Veillance and Reciprocal Transparency: Surveillance versus Sousveillance, AR Glass, Lifeglogging, and Wearable Computing

Steve Mann
~~Surv~~VeillanCeNTRE^{TM}, 330 Dundas Street West, Toronto, Ontario, Canada, M5T 1G5

***Abstract*—This paper explores the interplay between surveillance cameras (cameras affixed to large-entities such as buildings) and sousveillance cameras (cameras affixed to small entities such as individual people), laying contextual groundwork for the social implications of Augmented/Augmediated Reality, Digital Eye Glass, and the wearable camera as a vision and visual memory aid in everyday life.**

We now live in a society in which we have both "the few watching the many" (surveillance), AND "the many watching the few" (sousveillance). Widespread sousveillance will cause a transition from our one-sided *surveillance society* back to a situation akin to olden times when the sheriff could see what everyone was doing *AND* everyone could see what the sheriff was doing. We name this neutral form of watching "*veillance*" — from the French word *"veiller"* which means "*to watch*". Veillance is a broad concept that includes both surveillance (oversight) and sousveillance (undersight), as well as dataveillance, uberveillance, etc..

It follows that: (1) sousveillance (undersight) is necessary to a healthy, fair, and balanced society whenever surveillance (oversight) is already being used; and (2) sousveillance has numerous moral, ethical, socioeconomic, humanistic/humanitarian, and practical justifications that will guarantee its widespread adoption, despite opposing sociopolitical forces.

I. Wearable Computing and Augmediated Reality

This paper addresses some of the "Technology and Society" issues [1], [2] related to wearable computing, AR (Augmented or Augmediated[1] Reality), the personal seeing aid (Digital Eye Glass), the VMP (visual memory prosthetic) [4], [5], and issues of transparency [6].

These issues are not only of interest to academics. The issues are also of practical, commercial, and industrial significance now that wearable camera products are being mass-produced, sold, and widely used in everyday life. Moreover Wearable Computing and AR has grown to a $200 billion industry at a time when more and more business establishments and similar places are installing surveillance cameras yet at the same time are prohibiting individuals from using their own cameras. See Fig 1. These "no camera" policies adversely affect those who use wearable cameras for AR, wayfinding, etc., as well as such systems as *described memories for the visually impaired* (e.g. recording one's life in order to get after-the-fact assistance or advice at the end of each day [7]), or transmitting live video for remote assistance with sight (e.g. the "Seeing-eye-People project [8]).

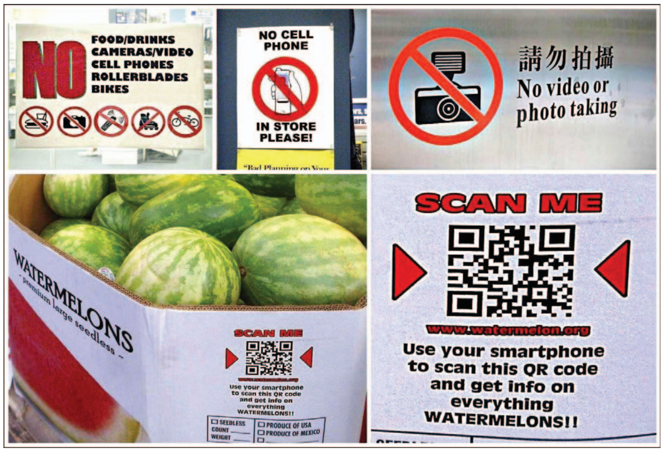


Fig. 1. Many business establishments prohibit cameras, e.g.: "**NO CELL PHONES**"; "**NO CAMERAS**"; "**NO CELL PHONE IN STORE PLEASE!**"; and "**No video or photo taking**", while at the same time requiring customers to bring and use cameras in order to read QR codes for pre-purchase product information. And while forbidding customers from having or using cameras, these establishments are installing their own cameras to keep their customers under **sur**veillance, creating a one-sided form of "veillance". Surveillance often embodies this hypocrisy — watching while forbidding others from watching. The *opposite (inverse) of hypocrisy is integrity*. Is there a veillance that is the opposite of surveillance — a veillance that embodies integrity rather than hypocrisy? **In this paper, we explore "sousveillance" (the opposite of surveillance) as a possible answer to that question.**

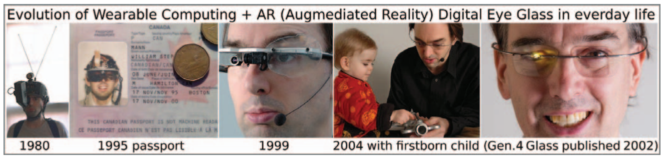

Evolution of Wearable Computing + AR (Augmediated Reality) Digital Eye Glass in everday life
1980
1995 passport
1999
2004 with firstborn child (Gen.4 Glass published 2002)

Fig. 2. Examples of the author's Digital Eye Glass and wearable computing [9] inventions used in everyday life over a more than 30-year time period. Digital Eye Glass causes the eye itself to, in effect, become both a camera and display [10], by way of the "Glass Eye Effect" [11] as originally developed in the MannGlas^{TM}computerized Augmediated Reality welding glass.

Wearable cameras and AR, when used in everyday life (see Fig 2) give rise to a new kind of "*veillance*" (watching) that is broader in scope than surveillance. To truly understand this new kind of veillance, and its surrounding social and intel-

[1] "Augmediated" is a portmanteau of "augmented" and "mediated". It refers to an ability not merely to *add* overlays (augment) but also to *subtract* (e.g. *deliberately diminish*) or *modify* reality. Examples include the MannGlass^{TM}/CYBORGlass^{TM}helmet fitted with a single piece of 4.5 by 5.25 Digital Welding Glass, through which both "EyeTapped" eyes look to see a *diminished* reality of the bright light of the arc and simultaneously an *augmented* reality of the darker areas of the scene, together with computerized overlays to annotate a workpiece being welded. [3] Specifically, an Augmediated Reality device has 3 elements: image sensing; image processing; and image display capabilities (i.e. it is a "wearcam", "wearcomp" and "weardisp").

978-1-4799-0929-2/13/$31.00 ©2013 IEEE

lectual landscape, we first need to understand **sur**veillance, which traditionally has been the more studied, applied, and well-known veillance.

II. Surveillance

Surveillance has recently emerged as a large commercial industry, sized at $22 billion in 2012 and estimated to grow to $26 billion in 2013, at an annual growth rate of 20.4% [12].

There are approximately 30 million commercial surveillance cameras in the United States, recording billions of hours weekly (Popular Mechanics magazine). Police and governments around the world are installing surveillance cameras throughout entire cities. Computer vision is also being used to bring video surveillance cameras into essential life and safety devices like automatic fire detection [13] (camera-based smoke detectors [14]), motion-detectors [14], and occupancy sensors for use in "classrooms, in private offices, and restrooms" [15]. These camera-based occupancy sensors "determine the number and positions of the occupants" for increased energy savings [16].

Just like there is a camera in most cellphones, soon there will be a camera in most light fixtures, including streetlights, for both occupancy sensing (see `http://www.lsgc.com/pixelview/`) and security (see `http://intellistreets.com/`):

> *"THOUSANDS of old-fashioned street lights in Merseyside are set to be dismantled and replaced with hi-tech CCTV-equipped lamps. The £32.7m scheme would see about 14,000 lampposts across Knowsley modernised ..."* —- Nick Coligan, Liverpool Echo, Nov 29 2007

Total surveillance has crept into most facets of our lives, including surveillance cameras in washrooms, changerooms, and locker rooms. A CBC news headline informs that Alberta's Privacy Commissioner is in favour of locker-room surveillance cameras: "Cameras can stay in Talisman's [athletic centre] locker room, says commissioner" (See `http://www.cbc.ca/news/canada/calgary/` `/story/2007/03/22/talisman-privacy.html`). And modern automatic flush toilets, faucets, and sensor-operated showers are starting to use more sophisticated camera-based computer-vision technologies (e.g. U.S. Patent 5828793).

A. Surveillance studies

Surveillance has also emerged as a field of study [17], [18]. For example, a "Surveillance Studies Centre" was created at Queen's University with a $2.5 million grant [19]. (see http://www.sscqueens.org/news/sp-receives-25-million-from-sshrc)

Numerous conferences and symposia are now dedicated to the topic of surveillance. For example, the IEEE, one of many different technical societies, offers the following surveillance-related conferences, symposia, and workshops each year:

- IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS);
- IEEE International Symposium on Monitoring & Surveillance Research (ISMSR);
- IEEE International Workshop on Socially Intelligent Surveillance and Monitoring (SISM);
- IEEE Workshop on Visual Surveillance;
- IEEE International Workshop on Performance Evaluation of Tracking and Surveillance,

and there are numerous other surveillance conferences, symposia, workshops, and the like.

