The Witnessential Net *

Steve Mann, and Robert Guerra
Assistant Mailroom Clerk EXISTech Corporation
284 Bloor Street West, Suite 701, Toronto, Ontario, M5S 3B8
mann@eecg.toronto.edu http://existech.com/mailroom.htm

Abstract

The Witnessential Network for the protection of Human Rights workers, and others who may be subjected to violence, is achieved through a new kind of imaging and hierarchical architecture having special properties ideal for defense against unaccountability of attackers. Incidentalist video capture and self-demotion are introduced as new collegial forms of defense against unaccountability. Results of various experiments conducted worldwide over the past 20 years, on the inventing, designing, building, and using of wearable photographic apparatus having these special properties are also described. Other fundamental concepts with respect to a Personal Safety Device suitable for Human Rights workers are introduced.

Keywords Protection of human rights, Accountability, Self demotion, Self bureaucratization, Personal Imaging, Augmented Reality (AR), Mediated Reality, Human Rights, Witnessential Network.

1 Introduction: The need for Witnessential Computing

There have been previous attempts to equip Human Rights workers with hand-held cameras so that they can document violence, and many of these attempts have even been backed with massive corporate funding:

> We began when Amnesty International invited us to be the sole sponsor of Human Rights Now!, a 1988 world concert tour which reached millions of young people on five continents. ...In partnership with musician Peter Gabriel and the Lawyers Committee for Human Rights we founded Witness, a program that equips frontline activists with hand-held video cameras to document human rights abuses.

www.reebok.com/about_reebok/human_rights/home.html

Unfortunately, in many situations, the mere presence of a video camera results in immediate violence directed to a person with a camera. Thus hand-held cameras often serve to provoke rather than deter violence.

This violence directed at camera operators is almost globally universal, and can be observed in nearly any country. The author(s) have observed that when trying to use a camera to collect evidence of wrongdoing, that even otherwise mild mannered clerks will sometimes jump over a counter and punch a camera operator in the face, knocking the camera to the ground. Even in countries like Canada which is said to have a very good Human Rights record (Canada's first place standing in the UN Development Index [1]), camera operators have been physically assaulted and unlawfully detained for merely using a hand-held camera to collect evidence of wrongdoing. (See for example, some of the mpeg movies linked from http://wearcam.org/shootingback.html)

Additionally, the use of cameras can sometimes actually intensify violence that is already present, when the explicit use of cameras angers the authorities or other perpetrators of this violence.

1.1 Incidentalist image capture

Over the last 30 years, we had been developing wearable cybernetic personal imaging systems that overcame many of the limitations of the more recent approaches taken by organizations distributing hand-held video cameras to human rights workers, apparently unaware of our previous work.

For example, it was found that officials who reacted violenty to hand held cameras, did not seem to mind at all when being captured using an EyeTap device (wearable cybernetic personal imaging system) transmitting realtime video to the Internet. (See Fig 1.)

Some people have tried to explain this phenomenon by merely stating that the perpetrators did not know that the EyeTap device has camera-like properties, or even what the EyeTap device was.

Thus a series of experiments were conducted in

*Thanks to Xybernaut, Kodak, Digital Equipment Corporation (DEC), Compaq, Kopin, VALinux, CITO, NSERC, and Altera for assistance in this project.

(a) (b) (c) (d)

Figure 1: EyeTap systems have been successfully used to document actions of various corrupt customs officials, corrupt airline officials, as well as officials trying to hide their name tags or otherwise shirk responsibility or accountability. This kind of documentation would not have been possible with cameras.

which it was made very obvious that the EyeTap device was transmitting live video [2].

This was done by attaching a very large flat screen television to the body (http://wearcam.org/weartv.htm) and having it running a web browser, mirroring images from the website that's receiving the signals from the EyeTap device.

To make it even more obvious it was transmitting, a flashing red light, and flashing indicia bearing terms such as "REC." (the common abbreviation for "record" regardless of language), were included together with making the transmitting antenna more obvious, and having words like "LIVE BROADCAST" (in the appropriate language of the country where used) flash across the screen in large letters.

A freeze frame effect was also used, so that the otherwise would-be perpetrator could see his face on the television screen in larger-than-life size.

