equiveillance—the equilibrium between surveillance and sousveillance.

ENDNOTE

1. A customer falsely accused of shoplifting, and fatally shot in the back by a shopkeeper as she attempted to walk out of the shop.

REFERENCES

Brown, S. & Rose, J. (1996). Fpga and cpld architectures: a tutorial. *IEEE Design and Test of Computers* 13(2), see also http://wearcam.org/jayarpubs.html.

Cooperstock, J. & Buxton, B. (1995). Reactive room. Available at: http://www.dgp.utoronto.ca:80/people/rroom/rroom.html.

Cooperstock, J. R., Fels, S. S., Buxton, W., & Smith, K. C. (1997). Reactive environments: throwing away your keyboard and mouse. Available at: http://www.csl.sony.co.jp/person/jer/pub/cacm/cacm.html.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, New York: Doubleday.

Jones, S. P. (1995). Turning the tables on video surveillance. *Technical Report*. Boston, Massachusetts: The Boston Herald (Monday, June 12).

Mann, S. (1997a). An historical account of the 'WearComp' and 'WearCamp' projects developed for 'personal imaging'. *International Symposium on Wearable Computing.* Cambridge, Massachusetts, 66–73. (October 13–14) IEEE.

Mann, S. (1997b). Smart clothing: the wearable computer and wearcam. *Personal Technologies* 1(1), 21–27. (March 1997b).

Mann, S. (1998). Humanistic intelligence/humanistic computing: 'wearcomp' as a new framework for intelligent signal processing. *Proceedings of the IEEE* 86(11), 2123–2151+cover, (November 1998). Available at: http://wearcam.org/procieee.htm.

Mann, S. (with Hal Niedzviecki). (2001). *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*. Randomhouse (Doubleday), ISBN: 0-385-65825-7 (November 6).