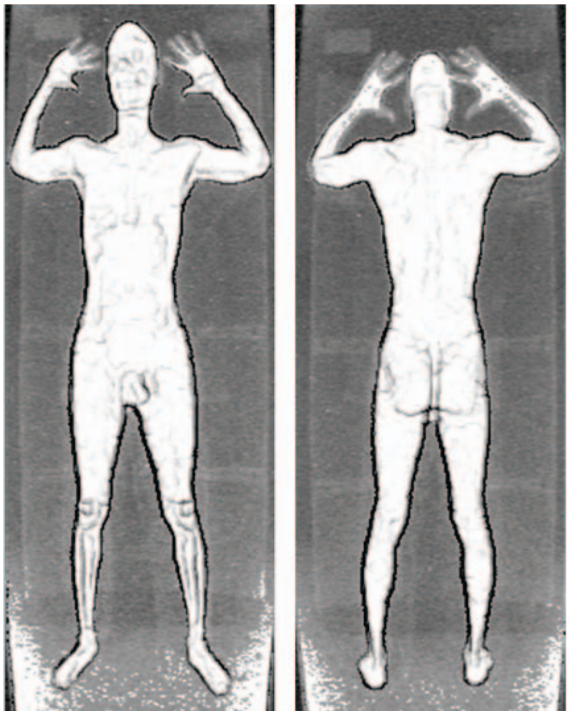


Fig. 3. The Transportation Security Administration (TSA) funds various studies and research into new surveillance technologies such as cameras and scanners that operate at higher frequencies of electromagnetic radiation than the visible light spectrum, in order to detect weapons by seeing through clothes. (public domain images obtained from Wikimedia Commons) Although the images in this early example are of poor quality, the technology is steadily being improved, and subsequent see-through-clothing camera models operate at much higher resolution. Some full-body scanners now provide enough detail to recognize and positively identify individuals [22].

B. Terrorism

Much of the practice, industry, and study of surveillance focuses on terrorism. For example, the US Department of Homeland Security, which was formed in response to the September 11 terrorist attacks [20], and the Transportation Security Administration (TSA), have funded studies and research on developing new technologies for surveillance, such as cameras and imaging systems that can see through clothing. [20] [21] See Fig 3. While promises have been made that these systems don't record images, it has been found that they often do record images, and recording capability was among the requirements of the TSA (http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf).

In some ways this parallels how every student was required to pose nude for pictures at certain Ivy League universities, so researchers could evaluate their physiques [23], [24]. Studies compared physical body shapes of Ivy League students with body shapes of prisoners, to understand the relationship between physique and the likelihood a person would commit

Fig. 4. France, approximately 200 years ago when and where the words “terrorism” and “surveillance” were first coined at the Reign of Terror [27], and Today, where surveillance cameras overlook residential streets (and people’s private balconies). Images from Wikimedia Commons.

crime-in-general [23], [24], although the focus was not specifically on contraband or terrorism.

Terrorism, in the modern sense, is defined as by Merriam-Webster, Dictionary.com and Wikipedia as:

> **ter·ror·ism** /’terə,rizəm/ *noun* **“The use of violence and intimidation in the pursuit of political aims.”**

The modern use of this word differs somewhat from the original use of the word. The words “surveillance” and “terrorism” both originated in the late 1700s and early 1800s from the “Terror in France” [25]. During this “Reign of Terror”, 41,594 people were executed, many merely for their political views or associations [26]. See Fig 4.

The word “Terrorism” comes from the French word “terrorisme”, referring specifically to state-terrorism in the form of violence practiced by the French government against its own people [28] [29] [30]. This “terrorism” was used as a “weapon for political repression in a time of ... civil upheaval” during the “Reign of Terror” (“la Terreur”) [28] [29].

The CoPS (Committee of Public Safety, French Comité de salut public), created by the French leglislative assembly in 1793, was the first “terrorist organization”. Its agents enforced the policies of the government’s “Reign of Terror” and the government employees of the CoPS were referred to as “Terrorists”. [28] [29] [26]

The word “terrorism” entered the English language by way of the London Times in January 30, 1795, and was first recorded in English-language dictionaries in the 1790s as meaning “systematic use of terror as a policy”, by a government against its own people, to, for example, suppress civil unrest. [28] [29] [26] [30] This original usage of the word is somewhat different from its modern meaning that includes acts perpetrated by individuals or by non-government organizations.

C. *Etymology and origin of the word “surveillance”*

The primary definition of the word **“surveillance”** is:

> **sur-veil-lance** [ser-vey-luh ns] *noun*
>
> 1) **“a watch kept over a person, group, etc., especially over a suspect, prisoner, or the like**: *The suspects were under police surveillance.*” [25]

The etymology of this word is from the French word “surveiller” which means “to watch over”. Specifically, the word “surveillance” is formed from two parts: (1) the French prefix “sur” which means “over” or “from above”, and (2) the French verb “veiller” which means “to watch”. The closest pure-English word is the word “oversight” [31], which emerged around the year 1300, and, in current English usage, has a similar, though broader and slightly different meaning than “surveillance”. “Oversight” can mean: (1) “an omission or error due to carelessness. *My bank statement is full of oversights.*” or (2) “supervision; watchful care: *a person responsible for the oversight of the organization.*” Google Translate returns the french word “surveillance” when presented with the English word “oversight”.

See Table 1. In particular, note the **difference between veillance and surveillance**.

English	French
to see	voir
to look (at)	regarder
to watch	**veiller**
watching (monitoring)	**veillance**
watching over (oversight)	**surveillance**
to oversee (to watch from above)	**surveiller**
over (from above)	**sur**
under (from below)	**sous**
“undersight” (to watch from below)	**sousveillance**

Table 1: Some English words and their French counterparts.

III. SOUSVEILLANCE

A more recently coined word is the word “sousveillance”, which is an etymologically correct opposite formed by replacing the prefix “sur”, (which means “over”, as in “surtitles” or “surcharge”) in “surveillance”, with its opposite, “sous” [32]–[35], which means “below,” “beneath,” or “under,” (as in “sous-chef”). See last 3 entries of Table 1.

A. *Hierarchical sur/sousveillance*

A literal interpretation of veillance (sur and sous) gives rise to the simple definitions [36] that embody a twentieth-century “*us versus them*” dichotomy:

- **Surveillance**: Observation or recording by an entity in a position of power or authority over the subject of the veillance. Examples: Police observing or recording the activities of citizens; shopkeepers watching over shoppers; a taxicab driver recording activities of passengers in the taxi;
- **Sousveillance**: Observation or recording by an entity **not** in a position of power or authority over the subject of the veillance. Examples: Citizens observing or recording activities from their own perspective, which includes the recording of the activities of police in the area (as well

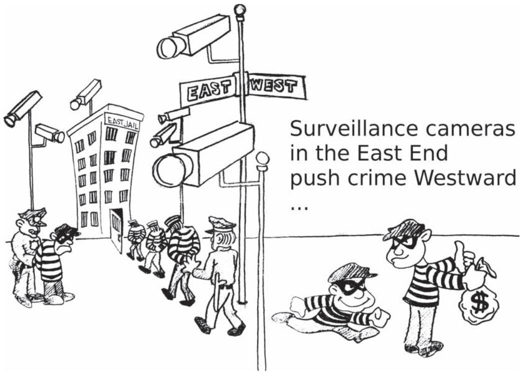


Fig. 5. Placing some members of society (e.g. those in the East End of town) under surveillance merely "pushes" crime elsewhere in the society.

as fellow citizens); Shoppers recording the activities in a shop (including those of the shopkeeper), etc..

These definitions address power relationships of the involved parties, as distinct from other sociological frameworks such as *ANT (actor-network theory)* [37]. Sousveillance is not anti-surveillance or counter-surveillance! A person can, for example, be in favour of both veillances, or opposed to both, or can favour one and not the other.

B. The Ladder Theory of Veillance and the Fruit Analogy

In a heirarchical civilization, people exist on different "rungs" of a sociopolitical or socioeconomic "ladder", from the chimney sweep at the "bottommost rung", to middle class shoppers, to the security guards and police, to the police chiefs, to the mayor, all the way up to congressional *oversight committees*, and the like.

In a surveillance society, security guards and police watch over the citizens, the police chief watches the police, and perhaps an oversight committee watches over the police chief. This raises the important questions:

1) "Who watches the watchers?";
2) "Who watches the watchers of the watchers?";
3) "Who watches the watchers of the watchers of the watchers?";

and so on ..., *to which an obvious answer is the democratic process of citizen "undersight" — the "swollag [7]" of democracy itself!*

In many modern cities, surveillance cameras are first installed in some areas of the city, which is said to "push crime" elsewhere. See Fig 5. Surveillance cameras do provide "situational crime prevention" [38], [39] (http://www.popcenter.org/), which contribute to some prevention and deterrence of crime, but other crimes merely move in response to the cameras.

Putting surveillance cameras throughout all areas of the city at "street-level", e.g. throughout shopping malls, underground parking garages, and city streets, does not completely extinguish crime. While it hinders low-level street crimes, surveillance may still allow, and in fact can actually cause, higher-level crimes, as follows: Street thugs may be caught and sent to jail, or otherwise slowed down, causing a shift in the market equilibrium. For example, the increased effectiveness of security guards and law enforcement officials may create a vacuum in the marketplace for stolen goods. The demand for stolen goods remains, but the reduced supply can drive up the price of the stolen goods. This increased price of stolen goods makes the criminal activity more lucrative, which may cause more Upward inhabitants to consider criminal activity.