Moreover, in case would-be perpetrators might not have believed that the devices were actually capable of transmitting video, some experiments/performances were done with one person wearing a transmitting device, and another person receiving the images and browsing them on a wearable web browser to show to the subject of the experiment or performance.

For example, in some situations, the web browsers were shown to high level officials (such as the director of security) in an establishment where photography was strictly prohibited. When blatantly showing such officials pictures of themselves received on portable web browsers, it was, quite surprisingly, found that approximately 9 times out of 10, the officials did not object to having their pictures taken, even when it was explained to them that these pictures were being transmitted onto the Internet and backed up in several different countries around the world.

Additionally, various performances and experiments were conducted using devices having varying degrees of obviousness, and varying degrees of camera-like appearances, as shown in Fig 2.

These situations seldom resulted in violence, even though the image capture was made very obvious.

Although the results varied slightly from one country to another, there was enough consistency that the findings of these experiments/performances suggest that in addition to covert wearable image capture devices, that a more overt and obvious form of image capture device, as well as conspicuously concealed devices may be useful as a new form of civil disobedience. Such is the role of the international day of protest against video surveillance, World Subjectrights Day (http://wearcam.org/wsd.htm) held every December 24th.

When engaging in such acts of civil disobedience (or wearing the "maybecameras" of Fig. 2), it is preferable that large numbers of persons participate so that certain individuals are not singled out as victims of state-sponsored terrorism.

1.2 Can humans being clerks make clerks be human?

The inherent and fundamental assymetry that an individual encounters when reacting against (or documenting the autrocities of) a police state is the fact that the members of the police state assume the role of clerks who can say "we were just following orders" whereas the individual person acts (or is seen to act) of his or her own free will.

This situation is better understood with reference to figures depicting an individual interacting with a clerk.

Figure 3 illustrates an individual interacting with a clerk who either is, or pretends to be, under the control of a manager who either is, or pretends to be under the control of a chief executive officer, who either is, or pretends to be, under the control of a board of directors, etc..:

Not all of us regularly encounter systematic violence, such as torture or mass murder, in our daily lives. A more common kind of situation many of us might encounter, that illustrates the principle of Fig 3 is when a person tries to negotiate with a used car salesman, and the used car salesman might say something like "I'd love to give you the car for one thousand dollars; let me check with my manager". The used car salesman then disappears into a back room, has a coffee, and reads a newspaper for a few minutes, and then comes out and says "I'd love to give you the car for one thousand dollars but my manager won't let me.". Although the salesman never talked to a manager, the salesman has some degree of power over the customer by virtue of being able to credibly pretend that he is bound by a higher authority. A credible, articulable, higher and unquestionable authority allows representatives of or-

(a) (b) (c) (d)

Figure 2: Hundreds of different kinds of "maybecameras" were made as part of a twenty year long experiment in how persons react to being photographed without their permission. These devices were constructed in varying degrees of obviousness, some being more provocatively "conspicuously concealed" than others. Insights gained in these experiments formed the basis for the design of the Witnessential Computer. (a) Closeup of T-shirt with hidden netcam and computer sewn into fabric of shirt. Camera is conspicuously concealed behind smoked plexiglass, and text of shirt emphasizes the uncertainty afforded by the concpicuous concealment. (b,c) Wearable dome camera systems were used for more provocative versions of the conspicuous concealment. (d) Various wearable television displays made the images more evident. Here a person trying to make eye contact with the wearer of the device sees instead a reflection of themselves in the outward facing computer screen on the wearer's eyeglasses.
.

ganizations to obtain external blame and excuses for their otherwise irrational or disagreeable actions.

Unfortunately the individual person does not ordinarily enjoy the same luxury as the clerk, and must therefore behave more rationally, or risk seeming irrational, rude, or otherwise inappropriate. For example, if an individual carried a handheld video camera around videotaping clerks, casino operators, police officers, customs officials, and the like, the individual might be regarded as strange, rude, or otherwise acting in an inappropriate manner.

The individual could rely on religion, as a manager, by, for example, wearing a camera contraption as part of a religious order. Just as religion allows individuals to wrap their heads in various materials that would otherwise be regarded as inappropriate, a new religion such as the "personal safety religion" could be invented, that required its members to wear cameras.

