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

Steve Mann

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, humanitarian, and practical justifications that will guarantee its widespread adoption, despite opposing sociopolitical forces.

I. WEARABLE COMPUTING AND AUGMENTED REALITY

This paper addresses some of the “Technology and Society” issues [1], [2] related to wearable computing, AR (Augmented or Augmediated1 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]).

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™/CYBORGlass™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”).
lectual landscape, we first need to understand surveillance, which traditionally has been the more studied, applied, and well-known veil.

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, change rooms, 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.sssqueens.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.

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...
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:

**terrorism** /'terər-izəm/ 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 legislative 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:

**surveillance** [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.

<table>
<thead>
<tr>
<th>English</th>
<th>French</th>
</tr>
</thead>
<tbody>
<tr>
<td>to see</td>
<td>voir</td>
</tr>
<tr>
<td>to look (at)</td>
<td>regarder</td>
</tr>
<tr>
<td>to watch</td>
<td>veiller</td>
</tr>
<tr>
<td>watching (monitoring)</td>
<td>veillance</td>
</tr>
<tr>
<td>watching over (oversight)</td>
<td>surveillance</td>
</tr>
<tr>
<td>to oversee (to watch from above)</td>
<td>surveiller</td>
</tr>
<tr>
<td>over (from above)</td>
<td>sur</td>
</tr>
<tr>
<td>under (from below)</td>
<td>sous</td>
</tr>
<tr>
<td>“undersight” (to watch from below)</td>
<td>sousveillance</td>
</tr>
</tbody>
</table>

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 “subtitles” 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
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 hierarchical 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?”;

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 suddenly 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 opportunities 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=5jaxyRfWw5Y
- 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]. 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]
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 P0 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 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 accounts [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 P1 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 P2 in Fig. 7.

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 P3 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...
recordings in addition to the four surveillance recordings, so as to position us at point $P_1$ 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 premises.

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 earlier, 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” / “spitwear” 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 “Use 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 Augmented 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...
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 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, lifeloggers, 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 Legislature 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.

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 differently 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.

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
This page contains a discussion on copyright law and its implications on surveillance, reporting, and privacy. It highlights the asymmetric nature of copyright, where the rights of the subject (photograph) are often absent, whereas the rights of the photographer (transmitent) are protected by copyright laws. The text mentions the concept of Subjectrights, which is a proposed solution to balance the protection of passive contributions of the subject with the rights of the transmitter, aiming to create a more equitable copyright framework.

The text also refers to sousveillance (mounting cameras on property like land and buildings) and discusses its implications on property versus human favoritism. It notes that sousveillance tends to favor property rights, while intellectual property, trade secrets, national security/secretty, and privacy are discussed as critical inquiry domains in public, semi-public, and private business settings.

The text mentions the importance of copyright and related rights, such as the right to copy, and the debate around these rights and their enforcement in various contexts. It touches on the Legality of Artistic Social Commentary, play, and the implications of sousveillance as a form of surveillance directed towards people.

The text also discusses the protection of intellectual property rights and the role of copyright in relation to fair use. It mentions the example of the Three Entities: 1) the subject, 2) the photographer (transmitent), and 3) a recipient of the image (the person viewing the photograph).

Additionally, the text references the idea of a Lifelogging system as a form of surveillance that mimics the appearance of typical surveillance domes but is instead a full-functional Wearable Wireless Webcam for sousveillance, also known as lifelogging (lifelong cyborglogging), lifelogging, moblogging (mobile logging), or the like. The 1998 system featured built-in augmented reality and gesture recognition by way of a 3d laser-based projection system having infinite depth-of-focus.

It is noted that while the right to copy (e.g., enforcement of fair use access rights) is essential, there are also concerns about the moral and ethical implications of various uses of technology, including surveillance and reporting. The text concludes with a reminder of the importance of balancing individual rights with the needs of society and the environment.
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 dismissal 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 technologies and the good and prosperity that wearable computing will bring to society is inevitable. 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 INEVITABILITY 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 McVeillance 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 Surveillance Society that began to emerge in recent history. But will sousveillance be co-opted by centralized “cloud control”? Will surveillance be rev-opted as “intervveillance”? 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 Ubervveillance [70], [71], and all other veillances — hence the formation of the Surveillance Centre.

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 helpful 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


5Is it a joke if I say “GOOGlass brings Gooveillance to the Goolag”?
The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for sousveillance

Mir Adnan Ali and Steve Mann
Department of Electrical and Computer Engineering
University of Toronto, 10 Kings College Rd, Toronto, ON, CANADA

Abstract—Surveillance is a French word that means “to watch from above” (e.g. guards watching prisoners, police watching citizens, etc.). Another form of veillance (watching) is sousveillance, which means “to watch from below”. Whereas surveillance often means cameras on large entities (e.g. buildings and land), sousveillance often means cameras on small entities (e.g. individual people). The importance of sousveillance has come to the forefront recently with advancements in wearable computing and AR (augmented or augmented reality).

We characterize sousveillance from both an economic and moral perspective. We argue that societies that reject sousveillance will be impoverished, relative to those accepting sousveillance. We further argue that sousveillance as a form of social action has positive survival characteristics, so that in the long run, assuming that social and technological trends continue, the widespread adoption of sousveillance is inevitable.

I. I NTRODUCTION

A. Surveillance

The primary definition of the word “surveillance” is:

• “a watch kept over a person, group, etc., especially over a suspect, prisoner, or the like: The suspects were under police surveillance.” [1]

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 English word is “oversight”, although the latter has two meanings: (1) watching from above, as in “oversight committee” and (2) an omission or error, as in “that was an oversight on our part”. Because the French word gives less ambiguity and flexibility “veillance” will serve as the root of a set of categories.