C. Does surveillance turn pickpockets into politicians? ... The Fruit Analogy

We don't expect an uneducated "pickpocket" street criminal to suddently become a politician because of surveillance. More likely many such "pickpockets" and other street criminals will simply be arrested and imprisoned, and low-level crime will be reduced — opportunities in lower places will be extinguished or diminished by surveillance, while new opportunties in higher places will remain or even grow (examples where surveillance actually causes crimes).

The kinds of crimes caused or facilitated by surveillance require some degree of sophistication, cleverness, intelligence, or "specialized access" [40]–[42] to perpetrate, and are thus not the same types of crime perpetrated by less-educated street criminals. Specialized access often requires specialized skills.

Whereas much of the East-West migration of criminals illustrated by example in Fig 5 occurs through actual movement of criminals, the upward crime-shift occurs mostly through a form of "motion without movement" [43], analogous to the "light chasers" used on theatre marquees where motion (without movement) is generated by extinguishing a light source in one place while illuminating a light source elsewhere.

This upward crime-shift can be understood by way of the "Fruit Analogy". The Low-Hanging-Fruits (LHF) of crime are removed at street-level, driving up the price in stolen "fruit", thus creating new opportunities for crime in higher places, or insider-trading in stolen "fruit". And, since "ladders" are needed to reach the higher-hanging fruits, there exists: (1) an increased incentive for thieves to climb such ladders; (2) an increased incentive for those already further up these ladders to consider the possibility of stealing these higher fruits; and (3) the possibility of using the ladder itself as a tool for crime.

This third new possibility of using (or temptation to use) the surveillance cameras themselves for criminal purposes (e.g. security professionals or police stalking potential victims) could be more tempting to certain members of the security forces. For example:

> "A SECURITY guard at one of Edinburgh's best-known visitor attractions used CCTV cameras to stalk a young female worker and spy on the public.
> James Tuff used the camera system at Our Dynamic Earth, Edinburgh, to track his victim and then radio her with lewd comments.
>
> He even trained the cameras on members of the public milling about outside, in one case saving footage of two girls kissing to show to colleagues.
>
> Tuff eventually sexually assaulted Dora Alves ... He was fined and placed on the sex offenders register for three years. ... She said: "At first it was just the odd comment about my body; he would say things about me having a real woman's body ... But soon after he would appear out of nowhere when I was cleaning in the toilets. ..." as she walked to the canteen on her break and stopped to collect something from her locker. "Mr Tuff came out of his office

> and grabbed me from behind. ...” She said CCTV footage which could have proved the incident took place had gone missing.” [44]

Thousands of other examples — too numerous to enumerate here — have appeared in recent media, and the phenomena of surveillance-induced corruption is well-documented in the scholarly literature [45]–[47].

These cases raise two interesting issues: (1) the conflict-of-interest inherent in surveillance (e.g. CCTV footage mysteriously disappearing when under the control of authorities); and (2) the fact that the surveillance equipment facilitates or helps in the perpetration of many crimes, as well as the coverup (1) above. This is not to suggest that all security guards, police, politicians, priests, etc., are corrupt — most of them are good people. But they — apart from the screening and filtering process they undergo to enter their positions of power — are just like the rest of us — mere humans who are subject to the same temptations and character flaws that all of us have. For example, Roman Catholic priests have — despite the various checks and balances (screening and filtering processes, etc.) — used their high positions of power and their access to impressionable children to perpetrate crimes such as child abuse — while using their respected positions and church hierarchy to stifle scrutiny [48].

Moreover, the screening and filtering process for those in positions of authority is itself undermined in situations where there is a shortage of police. “In the Metropolitan Police, a shortage of applicants made it unnecessary to apply sophisticated selection techniques.” [49].

Thus there is no reason to assume that those in high places (e.g. priests, politicians, police, etc.) are flawless and should thus be able to watch over us without us being able to watch back! Otherwise, the one-sided nature of surveillance allows it to, under certain circumstances, become the very “ladder” that facilitates this high-level corruption. See Fig 6.

D. *Sousveillance (undersight) as a possible remedy*

In the context of the *Ladder Theory*, surveillance can lead to corruption, and absolute surveillance can lead to absolute corruption. Simply having oversight committees to oversee other oversight committees could result in an endless spiral of upwardly-mobile corruption. In this situation, sousveillance could function as a possible remedy to balance the otherwise one-sided nature of surveillance.

E. *Sousveillance to bring positive actions to light*

Sousveillance is not only about bringing wrongdoing to light. There are numerous examples of candid citizen sousveillance being used to catch police doing acts of good:

- Security Appreciation Week (http://wearcam.org/saw.htm);
- the heroic actions of Seargeant Mark Colombo of the Boston Police Department, against a drug-crazed car thief, http://www.youtube.com/watch?v=-SJakYMWnnY
- the kindness of New York Police Officer Larry DePrimo, who noticed a[n apparently] homeless man without shoes on a cold winter night. The officer bought shoes for the man, with money out of his own pocket, and, unbeknownst to the officer, the incident was photographed by a passing tourist. The picture was sent to NYPD headquarters and posted on Facebook.com and got more than 500,000 likes and 39,000 comments [51].

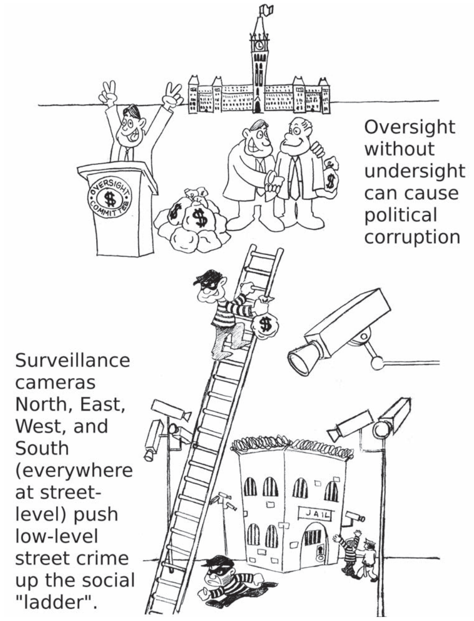

Oversight without undersight can cause political corruption
OVERSIGHT COMMITTEE
$
Surveillance cameras North, East, West, and South (everywhere at street-level) push low-level street crime up the social "ladder".
JAIL

Fig. 6. Children’s drawing (redrawn by artist M. Zandwyk) makes an oversimplification that is nevertheless illustrative. It suggests that *surveillance everywhere down at street level “pushes” crime up the “rungs” of the social ladder — so that it rises above the purview of the downward gaze of the cameras that watch from above.* In reality, surveillance is unlikely to cause an uneducated street criminal to rise to a position of power, the upward-shift in crime occurs instead due to shifts in market equilibrium [45]–[47] and other sociopolitical factors. Despite checks and balances, oversight without undersight can cause high-level political corruption that gives rise to an “upward” shift in crime, elevating low-level street crime to higher-level corruption. Ironically, the thief’s ladder is clearly visible to the surveillance cameras — as if to suggest that those in high places might be aware of — and continue to allow — crime and corruption that benefits them. Indeed, some criminals carry some of their proceeds “up” the “ladder” in the form of bribes, and the like [50].

These examples show how sousveillance and citizen undersight through social media can capture incidents — whether good or bad — and serve as a potentially less-biased and more neutral feedback mechanism than police-owned surveillance-only media.

F. *Participatory veillance*

In the past, the word “surveillance” primarily meant “the few watching the many”, as for example, described by Michel Foucault in his writings about Jeremy Bentham’s Panopticon [52]. Until recently surveillance was done by human observation: those “on top” watching those below, with their own eyes. But today, surveillance more commonly involves surveillance cameras, and in particular, a more modern definition of surveillance is the recording or observing of an activity by a non-participant in the activity [32], [34]–[36], [53].

Surveillance is the observation or recording of an activity by a person **not participating** in the activity. [32], [36], [53]

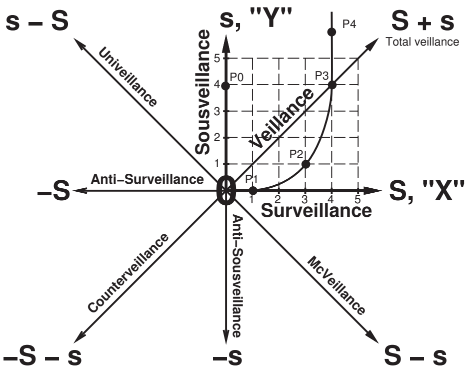


Fig. 7. The Veillance Plane and the "8-point compass" model of its directionalities: Surveillance and Sousveillance may be thought of as orthogonal vectors. The amount of sousveillance can be increased without necessarily decreasing the amount of surveillance. The amount of surveillance in a given space can be added *or* subtracted, and so can sousveillance, and both these veillances are additive (and subtractitive), giving rise to a vector space with infinitely many directions, 8 of which are noteworthy, and are thus illustrated here.