Thus religion could form a similar purpose to the manager for the individual, but there is the danger that others (including clerks) may dismiss the individual as a religious fanatic. Therefore, what is needed is a similar way for the individual to have excuses for and to externalize blame for otherwise irrational or disagreeable actions. Alternatively, artistic freedom is useful in this regard. For example, the piece depicted in Fig 2(d) was worn in numerous places where photography was prohibited, as part of a week long internationally popular performance at Ars Electronica in September 1997 (http://wearcam.org/ars/index.html).

An important aspect of the Witnessential Network is for the individual to be able to nonconfrontationally inflict fear of accountability, uncertainty, or doubt on persons exerting physical or other coercive force, or the threat or possibility thereof, upon the user of the invention. This can be done by way of an incidentalist imaging *possibility*. In particular, a collegial form of disobedience to authority, in the form of what is, or appears to be, an incidentalist act, can be generated where an overtly certain act of disobedience would be forbidden.

Incidentalist imaging refers to imaging which can be made to seem as if it occurs merely by chance or without intention or calculation. An incidentalist imaging system may in fact blatantly capture images (as by an articulable requirement from a higher authority to do so), or it may present itself as a device that could capture images in a way in which it is difficult to discern the intentionality of the use of the invention.

In addition to incidentalism, another similarly desirable property for minimization of confrontation with would-be perpetrators is self-demotion: figure 4 illustrates the situation of a wearable computer user who is able to either be, or pretend to be, under the control of a Safety Management Organization (SMO). This figure shows an embodiment of the WearComp invention in which the INDIVIDUAL has a credible mechanism to externalize at least a portion of his or her image capture

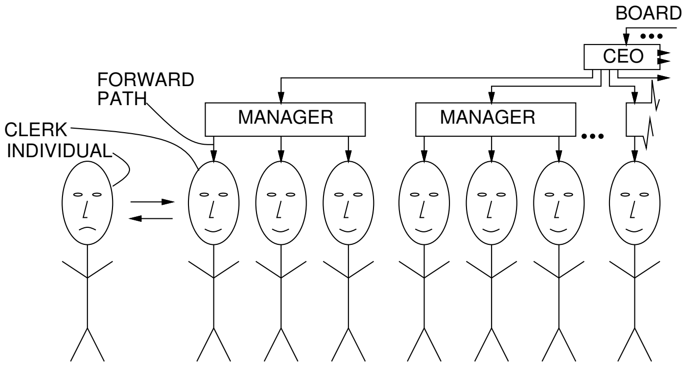


Figure 3: This figure is a diagram depicting an INDIVIDUAL versus a CLERK. The CLERK is bound by, or pretends to be bound by, conditions from a MANAGER. For example, the CLERK may be protected by a surveillance camera, or may be protected by a conspicuously covert container for a surveillance camera (such as a large plexiglass hemispherical dome of wine dark opacity). Alternatively, the CLERK may be protected by a blatentized covert surveillance potential, such as a blatently displayed television connected to a hidden camera. If the INDIVIDUAL complains about the surveillance, or about the potential for surveillance (e.g. by asking about plexiglass hemispherical domes of wine dark opacity within the establishment), the CLERK can either claim to not know what's in the domes, or can absolve himself or herself from responsibility for the situation by making reference to the MANAGER. The CLERK can either claim that the MANAGER installed the surveillance cameras, or authorized or required the installation of the cameras, or that the MANAGER decides whether or not images are captured from these domes. Alternatively the CLERK can completely deny knowing whether or not the domes actually contain cameras. Similarly, the MANAGER is bound by, or can pretend to be bound by conditions from a chief executive officer (CEO). The CE0 is bound by, or pretends to be bound by what the insurance company requires, or by a board of directors, denoted BOARD.