The Glosbe dictionary defines sousveillance using this more modern *participatory veillance* definition as:

> **Sousveillance** *noun*, "**The recording of an activity from the perspective of a participant in the activity**".

A more detailed definition of sousveillance, from primary reference sources, is as follows:

> **Sousveillance** means "**to watch from below**". The closest purely English word would be "**undersight**" [32], [33], [54], [55].
>
> Whereas, **surveillance generally refers to cameras affixed to property**, i.e. real-estate — either buildings (e.g. mounted to inside or outside walls or ceilings), or to land (e.g. mounted to lamp posts, poles, and the like), **Sousveillance generally refers to cameras borne by people**, e.g. hand-held cameras or wearable cameras [32], [34], [35].

Surveillance and sousveillance can vary independently. For example, consider a small business that has 4 surveillance cameras in it. If six customers each have their own cameras running, then we can think of this situation as a point at coordinates (4,6), i.e. at point labeled P4 in Fig 7.

Visual surveillance often stems from "surveillance cameras". The word "camera" is a Latin word that means "room". It is an abbreviation of the Latin phrase "camera obscura" which means "dark room", i.e. a chamber, vessel, or housing in which an image can be formed. The human eye, for example, is a camera, and the human mind and brain is its recording device. Since the beginning of human civilization some 10,000 years ago [56] (and even earlier if we consider pre-civilization and pre-human "veillance") until the relatively recent invention of the camera-obscura, the only cameras were biological eyes, and the only recording devices were biological brains.

Back in those days, a king, or emperor, or the sheriff of the Wild West could see what everybody was doing. But everybody could also see what the sheriff was doing.

Veillance worked both ways. While it was true that the king or emperor or sheriff had more power the observational component of that power was more approximately equal than it is today, with the proliferation of surveillance cameras that allow police and other powerful entities to watch citizens but prevent citizens from watching back.

Before approximately 50 years ago — and going back millions of years [56] — we have what we call the "sousveillance era" because the only veillance was sousveillance which was given by the body-borne camera formed by the eye, and the body-borne recording device comprising the mind and brain.

Suppose, for example, there were four people drinking whiskey in a saloon, back in the year 1800. Then let's say, for argument's sake that Sousveillance, denoted by lowercase "s" is four, and that Surveillance, denoted by uppercase "S" is zero. This corresponds to the point P_0 in Fig 7, at coordinates $(0, 4)$, given by $s = 4$ and $S = 0$, i.e. four units up the "Y" axis.

But within the last 50 years or so — the surveillance era — we've seen an unprecedented growth in surveillance cameras that record almost our every move. So strongly has surveillance video been as a record of evidence, that in many ways it trumps eye-witness accounts.

So let's suppose the year is now 1990, and the owner of the tavern installs one surveillance camera. Just this one surveillance camera can overpower the eyewitness accounts [57] of four people drinking whiskey, who, for example, were involved in a barroom brawl — assuming the camera has a good clear high-definition view of the four whiskey drinkers.

The surveillance camera is so powerful in a court-of-law, that it has, in many ways, surpassed eyewitness acounts [57]. Therefore adding the one surveillance camera to a tavern where four people are drinking does not move us to coordinates $(1, 4)$ with $S = 1$ and $S = 4$. Instead, a more accurate model is to say that it moves us to approximately $(1, 0)$ as indicated by point P_1 in Fig 7.

Now suppose in the year 2000, the owner of the tavern installs 2 more surveillance cameras, bringing the total to 3 surveillance cameras. And suppose at this time, one person in the tavern is wearing a camera making a lifelong video recording. This situation is illustrated as point P_2 in Fig. 7[2].

Now suppose the year is 2013, Today, and there are four surveillance cameras in the tavern where four people are also wearing cameras that are all recording. This situation is depicted as point P_3 in Fig. 7.

Now consider the year 2020, where, perhaps widespread adoption of Digital Eye Glass means that nearly everyone is wearing a camera of some kind. Thus if there are six people in the tavern, it might be likely that there are six sousveillance

[2] For simplicity, let the length of any vector be given by the L_1 norm, i.e. the total number of cameras (surveillance plus sousveillance), which is 4 in the case of P_2. As a further simplification, we are going to say that when no cameras are present, the amount of surveillance is zero and the amount of sousveillance is the number of eyewitnesses. When cameras are present, each surveillance camera moves us one point to the right on the "X" axis, and each sousveillance camera moves us one point up the "Y" axis.

recordings in addition to the four surveillance recordings, so as to position us at point P_4 in Fig. 7.

IV. Inequiveillance

When surveillance and sousveillance are treated equally, we say that there is "equiveillance" [58]. But not all situations afford equal favoritism to surveillance versus sousveillance.

In particular, there are two kinds of inequiveillance: Univeillance (one-party consent), and McVeillance (where a non-party records some or all parties while at the same time forbidding those parties from recording themselves). Univeillance favours sousveillance whereas McVeillance favours surveillance.

A. Univeillance

Consider the recording of telephone conversations. Surveillance refers to the recording (in this case, sound) of a telephone conversation by a non-participant party in the conversation. Sousveillance refers to the recording (of sound) by a participant in the activity (the telephone conversation) [32], [33], [54], [55].

In most countries, e.g. Canada, Denmark, Finland, and most of the United States (32 of the 50 states) one party of a conversation may legally record the conversation without notifying others. Only in a small number of countries and only in 12 of the 50 states, is one required to notify all parties of a recording. But in all states, a non-party may not legally record a telephone conversation except under very limited law enforcement exceptions. Thus sousveillance is more permissible than surveillance in most circumstances regarding the recording of audio.

B. McVeillance

More and more people are using cameras as seeing aids, whether to photograph a restaurant menu and magnify the text, or to use a smartphone with optical character recognition to translate foreign text to their own language, or to read 2d barcodes on products.

But owners and employees of many business establishments often assert rules or policies that dictate a kind of "sensory entitlement" over those entering their premeses.

For example, on July 1st, 2012, S. Mann was physically assaulted by three McDonalds employees because he was wearing a "Digital Eye Glass" computerized seeing aid.

A year ealier, Penny Sheldon, a travel agent from Boise, Id., was also physically assaulted by McDonalds staff in Paris, France, because she photographed their menu.

McDonalds has admitted to enforcing laws that don't even exist — laws that their own surveillance cameras would violate if they did exist! [http://wearcam.org/mcveillance]

"McVeillance" is not merely the mass-production of surveillance, but also its one-sided sight: watching everyone while forbidding them from watching back.

Here's a definition:

McVeillance is the **installation or using of surveillance cameras while simultaneously prohibiting people from having or using their own cameras**, hand-held magnifiers, smartphones, or the like.

More precisely, McVeillance is surveillance minus sousveillance, $S - s$, denoted on Fig 7.

As a personal visual memory prosthetic, or a seeing aid for AR, a camera for personal use (i.e. not distributing the images to others) should always be considered fair use.

But whether or not the reader agrees with this viewpoint, McVeillance can still be a useful construct with which to argue for or against this viewpoint.

C. Counterveillance

A number of technologies have been developed to detect and prevent veillance. For example, various research groups have created devices that detect and blind cameras [59]. These technologies also blind vision aids, assistive technologies, and the like, and may therefore be morally, ethically, and legally problematic.

These camera-blinding technologies could also be built in a body-wearable format to detect and neutralize surveillance cameras as well — perhaps as "spite fashion" / "spitewear" or just social commentary. Such counterveillance technologies, by their very nature, also use cameras. In this sense wearing or installing a camera detector is adding yet another camera to be detected by other camera detectors.

Because veillance has both morally positive and negative aspects, the moral imperative of counterveillance is therefore not morally right in itself.

V. The right to sensory integrity

A. Forbidden QR codes

Recall the group of pictures shown in Fig 1, on Page 1. It depicts establishments where McVeillance is in force, much to the detriment of the stated desire for customers to "User your smartphone to scan this QR code". Customers are **simultaneously required to use a camera, and forbidden from doing so**, in order to see this content. And customers are frequently harrassed by store security staff when all they're doing is trying to experience Augmediated Reality [32].

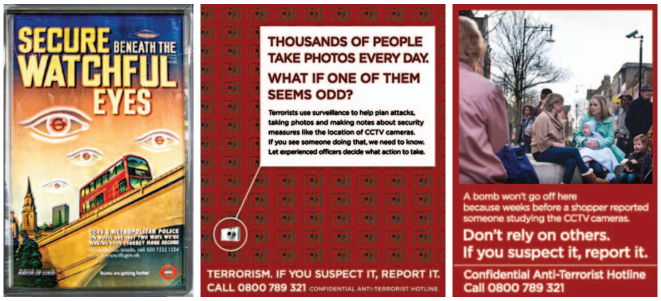
B. No Cameras!