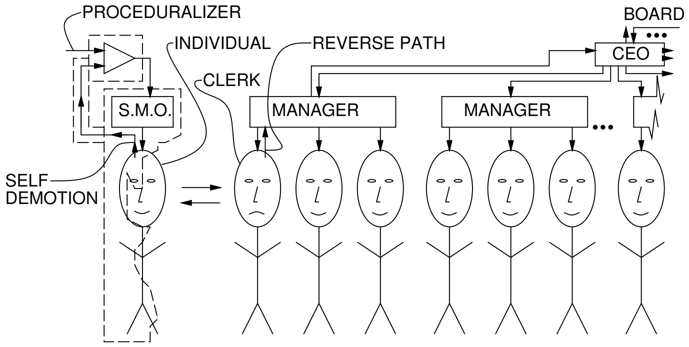


Figure 4: Witnessential Network versus the Police State. The Witnessential Network enables the individual to be empowered by self-demotion, in the same way that clerks in a Police State facilitate empowerment of large organizations. The self-demotion provides a deliberate self-inflicted dehumanization of the individual that forces the clerk to become human. In summary, humans being clerks can make clerks be human.

actions to a Safety Management Organization (SMO). The SMO provides an articulable basis upon which to deny free will or self determination. The SMO creates a management system, either real or perceived by others, that forces the CLERK out of the normal role, making necessary a true back channel (REVERSE PATH) from the CLERK to the MANAGER, which will often also require a true back channel to the CEO, etc..

Ordinarily there would be no such back channel, or the back channel would be reduced. For example, if an INDIVIDUAL complains about video surveillance systems in use by a CLERK, then the CLERK will simply refer the INDIVIDUAL to management, and management will be likely only available on certain limited hours, and after waiting extensively and being held up and delayed in line extensively. Then management will likely say the directive for use of surveillance comes from head office, and refer the INDIVIDUAL to a head office, where the INDIVIDUAL will spend several hours waiting on hold and calling various telephone numbers, etc.. The head office will then often say that the surveillance is used because the insurance company requires it.

However, if the INDIVIDUAL takes out his or her own personal handheld camera and photographs the CLERK, indicating that the SMO requires it, a very fast back channel (REVERSE PATH) will arise. Quite often the MANAGER of the CLERK will immediately become available, and the INDIVIDUAL will no longer have to wait in line or come back on a certain special day to talk to the manager. The matter will rapidly escalate to the highest available level of authority.

The Witnessential Network has a symmetrizing effect in which the individual and manager either snap out of their respective roles, or a back channel is forced, disrupting the normally one-way nature of the control flow from the top-down of management to the CLERK. Thus the INDIVIDUAL demoting themselves to CLERK forces the other CLERK to become an INDIVIDUAL accountable human and make responsible decisions outside the scope of just being a clerk.

In addition to an SMO, the INDIVIDUAL can also choose to be bound by (or to pretend to be bound by) an SMO that is itself bound by a higher authority such as an insurance company. Thus, in one embodiment, the INDIVIDUAL could, for example, take out a life insurance policy that required him to wear a personal safety device that recorded video at all times.

Thus the life insurance company provides the individual with a means for articulably externaizing his own irrational actions. Now the individual can say "I'm wearing this camera because my manager (SMO) requires it, and the insurance company requires the

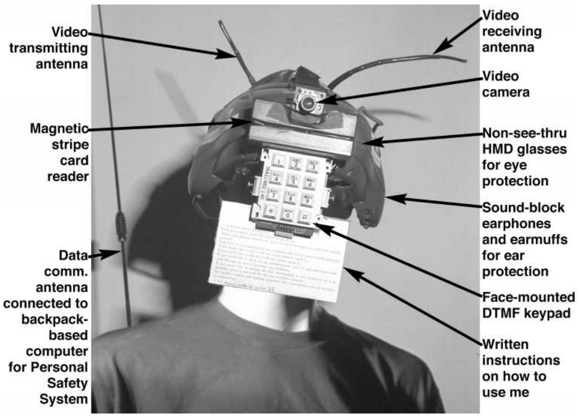


Figure 5: Extreme example of subservience empowerment used in the study entitled "Humans being clerks can make clerks be human". Clerks are invited to a proceduralized and self-corporatized human who has become a bureaucratized with a face-mounted telephone touch pad. The wearer of the apparatus communicates to clerks through a voice synthesizer, that says such messages as: "Your organization's time is very important to me, so PLEASE WAIT for my next available moment!" If you would like to try to sell me a new product, press 1; If you would like to ask me to fill out a form, press 2; If you would like to show me an advertisement, press 3, and slide your credit card through my slot to purchase my attention. For quality-control and training purposes, this conversation may be recorded or monitored. If you would like to inform me that photography is not permitted on your premises, press 9, and wait for my next available moment.

SMO to require me to wear it", etc..

Preferably, in the experimental apparatus, a PROCEDURALIZER is used to allow the individual to follow, or to appear to follow, a prescribed procedure without appearing to be thinking for himself or herself. The lack of apparent individual thought or intentionality, allows the individual to become or seem to become a clerk, which is what forces the CLERK to be human in being forced to think and make decisions for himself or herself.

An extreme example appears in Fig 5. Although this piece, entitled "Please Wait", was mainly a form of social commentary and satire, performances and experiments with this piece and many related pieces formed valuable insight into the formulation of the philosophical background for the Witnessential Network.

Moreover, self-demotion can occur internally without the need for an external manager. An example of such a system, as shown in Fig 2(b), uses heart ECG electrodes, respiration sensors, and the like, to control the video capture process. In this way, the wearer can deny having any control over the process. Images are only captured when heart rate or sweatiness index exceeds a certain threshold, compared to motion as sensed by the device.

If the wearer is being harassed by a prospective terrorist, the terrorist has only himself to blame for inducing the image capture by causing the wearer to be sweaty and her heart to beat more quickly.

2 Properties of the Witnessential Network

A series of experiments and performances conducted over a twenty year period from 1981 to 2001, building more than a hundred different kinds of wearable photographic apparatus, and wearing them in many different countries around the world, culminated in a conceptual framework for the Witnessential Network:

- The Witnessential Cyborg must be Incidentalist in the sense of being an embodiment of Incidentalist Video Capture;
- The Witnessential Cyborg must at least appear to be nonselective in what subject matter is captured, and for this reason, the Witnessential apparatus should be within the Corporeal Envelope (e.g. wearable or implantable), so that perpetrators of violence do not feel singled-out by the reportage;
- The Witnessential Cyborg must be "always ready" to remember incidents, e.g. the Witnessential apparatus must run all the time, even when it is not being "used" (e.g. it must be a successful embodiment of Humanistic Intelligence as described in http://hi.eecg.toronto.edu/hi.htm), the Retroactive Record feature being essential to document surprise abductions or violence by middle-of-the-night "no knock entry" thugs;
- The apparatus of the invention must be difficult to remove, a typical embodiment being attached securely on or inside the body, setting forth an equivalence class between torture and removal of the means for documenting torture, even within a holding compound or torture facility at a police station or obscure hideout (depending on the wearer's choice, either the apparatus only, or the combination of apparatus and wearer, would self-destruct on forced clothing removal);
- The Witnessential Cyborg must have the possibility to transmit live video, not just video that is recorded locally, whether the clothing is forcibly removed, or the wearer is murdered and the body is disposed of (e.g. transmission of video despite destruction of local memory of it);
- The Witnessential Cyborg should have the capability for self-demotion in order to have an articulable basis upon which to discount his or her

own freewill or personal interest in Human Rights (see http://wearcam.org/itti/index.htm for explanation of self-demotion), a corporate hierarchy being a preferred method of attaining self-demotion, the preferred Witnessential element being duty (e.g. "leave me alone, I'm just doing my job as a reporter") to conceal or negate any perceived passion or dedication to Human Rights;

- The Witnessential Network must be robust, and must not depend on any covernment (government+corporate) infrastructure (infrastructure that can be shut down by a government or corporation), although certainly some of the equipment can be donated by governments and corporations to the extent that we can verify it does not contain any hidden trojan horse-like "features";
- The Witnessential Cyborg must implement the Fear of Functionality (FoF) model (now described, in the next section).

Indeed, a lack of received picture signal could indicate non-observance of agreed-upon monitoring, and should therefore be considered at least equal to a violation of human rights. (Perhaps this concept could be written into the standard declaration of human rights, http://www.un.org/Overview/rights.html.)

2.1 Fear of Functionality

A direct result of Edgertonian sampling[3] is that a single picture from a picture sequence has a high degree of relevance and meaning even when it is taken in isolation.