Although there are no laws against taking photographs of private buildings from public spaces (e.g. public roads and sidewalks), there have been numerous cases of security guards harrassing photographers for doing so:

> *"... [A] simultaneous increase in state surveillance and the restriction of the right to take photographs in public ... monopolize the decision as to who constitutes the 'citizenry of photography', ... [and raise] questions about artistic and political responses to surveillance and photography restrictions"* [60]

When citizens point their cameras at the architects of the "surveillance superhighway", or simply when photographers take pictures of bridges, buildings, or surveillance cameras, they have often come under attack, especially as police have placed photographers under suspicion. See Fig 8.

This comes at a time when innocent suspects have been roughed up by police. Some have even been killed as a result of heightened suspicion and mistaken identity, e.g. Jean Charles de Menezes, a Brazilian electrician, was shot to death by police in a London subway. And police seized the CCTV


SECURE BENEATH THE WATCHFUL EYES
CCTV & METROPOLITAN POLICE ON BUSES ARE JUST TWO WAYS WE'RE MAKING YOUR JOURNEY MORE SECURE
Buses are getting better
MAYOR OF LONDON

THOUSANDS OF PEOPLE TAKE PHOTOS EVERY DAY. WHAT IF ONE OF THEM SEEMS ODD?

Terrorists use surveillance to help plan attacks, taking photos and making notes about security measures like the location of CCTV cameras. If you see someone doing that, we need to know. Let experienced officers decide what action to take.

TERRORISM. IF YOU SUSPECT IT, REPORT IT. CALL 0800 789 321 CONFIDENTIAL ANTI-TERRORIST HOTLINE

A bomb won't go off here because weeks before a shopper reported someone studying the CCTV cameras.

Don't rely on others. If you suspect it, report it.

Confidential Anti-Terrorist Hotline Call 0800 789 321

Fig. 8. Police advertising campaigns promote surveillance (leftmost), but also ask people to **report anyone "taking photos and making notes about security"** to the police. Thus a professor or student openly studying surveillance is likely to be harrassed, investigated, and possibly harmed by possibly overzealous security guards or police. (The text in the rightmost 2 images has been accessibilized/legibilized.)

recordings and claimed they were blank! Menezes was shot in a crowded subway car where lots of people could have recorded the incident. But police and security guards have made people afraid to record what they see. For example, NBC News and the Miami Herald reported that:

> *"On Memorial Day 2011, Narces Benoit witnessed and filmed a group of Miami police officers shooting and killing a suspect ... He was then confronted by officers who handcuffed him and smashed his cell phone, but Benoit was able to sneakily preserve the video ... he discreetly removed the [memory] card and placed it in his mouth."*

Some locations such as changerooms and movie theatres have emerged as particularly inaccessible to those using a computational visual and memory aid.

Accessibility requirements will force changerooms and washrooms to become "universal" (i.e. family-oriented with individual compartments). **Washrooms are a basic need that cannot be denied to those who happen to have computer chips on or in their bodies! But movie theatres will remain as the central locus of contention between the "cyborg" and his or her environment.**

The Criminal Code of Canada states:

> "(1) A person who, without the consent of the theatre manager, records in a movie theatre a performance of a cinematographic work within the meaning of section 2 of the Copyright Act or its soundtrack (a) is guilty of an indictable offence and liable to imprisonment..."

Interpreted most broadly, the human brain is a recording device, and remembering a portion of a "cinematographic work" is a criminal offence. But such a law is likely to be applied in a discriminatory way that criminalizes cyborgs as "existential contraband" (those who *are* cameras are, by their mere existence, contraband). As more people use electric eyeglasses, AR, lifelong video capture devices, lifegloggers, Personal Safety Devices, etc., a large percentage of the population could be criminalized for mere memory even if they never disseminated any of their memories!

Thus we can see a number of problems as the interests (some legitimate and some excessive) of copyright clash with the interests of personal use. A person with a vision aid that helps in remembering names and faces (by capturing pictures from real life or from a movie screen) should not be charged with a crime, and in fact the law is inconsistent with itself in this regard (e.g. the above Criminal Code is in violation of human rights laws against discrimination of persons with special needs).

C. Sensory entitlement principle

Being a master of one's own senses is a human-centred idea. We are each in control of our own ability to see, to hear, to touch a wall or a floor, with our feet, or with a cane to help us if we're blind. We're generally in control of our own eyeglass prescription, by way of choosing our eye specialists and choosing whether or not to wear eyeglasses (including, possibly, Digital Eye Glass). And people who can see quite well without eyeglass, are likely to start wearing it anyway, owing to other benefits like AR. This mass-production will help speed the development of digital eyeglass for those who really need it to see.

If a facility owner were to ask someone to remove their eyeglasses, it would be a much greater affront than merely asking someone to stop using a hand-held device. Because eyeglass affects how we see and understand the world, the demand to remove it is a much more onerous demand.

When another entity such as a business owner feels entitled to our senses, whether to dictate how we sense our world, or to prevent us from sensing it in a particular way, that entity must assume liability (for example if we trip and fall because the entity has demanded and forced upon us a different way of seeing than the way we would have otherwise chosen to see and understand the world).

An entity that prohibits eyeglass, a guide dog, or a cane, is not only in violation of human rights laws, but must also be held liable for any mishap that results from such prohibition.

VI. Reciprocal recording rights: The contract analogy

A recently proposed law to be placed before the New York Leglislature aims to prevent those conducting surveillance from prohibiting sousveillance [61]. Whereas there may exist certain places like changerooms where recording is not appropriate, it has been suggested that in any place where surveillance is used, that sousveillance must also be permitted.

The justification for such a reciprocal recording right can be understood by way of the "*contract analogy*" or the "*veillance contact analogy*": Imagine A and B enter into a written contract but that only A has a copy of the contract. If B chose to carelessly lose the copy of the contract, the contract is still valid. But if the reason B does not have a copy of the contract is that A prohibited B from having a copy, then the contract is not valid. The reason for this rule is to prevent falsification.

Let's suppose we have a 50 page contract A and B both agreed to, with their signatures on page 50. Later, A could go back and change page 49 (one of the non-signature pages). But if A and B both had copies, the copies would differ, and the courts would place higher scrutiny on the remaining parts, maybe examining the papers by microscope or other forensics to determine which copy was falsified.

By prohibiting these checks and balances (i.e. by prohibiting B from having a copy of the contract), A is creating a potential conflict-of-interest, and a possibility (maybe even an incentive) for falsification of the contract.

In today's world we live a social contract of the oral and action-based variety. Much of what we do is spoken or acted out, and not written. An an oral contract is still legally binding. So if one entity insists on having the only copy of what was said or agreed upon, A is creating the possibility to falsify (whether by editing or simply by omission, i.e. by deleting some pictures and keeping others) the recorded evidence.

Such a monopoly on sight can create "surveillance curation", i.e. the person doing the surveillance "curates reality" by selecting certain "exhibits" to keep, and others to delete.

In response to such a proposal, Paul Banwatt, a lawyer at Gilbert's LLP (personal communication by way of the *Veillance Group* on LinkedIN.com), has suggested that: *(1) Surveillance cannot be secret, or else individuals will be unable to tell when their right exists, or if one assumes the right is assumed to exist then; and (2) those who sousveil must be informed that they are NOT being recorded in order to form the necessary basis for a demand to stop sousveillance.*

A practical solution is to at least agree that when a person is prohibited from recording their own side of an interaction (i.e. their own senses), that the person who prohibited should have their side also removed from admissibility in any court of law.

Such a "veillance contract" does not require either party to know whether or not their actions are being recorded!

Under the proposed rule, an organization installing a "no photography" sign, or otherwise discouraging people from keeping their own copy of the "veillance contract", would make their own surveillance recordings inadmissible in a court of law.

A. Priveillance: The right to sensory/veillance privacy

Surveillance is often done in secret, through a network of hidden cameras. Cameras are often concealed in dark hemispherical domes so people cannot see which way they are "looking". Imagine if we all walked around wearing such domes so that people could not see which way we were looking. It is impolite to stare, but surveillance cameras have been granted the right or affordance to bypass such politeness.

Whereas "sight" has now been granted to inanimate objects like buildings and light posts, which are exempt from social rules, humans should at least have a right to their own senses, and a right to secrecy or privacy regarding their functionality (i.e. not having to disclose whether or not one is recording). A person using a vision aid, or visual memory aid, should not have to disclose the fact that they are differenlty abled. And a person recording an encounter with a robber or a (possibly corrupt) police officer should not need to disclose (and therefore risk violence) the nature of their senses.

Just as buildings keep secrets about their surveillance systems "for security reasons", people should be able to too! Thus a person should not need to prove that they are disabled before being "allowed" to use a camera. Likewise it would be absurd if one needed special permission to use a cane, or to wear eyeglasses, regardless of a lesser or greater need that may exist for these items. "Priveillance" can also mitigate privacy loss[3] with "videscrow" (visual key escrow).

VII. My Property, My rules!!!

A simple (though somewhat naive) form of sensory entitlement goes as follows: *This is my store [or mall or gas station, or city], and if you want to shop [or come] here you need to play by my rules, which means no cameras!.*

This propertarian model of veillance, in effect, defines surveillance as recording one's own property (e.g. a department store recording their own premeses, or a city's police force recording "their" streets), and sousveillance as recording someone else's property (e.g. a shopper or citizen recording the aisles of a store they don't own, or a street they don't own).