Similarly, a direct result of Picture Transfer Protocol (PTP)[3] is that a single packet from a packet sequence has a high degree of relevance and meaning even when it is taken in isolation (for example when the packets before and after it have been corrupted).

It is therefore apparent that if a system were made serendipitous, even if doing so made the system highly unreliable, to the extent that pictures could only be transmitted occasionally, but really well unpredictably, then the Edgertonian sampling combined with PTP would provide a system that would degrade gracefully.

Indeed, if we were to randomly select just a few frames from one of Harold Edgerton's motion pictures, we would likely have a good summary of the motion picture, since any given frame would provide us with a sharp picture in which subject matter of interest could be clearly discerned. Likewise, if we were to randomly select a few packets from a stream of thousands of packets of PTP, we would have data that would provide a much more meaningful interpretation to the human observer than if all we had was randomly selected packets from an MPEG sequence.

Personal Imaging systems are characterized by a wearable incidentalist "always ready" mode of operation in which the system need not always be functioning to be of benefit. It is the *potential* functionality, rather than the actual functionality of such a system that makes it so different from other imaging systems like hand held cameras and the like.

Accordingly, an object of the Personal Imaging project is to provide a system that transmits pictures in harsh or hostile environments. One such application of such a system is the Personal Safety Device described in [4].

The Personal Safety Device differs from other wireless data transmission systems in the sense that it was designed for "Best Case" operation. Ordinarily, wireless transmissions are designed for worst case scenarios, such as might guarantee a certain minimum level of performance throughout a large metropolitan area. The Personal Safety Device, however, is designed to make it hard for an adversary to guarantee total non-performance.

It is common that state-sponsored terrorists use electronic devices to jam radiowaves, allegedly to prevent independent terrorists from activating explosives by radio remote control, or the like. Another effect, whether intended or not, is to adversely affect traditional personal safety devices such as cellular telephones. Therefore, a system is needed to potentially send the radio signals for personal safety and accountability.

Rather than traditional anti-jamming and frequency hopping technologies, the Witnessential Network makes use of serendipitous communications.

It is not a goal of the Personal Safety Device to guarantee connectivity in the presence of hostile jamming of the radio spectrum, but, rather, the goal is to make it difficult for the adversary to guarantee the absence of connectivity. Therefore, an otherwise potential perpetrator of a crime would never be able to be certain that the wearer's device was non–operational and would therefore need to be on his or her best behavior at all times.

Traditional surveillance networks, based on so–called "public safety" camera systems have been proposed to reduce the allegedly rising levels of crime. However, building such surveillance superhighways may do little to prevent, for example, crime by representatives of the surveillance state, or those who maintain the database of images. Human rights violations can continue, or even increase, in a police state of total state surveillance. The same can be true of owners of an establishment where surveillance systems are installed and maintained by these establishment owners. Examples such as the famous Latasha Harlins case in which a shopper, falsely accused of shoplifting by a shopkeeper, was shot dead by the shopkeeper [5]. Therefore what is needed is a Personal Safety Device, to function as a crime deterrent, particular with regards to crimes perpetrated by those further up the organizational hierarchy.

Since there is, and would be, the possibility of just one packet, which contains just one picture, providing incriminating evidence of wrongdoing, an individual can simply wear a personal safety device to obtain protection from criminals, assailants, and attackers, notwithstanding any alleged public or corporate video surveillance system already in place.

An important aspect of this paradigm is the Fear of Functionality (FoF) model. The balance is typically tipped in favour of the state or large organization, in the sense that state owned, or corporate owned surveillance cameras are typically mounted on fixed mount points, and networked by way of high bandwidth land lines. The Personal Safety Device (PSD), on the other hand, is connected by way of wireless encrypted [6] communication channels of limited bandwidth and limited reliability. For example, in the basement of a department store, the individual has a lesser chance of getting a good reliable data connection than the store–owned surveillance cameras. Just as many department stores use a mixture of fake nonfunctional cameras and real ones, so that the customer never knows whether or not a given camera is operational, what is needed is a similar means of best case video transmission. Not knowing whether or not one is being held accountable for one's actions, one must be on one's best behavior at all times. Thus a new philosophy, based on FoF, can become the basis of design for image compression, transmission, and representation.