This model is problematic. (1) If property ownership were absolute, then it must also factor in the absolute ownership of one's own senses, sensory information, body, clothes, eyeglasses, and the like as personal property and personal space. In this sense there is an intersection of two different absolute properties, i.e. one absolute property inside another absolute property. And it can get even more complicated: **Consider entity A driving a car owned by entity B, parked in an auto mechanic shop owned by entity C, while witnessing a crime being perpetrated by entity D, in a city governed by entity E, in state F of country G, etc...** — A has a moral and ethical duty to witness and record the crime regardless of what B, C, D, E, etc... wish.

(2) Property ownership is actually not absolute. Human life is a more fundamental value than the property rights of another person. Therefore the most morally and ethically right thing for A to do is to secretly record the activities taking place, regardless of any rules set forth by B, C, D, etc.. And if property owners continue to enforce such absolutist rules, then manufacturers have a moral and ethical duty to favour human health and safety by making computerized vision aids and the like as covert as possible. Thus sousveillance is inevitible, either by becoming acceptable, or becoming covert (with strong moral and ethical justification) by design.

The boundaries of private property range from complete abolishment (e.g. certain forms of communism) to, at the other extreme, excesses that lead to a "tragedy of the anti-commons" effect of extreme underutilization of resources [62]. A full understanding of the boundaries of private property enters into such concepts as *nail houses*, *spite houses*, and *spite fences* [62], [63]. From these concepts the author also extrapolates/introduces the concept of *spite veillance* (both *spite surveillance* and *spite sousveillance*), as for example, the spite fence case of Gertz v. Estes, 879 N.E.2d 617 (Ind. App. 2008) involving also surveillance cameras installed merely to

[3] e.g. cyborglogs encrypted by key unknown to owner: prevents disclosure under police interrogation, e.g. owner can't be held held in contempt of court.

annoy a neighbour. But where does legitimate artistic social commentary, for example, play into this matter? Consider, for example, the legitimate use of sousveillance as a form of critical inquiry in public, semi-public, and private business establishments [64], [65].

Many issues regarding veillance relate to property, and defense of property[4].

VIII. Copyright, Copyleft, and Subjectright

Surveillance (mounting cameras on property like land and buildings) tends to favour property rights, as opposed to sousveillance (mounting cameras on people) which tends to favour human needs more directly. Another area where this property versus human favoritism is evident is in the domain of intellectual property, trade secrets, national security/secrecy, and copyright.

> "The purpose of copyright and related rights is twofold: to encourage a dynamic creative culture, while returning value to creators so that they can lead a dignified economic existence, and to provide widespread, affordable access to content for the public." – www.wipo.int/copyright/

It has been argued that commercial entities and powerful lobbying groups have subverted the public's interest through excessive restrictions on fair use [62], as well as through implementations of technologies that restrict fair use. For example, the technologies discussed in Section IV-C have been applied to detect and sabotage cameras in movie theatres, and as discussed, such technologies problematize fair use with regards to use of computerized vision aid.

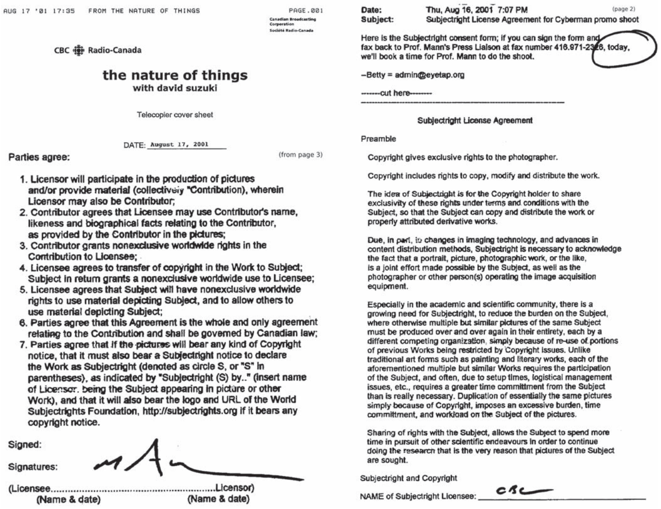
To understand copyright, consider a simple example of photographing a person. Consider the three entities:

1) the subject;
2) the photographer ("transmitient"); and
3) a recipient of the image (the person viewing the photograph).

Copyleft [66], if used, protects, to some degree, the recipient. Copyright laws protect the photographer, but adequate protection of the subject of the photograph is often absent. Some subject protection exists, e.g. in France or Quebec (Canada), "Le droit á l'image" (image rights) of the subject, but these rights are stripped away in many cases such as news reportage, or surveillance.

Recently the concept of Subjectrights (denoted by a circled "S" in contrast to the circled "C" of copyright) has been proposed for the protection of such "passive contributions". It is useful to consider Irving Goffman's distinction between that which we "give off" (passive contributions) and that which we "give" (active contributions). Copyright protects only the latter, and not the former. An example of a signed Subjectright agreement between a subject and a photographer with Canadian Broadcasting Corporation is shown in Fig 9.

Thus the veillance between (1) and (2) is asymmetric at best. Regarding the veillance between (2) and (3), this is also asymmetric. The recipient of the information has much less rights than the "transmitient" (sender/creator/author/photographer).



AUG 17 '01 17:35 FROM THE NATURE OF THINGS PAGE.001

Canadian Broadcasting Corporation
Société Radio-Canada

CBC Radio-Canada

the nature of things
with david suzuki

Telecopier cover sheet

DATE: August 17, 2001

Parties agree: (from page 3)

1. Licensor will participate in the production of pictures and/or provide material (collectively "Contribution), wherein Licensor may also be Contributor;
2. Contributor agrees that Licensee may use Contributor's name, likeness and biographical facts relating to the Contributor, as provided by the Contributor in the pictures;
3. Contributor grants nonexclusive worldwide rights in the Contribution to Licensee;
4. Licensee agrees to transfer of copyright in the Work to Subject; Subject in return grants a nonexclusive worldwide use to Licensee;
5. Licensee agrees that Subject will have nonexclusive worldwide rights to use material depicting Subject, and to allow others to use material depicting Subject;
6. Parties agree that this Agreement is the whole and only agreement relating to the Contribution and shall be governed by Canadian law;
7. Parties agree that if the pictures will bear any kind of Copyright notice, that it must also bear a Subjectright notice to declare the Work as Subjectright (denoted as circle S, or "S" in parentheses), as indicated by "Subjectright (S) by.." (insert name of Licensor, being the Subject appearing in picture or other Work), and that it will also bear the logo and URL of the World Subjectrights Foundation, http://subjectrights.org if it bears any copyright notice.

Signed:

Signatures:

(Licensee...Licensor)
(Name & date) (Name & date)

Date: Thu, Aug 16, 2001 7:07 PM (page 2)
Subject: Subjectright License Agreement for Cyberman promo shoot

Here is the Subjectright consent form; if you can sign the form and fax back to Prof. Mann's Press Liaison at fax number 416.971-2326, today, we'll book a time for Prof. Mann to do the shoot.

–Betty = admin@eyetap.org

-------cut here--------

Subjectright License Agreement

Preamble

Copyright gives exclusive rights to the photographer.

Copyright includes rights to copy, modify and distribute the work.

The idea of Subjectright is for the Copyright holder to share exclusivity of these rights under terms and conditions with the Subject, so that the Subject can copy and distribute the work or properly attributed derivative works.

Due, in part, to changes in imaging technology, and advances in content distribution methods, Subjectright is necessary to acknowledge the fact that a portrait, picture, photographic work, or the like, is a joint effort made possible by the Subject, as well as the photographer or other person(s) operating the image acquisition equipment.

Especially in the academic and scientific community, there is a growing need for Subjectright, to reduce the burden on the Subject, where otherwise multiple but similar pictures of the same Subject must be produced over and over again in their entirety, each by a different competing organization, simply because of re-use of portions of previous Works being restricted by Copyright issues. Unlike traditional art forms such as painting and literary works, each of the aforementioned multiple but similar Works requires the participation of the Subject, and often, due to setup times, logistical management issues, etc., requires a greater time committment from the Subject than is really necessary. Duplication of essentially the same pictures simply because of Copyright, imposes an excessive burden, time committment, and workload on the Subject of the pictures.

Sharing of rights with the Subject, allows the Subject to spend more time in pursuit of other scientific endeavours in order to continue doing the research that is the very reason that pictures of the Subject are sought.

Subjectright and Copyright

NAME of Subjectright Licensee: CBC

Fig. 9. Example of Subjectright (S) agreement, signed August 2001, by the Canadian Broadcasting Corporation in connection with a television broadcast and the 35mm motion picture film Cyberman. The agreement recognizes the passive contribution of the subject in a photograph, and the fact that the photographer and subject are collaborators.

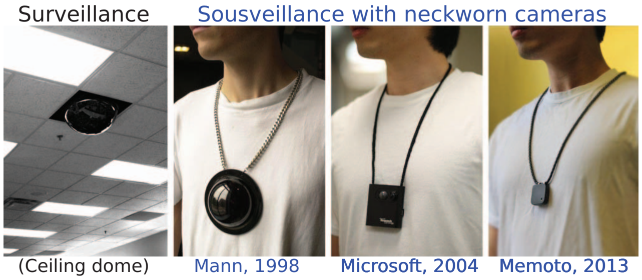


Fig. 10. Whereas Digital Eye Glass helps people see better, without *necessarily* recording video, the cameras shown above do the opposite: lifelong video recording without *necessarily* trying to help people see better. The 1998 sensor camera device originally took the form of a camera necklace that mimics the appearance typical surveillance domes, but being instead a fully functional Wearable Wireless Webcam for sousveillance, also known as lifeglogging (lifelong cyborglogging), lifelogging, moblogging (mobile logging), or the like. The 1998 system also featured built-in augmented reality and gesture recognition by way of a 3d laser-based projection system having infinite depth-of-focus [4], [67].

The word "copyright", if read literally, ought to mean "the right to copy". Copyright enforcement ought to mean the enforcement of the right to copy (e.g. enforcement of fair use access rights). These "fair use enforcements" ought to include access requirements for persons with special needs. Currently, due to copy protection mechanisms, copyright material is often inaccessible to persons with special needs. As copy protection can exclude such fair use, its moral imperative is immoral in and of itself. As we age, many of us will replace portions of our mind/brain with computer systems, giving rise to the Silicon Brain / Silicon Mind / Mind Mesh [4]. A person with Alzheimer's who has a silicon brain/mindmesh cannot be legally, ethically, or morally excluded from viewing copyrighted material, (e.g. a movie theatre). Additionally, more and more people will likely wear lifelong recording devices (Fig 10).

In this way it will be impossible, or at least morally, ethically, and legally troublesome, for a movie theatre owner or anyone else to prevent a movie from being "recorded" (remembered) for strictly personal usage. Accordingly, copyright

[4] Here "property" means both complex parts: $\mathbb{R}$P ($\mathbb{R}$eal Property, or $\mathbb{R}$eal Estate); and $\mathbb{I}$P ($\mathbb{I}$maginary Property, "Imagistate" or Intellectual Property).

restrictions already are (or will have to be) based on preventing dissemination, as mere acquisition for personal use must be considered fair use.

Similarly in matters of national or corporate security, once wearable and implantable computing becomes commonplace [4], we will have to learn to accept the "cyborg" being as a human being. It will all have to come down to mutual trust, and no longer the one-sided trust of the totalitarian or surveillance-only society.

Would it be right to prohibit artist Stephen Wiltshire from seeing a movie or deny him employment in a job interview because he has a photographic memory? Yes, there is a danger he could violate copyright or expose corporate or national secrets. But simply having a good memory should not be grounds for dissmissal or rejection. And whereas the courts already have redress for such violations of copyright or trade/national secrets, regardless of whether they were done with natural or computerized memory, assistive techologies and the good and prosperity that wearable computing will bring to society is inevitible. Moreover, perhaps the best way to prevent abuse of sousveillance (e.g. voyeurism, extortion, etc.) is more sousveillance. For example, extortion requires secrecy, such that a person trying to threaten an entity with revealing recorded secrets might actually be caught in the act by way of the very technology used to perpetrate the crime.

IX. The inevitibility of sousveillance: Universal needs rather than individual wants

Sousveillance is not merely a self-centered or narcissistic entitlement or human right/freedom. Rather, it meets universal human needs — wayfinding, personal safety, justice, and prosperity — in the service of all of humanity — even when only used by a small percentage of the people in a society.

Consider two parallel societies, a McVeillance/*Surveillance Society* [68] (where only surveillance is allowed), and a "Veillance Society" (where both veillances are allowed, and participatory veillance is encouraged).

The Veillance Society meets basic needs of human security [69] and personal safety — for everyone — not just the safety and security of property and merchandise, or of persons in high places ("sur"). In environments where surveillance cameras are already being used, i.e. where there is already a reduced expectation of privacy, sousveillance meets the needs of sight, personal safety, human security, and the like, and people enjoy a higher quality of life.

Whereas some individual shopkeepers and some police would be upset with such two-sided Veillance, the society as a whole will tend to be more balanced, just, prosperous, and "livable". Corrupt police, department stores with their fire exits illegally chained shut, and the like, will likely be revealed. And the society as a whole will enjoy greater information and knowledge about how the society works, and what is happening — from things as simple as "How do I find my way back to my car?" to more complex things like "Is that politician accepting a bribe from the Chief of Police?".

A new market economy in AR products and services will flourish. The Veillance Society will tend to enjoy greater prosperity and people will want to migrate from the McVeilance society to the Veillance Society, assuming they are free to migrate. If they are not free to do so (i.e. if they are held prisoner in the McVeillance society), then they will likely be less happy, less productive, and the McVeillance Society will not be able to escape the resulting decrease in prosperity.

X. Conclusion and Deconclusion

Sousveillance (e.g. wearable cameras and Digital Eye Glass) and surveillance must co-exist, giving rise to a "Veillance Society". This will bring an end to the *Suveillance Society* that began to emerge in recent history. *But will sousveillance be co-opted by centralized "cloud control"*[5]*? Will surveillance be rev-opted as "unterveillance"?* It is still too early to know — as an emerging field, much work remains to be done! That work needs to be in the field of "Veillance Studies" and praxis, and needs to encompass sur/sousveillance, Clarke's dataveillance, Michael's Uberveillance [70], [71], and all other veillances — hence the formation of the ~~Sur~~VeillanCeNTRE™.

Acknowledgment

The author wishes to acknowledge EPSON, NSERC, and AWE, as well as Mir Adnan Ali, Ryan Janzen, Raymond Lo, Colin Lam, Jonathan Polak, Om Bhatt, Han Wu, and Amber Chang for proof-reads and many hepful suggestions. Figures 5 and 6 arose from a collaboration of the author with his children Stephanie Mann (age 5) and Christina Mann (age 9), and Mike Zandwyk.

References

[1] K. D. Stephan, K. Michael, M. G. Michael, L. Jacob, and E. P. Anesta. Social implications of technology: The past, the present, and the future. *Proc. IEEE*, 100:1752–1781, May 13th, 2012. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06187687.

[2] Roger Clarke. Cyborg rights. In *Technology and Society (ISTAS), 2010 IEEE International Symposium on*, pages 9–22. IEEE, 2010.

[3] Chris Davies. Quantigraphic camera promises HDR eyesight from Father of AR, Sep 12 2012, www.slashgear.com/quantigraphic-camera-promises-hdr-eyesight-from-father-of-ar-12246941/.

[4] Steve Mann. Wearable computing. In Mads Soegaard and Rikke Friis Dam, editors, *Encyclopedia of Human-Computer Interaction*. The Interaction Design Foundation. Available online at http://www.interaction-design.org/encyclopedia/wearable_computing.html, 2012.

[5] J. Gemmell, L. Williams, K. Wood, R. Lueder, and G. Bell. Passive capture and ensuing issues for a personal lifetime store. In *Proceedings of the 1st ACM workshop on Continuous archival and retrieval of personal experiences*, pages 48–55. ACM, 2004.

[6] David Brin and Ben Goertzel. *David Brin on the Path to Positive Sousveillance*. H+ Magazine, May 23 2011, http://goo.gl/u5qm6.

[7] Steve Mann. *The Sousveillance Scenarios*. Presented to at: "Identity, Privacy & Security by ReDesign", Monday 2012 October 22nd, 4pm to 5:30pm, Room 728, Bissell building, 140 St. George Street, http://wearcam.org/sousnarios.htm Archived as PDF and further timestamped at: http://www.webcitation.org/6CbxqQU49.

[8] EyeTap Digital Eye Glass Laboratory. *Seeing Eye People*. 2001, http://eyetap.org/tpw/.

[9] Steve Mann. Wearable computing: A first step toward personal imaging. *IEEE Computer; http://wearcam.org/ieeecomputer.htm*, 30(2):25–32, Feb 1997.

[10] S. Mann. Through the glass, lightly. *IEEE Technology & Society*, 31(3):10–14, 2012; see also supplemental material in http://wearcam.org/glass.pdf.

[11] Steve Mann. Mediated reality with implementations for everyday life. *Presence Connect*, August 6 2002. wearcam.org/presenceconnect.

[12] Global Video Surveillance Market to reach US $37.7 billion by 2015, openPR, 3551 St-Charles Blvd., Suite 558, Kirkland, QC. 2012.

[5] Is it a joke if I say "GOOGlass brings Gooveillance to the Goolag"?

[13] C.B. Liu and N. Ahuja. Vision based fire detection. In *ICPR*, volume 4, pages 134–137. IEEE, 2004.

[14] *SigniFire Video Flame, Smoke and Intrusion Detection System*. http://www.fike.com/products/favideo.html.

[15] Texas Instruments. *Intelligent Occupancy Sensing*. http://www.ti.com/solution/intelligent_occupancy_sensing, 2012.