Fig 6(a) illustrates an example of a comparison between two systems, SYSTEM "A", and SYSTEM "B". These systems are depicted as two plots, in a hypothetical parameter space. The parameter space could be time, position, or the like. For example, SYSTEM "A" might work acceptably (e.g. meet a certain guaranteed degree of functionality F_{GUAR}) everywhere at all times, whereas SYSTEM "B" might work really well sometimes, and poorly at other times. Much of engineering is motivated by an *articulability* model, e.g. that one can make an articulable basis for choosing SYSTEM "A" because it gives the higher Worst Case degree of functionality.

A new approach, however, reverses this argument, by regarding functionality as a bad thing — bad for the perpetrator of a crime — rather than a good thing. Thus we turn the whole graph on its head, and looking at the problem in this reversed light, come to a new solution, namely that SYSTEM "B" is better because there are times when it works really well.

Imagine, for example, a user in the sub basement of a building, inside an elevator. Suppose SYSTEM "A" would have no hope of connecting to the outside world. SYSTEM "B", however, through some strange quirk of luck, might actually work, but we don't know one way or the other, in advance.

The fact of the matter is, however, that one who was hoping that the system would not function, would be more afraid of SYSTEM "B", than SYSTEM "A", because it would take more effort to ensure that SYSTEM "B" would be nonfunctional.

The Fear of Functionality (FoF) model means that if there exists the possibility that the system might function part of the time, so that a would-be perpetrator of a crime against the wearer of the personal safety device must be on his or her best behavior at all times.

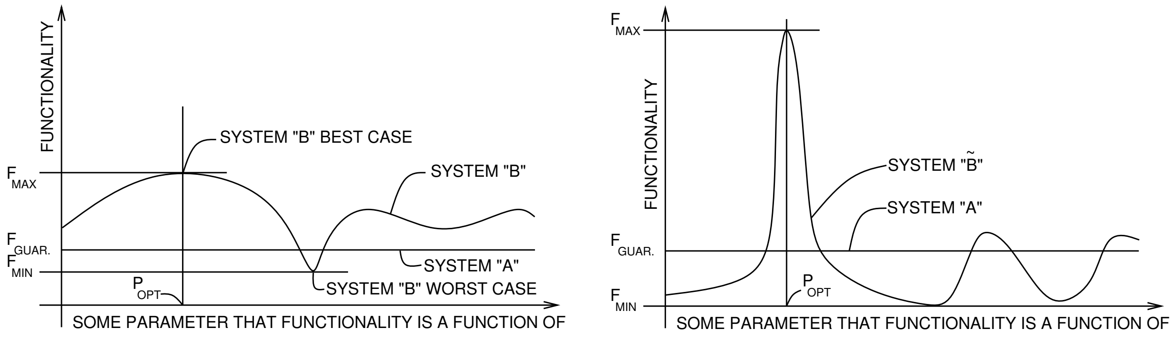
Fig 6(b) depicts what we might do to further improve the "fear factor" of our SYSTEM "B", to arrive at a new SYSTEM "$\tilde{B}$". The new SYSTEM "$\tilde{B}$" is characterized by making it even more idiosyncratic, such that the occasional time that SYSTEM "$\tilde{B}$" works, it works really well, but most of the time it doesn't work at all, or works very poorly.

Other technologies, such as the Internet, have been constructed to be robust enough to resist the hegemony of central authority. However, an important difference here is that the FoF paradigm is not suggesting the design of *robust* networks. Instead, **the FoF paradigm may suggest the opposite of robustness, in the sense that SYSTEM "$\tilde{B}$" is even more sensitive to mild perturbations in the parameter space about the optimal operating point, P_{OPT}, than SYSTEM "B".** In this sense, our preferred SYSTEM "$\tilde{B}$" is actually much less robust than SYSTEM "B". Clearly it is not robustness, in and of itself, that the author is proposing here.

The personal safety device need not work constantly, but, rather, must simply present criminals with the possibility that it could work sometimes, or even just occasionally. This scenario forms the basis for best-case design as an alternative to the usual worst-case design paradigm.

The Personal Imaging system therefore transmits video, but the design of the system is such that it will, at the very least, occasionally transmit a meaningful still image.

This rethinking extends from the transforms and compression approach right down to the physical hardware. For example, typically the wearer's jacket functions as a large low frequency antenna, providing trans-



(a) (b)

Figure 6: **Fear of Functionality (FoF)**: (a) Given two different systems, SYSTEM "A" having a guaranteed minimum level of functionality F_{GUAR} that exceeds that of SYSTEM "B", an articulable basis for selecting SYSTEM "A" can be made. Such an articulable basis might appeal to lawyers, insurance agents, and others who are in the business of guaranteeing easily defined articulable boundaries. However, a thesis of this paper is that SYSTEM "B" might be a better choice. Moreover, given that we are designing and building a system like SYSTEM "B", traditional Worst Case engineering would suggest focusing on the lowest point of functionality of SYSTEM "B". (b) Instead, it is proposed that one might focus one's efforts on the highest point of functionality of SYSTEM "B", to make it even higher, at the expense of further degrading the SYSTEM "B" WORST CASE, and even at the expense of decreasing the overall average performance. The new SYSTEM "$\tilde{B}$" is thus sharply serindipitous (e.g. peaked in its space of various system parameters. It is much harder for state-sponsored terrorists to guarantee that they can hide from accountability by jamming this system.

mission capability in a frequency band that is very hard to stop. For example, the 10 meter band is a good choice because of its unpredictable performance (owing to various "skip" phenomena, etc.). However, other frequencies are also used in parallel.

For example, a peer to peer form of infrared communication is also included, to "infect" other participants with the possibility of having received an image. In this way, it becomes nearly impossible for a police state to suppress the signal, because of the *possibility* that an image may have escaped an iron–fisted regime.

It is not necessary to have a large aggregate bandwidth to support an FoF network. In fact, quite the opposite.

Since it is not necessary that everyone transmit everything they see, at all times, very little bandwidth is needed. It is only necessary that anyone *could* transmit a picture at any time. This potential transmission (e.g. fear of transmission) need not even be to the Internet, e.g. it could simply be from one person to another to another person.

2.2 Verification of witnessential integrity

Cryptographic signatures are used to authenticate [7], time-stamp, and append heart rate, GPS, electronic compass info, etc., to the image header.

Additionally, a remote authentication committee certifies at least the time beyond which the images were produced, for example, that an image was sent within a sixtieth of a second after an event, so it can be thus assumed that it would have been very difficult to falsify an image within a sixtieth of a second.

In the very likely event of hostile jamming by well-equipped state-sponsored terrorists, images may be sent from one participant to the next, so that images still tend to spread locally among participants. Even if the image is passed to numerous participants, the original individual who captures the image signs it, thus granting a degree of credibility to the image and allowing the authentication committee to trust the authenticity of the image.

References

[1] S. Fukuda-Parr and R. Jolly, *Human Development Report 1997*. The Human Development Report Office, UN Development Program, 1997. www.undp.org/hdro ISBN 9211260817.

[2] S. Mann, "Can humans being clerks make clerks be human? *k onnen* menschen, die sich wie angestellte benehmen, angestellte zu menschlichem verhalten bewegen?," *Informationstechnik und Technische Informatik*, vol. 43, no. 2, pp. 97–106, 2001.

[3] S. Mann, "Comparametric transforms for transmitting eye tap video with picture transfer protocol (ptp)," in *Transform and Data Compression Handbook* (K. Rao and P. Yip, eds.), ch. 4, CRC, September 27, 2000. ISBN: 0849336929.

[4] S. Mann, "Smart clothing: The wearable computer and wearcam," *Personal Technologies*, pp. 21–27, March 1997. Volume 1, Issue 1.

[5] K. Umemoto, "Blacks and koreans in los angeles: The case of latasha harlins and soon ja du.," in *Blacks, Latinos, and Asians in Urban America: Status and Prospects for Politics and Activism.* (J. Jennings, ed.), Westport Conn.: Praeger, 1994. http://wearcam.org/latasha_harlins_reference.html.

[6] B. SCHNEIER, *APPLIED CRYPTOGRAPHY.* New York: WILEY, second ed., 1966. ISBN 0-471-12845-7.

[7] D. Chaum, "Achieving electronic privacy," *Scientific American*, pp. 96–101, 1992.