[16] Larry J. Brackney, Anthony R. Florita, Alex C. Swindler, Luigi Gentile Polese, and George A. Brunemann. Design and performance of an image processing occupancy sensor. In *Proceedings: The Second International Conference on Building Energy and Environment 2012987 Topic 10. Intelligent buildings and advanced control techniques*, 2012.

[17] G. T. Marx and G. W. Muschert. Personal information, borders, and the new surveillance studies. *Annu. Rev. Law Soc. Sci.*, 3:375–395, 2007.

[18] C. Norris, M. McCahill, and D. Wood. The growth of CCTV: A global perspective... *Surveillance & Society*, 2(2/3), 2002.

[19] D. Lyon. *Surveillance Studies An Overview*. Polity Press, 2007.

[20] Homeland operations. *Air Force Doctrine Document 2-10*, 21 Mar. 2006.

[21] G. Zentai. X-ray imaging for homeland security. *International Journal of Signal and Imaging Systems Engineering*, 3(1):13–20, 2010.

[22] Inc. SOURCE: Iscon Video Imaging. *New Iscon Whole Body Scanner Now Offers Integrated Biometric Capabilities to Detect All Objects and Verify Identities*. http://www.marketwire.com/press-release/new-iscon-whole-body-scanner-now-offers-integrated-biometric-capabilities-detect-all-1343909.htm, October 29, 2010.

[23] RON ROSENBAUM. The great ivy league nude posture photo scandal. *New York Times*, page 28, 1995 January 15.

[24] P. Vertinsky. Physique as destiny: William h. sheldon, barbara honeyman heath and the struggle for hegemony in the science of somatotyping. *Canadian Bulletin of Medical History/Bulletin canadien d'histoire de la médecine*, 24(1):291–316, 2007.

[25] Online etymology dictionary, douglas harper. 2010.

[26] Jean-Baptiste Clery. Journal of the Terror, Translation of Clery's Journal de ce qui s'est passé à la tour du Temple, and of Edgeworth de Firmont's Dernières heures de Louis XVI. Littlehampton Book Services Ltd; New edition edition, 1974, ISBN 0460041541.

[27] The main illustration from http://en.wikipedia.org/wiki/Reign_of_Terror, also avail. at La Guillotine en 1793 by H. Fleischmann (1908), p. 269.

[28] Donald Greer. *Incidence of the Terror During the French Revolution: A Statistical Interpretation*. Peter Smith Pub Inc., 1935.

[29] Dan Edelstein. *The Terror of Natural Right*. University of Chicago Press, 2009 ISBN 978-0-226-18438-8.

[30] Online etymology dictionary, douglas harper. 2001.

[31] Online etymology dictionary, douglas harper. 2010.

[32] S. Mann, J. Nolan, and B. Wellman. Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, 1(3):331–355, 2002.

[33] G. Fletcher, M. Griffiths, and M. Kutar. A day in the digital life: a preliminary sousveillance study. *SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1923629*, September 7, 2011.

[34] K. Michael and M. G. Michael. Sousveillance and point of view technologies in law enforcement: An overview. 2012.

[35] J. Bradwell and K. Michael. Security workshop brings' sousveillance'under the microscope. 2012.

[36] S. Mann. Sousveillance: inverse surveillance in multimedia imaging. In *Proceedings of the 12th annual ACM international conference on Multimedia*, pages 620–627. ACM, 2004.

[37] A.K. Martin, R.E. van Brakel, and D.J. Bernhard. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*, 6(3):213–232, 2009.

[38] Ronald Victor Gemuseus Clarke. *Situational crime prevention*. Criminal Justice Press, 1997.

[39] Derek B Cornish and Ronald V Clarke. Opportunities, precipitators and criminal decisions: A reply to wortley's critique of situational crime prevention. *Crime prevention studies*, 16:41–96, 2003.

[40] Marcus Felson and Rachel L Boba. *Crime and everyday life*. SAGE Publications, Incorporated, 2009.

[41] Marcus Felson. Routine activities and transnational crime. *International Crime and Justice*, pages 11–18, 2011.

[42] Janet P Near. Terry l. leap: Dishonest dollars: The dynamics of white-collar crime. *Administrative Science Quarterly*, 53(1):185–187, 2008.

[43] William T Freeman, Edward H Adelson, and David J Heeger. *Motion without movement*, volume 25. ACM, 1991.

[44] News Scotsman.com. Cleaner says she was stalked on cctv by security guard, March 2011.

[45] Stephen Irving Max Schwab. We're in it for the money: Tim shorrock: Spies for hire: The secret world of intelligence outsourcing, simon & schuster, new york, 2008, 439 p. *International Journal of Intelligence and CounterIntelligence*, 24(1):201–205, 2010.

[46] Peter Eigen. Corruption in a globalized world. *SAIS Review*, 22(1):45–59, 2002.

[47] Christopher P Wilson. *Cop knowledge: Police power and cultural narrative in twentieth-century America*. University of Chicago Press, 2000.

[48] Thomas P Doyle. Roman catholic clericalism, religious duress, and clergy sexual abuse. *Pastoral Psychology*, 51(3):189–231, 2003.

[49] Elizabeth Burbeck and Adrian Furnham. Personality and police selection: Trait differences in successful and non-successful applicants to the metropolitan police. *Personality and Individual Differences*, 5(3):257–263, 1984.

[50] Lawrence W Sherman. *Scandal and reform: Controlling police corruption*. Univ of California Press, 1978.

[51] Anthony M DeStefano. Larry deprimo, nypd cop, buys homeless man boots, Nov 29 2012.

[52] M. Foucault. *Discipline and Punish*. Pantheon books, New York, 1977. Translated from "Surveiller et punir".

[53] K. Dennis. Viewpoint: Keeping a close watch–the rise of self-surveillance and the threat of digital exposure. *The Sociological Review*, 56(3):347–357, 2008.

[54] C. Reynolds. Negative sousveillance. *First International Conference of the International Association for Computing and Philosophy (IACAP11)*, pages 306 – 309, July 4 - 6, 2011, Aarhus, Denmark.

[55] V. Bakir. *Sousveillance, media and strategic political communication: Iraq, USA, UK*. Continuum, 2010.

[56] P. Mellars and C. Stringer. *The human revolution: Behavioural and biological perspectives on the origins of modern humans*. Edinburgh University Press Edinburgh, UK:, 1989.

[57] J.S. Neuschatz, E.L. Preston, A.D. Burkett, M.P. Toglia, J.M. Lampinen, J.S. Neuschatz, A.H. Fairless, D.S. Lawson, R.A. Powers, and C.A. Goodsell. The effects of post-identification feedback and age on retrospective eyewitness memory. *Applied Cognitive Psychology*, 19(4):435–453, 2005.

[58] S. Mann, J. Fung, and R. Lo. Cyborglogging with camera phones: Steps toward equiveillance. In *Proceedings of the 14th annual ACM international conference on Multimedia*, pages 177–180. ACM, 2006.

[59] K. Truong, S. Patel, J. Summet, and G. Abowd. Preventing camera recording by designing a capture-resistant environment. *UbiComp 2005: Ubiquitous Computing*, pages 903–903, 2005.

[60] Daniel Palmer and Jessica Whyte. No credible photographic interest: Photography restrictions and surveillance in a time of terror. *Philosophy of Photography*, 1(2):177–195, 2010.

[61] Steve Mann and Pete Wassell. *Proposed law on sousveillance RESOLUTION: 000001 (MANN-WASSELL LAW)*. http://www.webcitation.org/6DGWgAmau, 2012.

[62] Michael A Heller. The boundaries of private property. *The Yale Law Journal*, 108(6):1163–1223, 1999.

[63] Richard Allen Epstein. *Takings: Private property and the power of eminent domain*. Harvard University Press, 1985.

[64] Steve Mann. Reflectionism and diffusionism. *Leonardo, http://wearcam.org/leonardo/index.htm*, 31(2):93–102, 1998.

[65] Steve Mann. Existential technology: Wearable computing is not the real issue! *Leonardo*, 36(1):19–25, 2003.

[66] P.B. De Laat. Copyright or copyleft?: An analysis of property regimes for software development. *Research Policy*, 34(10):1511–1532, 2005.

[67] Steve Mann. Telepointer: Hands-free completely self-contained wearable visual augmented reality without headwear... In *Proc. of the IEEE International Symposium on Wearable Computing 2000 (ISWC2000)*, pages 177–178, Oct 16-17, 2000. http://www.eyetap.org/docs/telepointer.pdf.

[68] D. Lyon. *Surveillance society*. Open University Press Buckingham, 2001.

[69] L. Axworthy. Human security and global governance: putting people first. *Global governance*, 7:19, 2001.

[70] Michael G Michael and Katina Michael. Toward a State of Überveillance. *IEEE Technology and Society*, 29(2):9–16, 2010.

[71] K. Michael, A. McNamee, MG Michael, and H. Tootell. Location-based intelligence-modeling behavior in humans using GPS. pages 1–8. IEEE ISTAS, 2006.