B. Sousveillance: Putting cameras on people

A more recently coined word is the word “sousveillance”, which is an etymologically correct opposite formed by replacing the prefix “sur”, in “surveillance”, with its opposite, “sous” [2], [3], [4], [5].

Sousveillance is typified by cameras borne by people, e.g. hand-held or wearable cameras controlled by the wearer, and not worn on behalf of another party [6], [7].

C. Specific definition of surveillance and sousveillance in the context of this work

In the present analysis, we select a particular meaning to focus on the social, and consequently informational, asymmetries of parties involved in veillance. As adjectives, these words are indicative of the properties of the object they describe. However, the use of the adjective does not imply that the object so described can only be used to accomplish the action indicated by the verbal form – in other words, a “surveillance camera” can be used for sousveillance, and vice versa. The meaning of interest here is the verbal form, where veillance is conscious action.

While commonly used to refer literally to visual signals, the meaning of surveillance and sousveillance have been generalized from vision to other sensory signals such as sounds, and observational data in general. For the purposes of this work, we specifyize our definition to exclude non-artifact producing veillance; that is, direct observation without transmission (i.e. translation in time or space) is not considered veillance in this paper. Therefore, the definitions used here are:

surveillance v. Monitoring undertaken by an entity in a position of authority, with respect to the intended subject of the veillance, that is transmitted, recorded, or creates an artifact.

sousveillance v. Monitoring undertaken by an entity not in a position of authority, with respect to the intended subject of the veillance, that is transmitted, recorded, or creates an artifact.

In these definitions, an entity having a position of authority means that the possessor of that authority has both ability and legitimacy, in a normative sense [8], to enforce their will. The definitions used here are concerned with the intentions and purposeful actions of the parties involved in veillance, as distinguished from other sociological frameworks such as actor-network theory or ANT [9], where inanimate objects are considered actors in their own right. There is no logically consistent way to ascribe legitimacy, intentions, or desires to inanimate objects, nor are we concerned with situational outcomes from the perspective of machines.

D. Model of Analysis

The model of analysis we use comes from an engineering perspective, namely Humanistic Intelligence (HI), as shown in
Fig. 1. The fundamental perspective of HI is that mechanistic systems are not of interest for any “inherent” capabilities, but rather they are of interest in the context of the directed application of any device towards ends determined by a human, who uses devices as a means toward a conscious end [10], [11, p. 68].

We use HI as our preferred embodiment of sousveillance, since the attributes of a system using HI are of economic consequence due to the costs involved – not merely the financial cost of the apparatus, but also in terms of the resources represented by the HI pathways. Specifically, the “cognitive bandwidth” (i.e. the attention needed to complete a transaction) of a participant is a significant resource in itself. This implies, for example, that a system that requires a user to complete 10 steps synchronously (e.g. unlock smartphone, swipe, swipe, launch application, select payee, input amount, initiate transaction, review transaction, confirm transaction, lock smartphone) is much less likely to succeed, due to its greater transaction cost,1 than one embodying HI, which may only take a single asynchronous step to complete the same transaction (e.g. an unmonopolizing prompt, triggered by the situational awareness of the HI device, requesting a payment of $4 to The Coffee Shop and requiring only an asynchronous binary response to accept or decline the payment). The same logic as for a financial transaction also holds for sousveillance, in that sousveillance accomplished using an HI system may require no conscious effort at all, and so less use of scarce resources, thus improving efficiency, and therefore again reducing transaction costs.

In this model of system analysis, human and machine are considered as a single unit – the human’s capabilities may be augmented or diminished by the devices they are joined with. “We prefer to regard the computer as a second brain, and its sensory modalities as additional senses, which through synthetic synesthesia are inextricably intertwined with the wearer’s own biological sensory apparatus” [16].

In this way, human-centric values (such as preferences, motivations, objectives, sense of justice, interests) preserve their usual meanings, allowing us to reason about them. In particular, the focus on human participants and their objectives also affords us consistency in reasoning about the future – capabilities may shape specific desired outcomes, but the underlying motivations (and the mechanisms that generate them) remain the same, and are distinctly human. To make the lack of distinction between human and cyborg (human+machine) clear, we note that all humans are equal in worth, but no two humans are equal in function. That is to say, cyborgs merely add to the natural and already existing variability of human abilities; they do not form an independent category of life-form. Furthermore, since sousveillance and surveillance are social actions, as in Fig. 2, a universe consisting of a lone cyborg cannot give rise to surveillance nor sousveillance; this result differs fundamentally from the ANT model, where inanimate objects are also considered actors in their own right.

E. Propositions

To provide some clarity, we note the following propositions that follow directly from our definition of sousveillance and surveillance. All veillance is purposeful action. All sousveillance and surveillance is purposeful social action, where society is two people, or one person plus a society. Therefore, a camera inadvertently left on is engaged in neither sousveillance or surveillance,2 and a universe consisting of only a single being supports neither sousveillance or surveillance.

Consider a person, engaged in sousveillance, producing artifact X. Later, X is turned over to the authorities in

---

1While here we mean “transaction cost” in a very literal sense, in general we mean the classic concept as introduced by Commons [12] and developed by Coase [13] and Williamson [14]. In particular, while we acknowledge the importance of trust in enabling efficient transactions, we share the perspective that mitigation of opportunism [15] provides many of the same advantages. See Sec. II-C. Furthermore, we see the cost of enforcing property rights, e.g. via courts or arbitration, as non-negligible. We examine this in more detail in Sec. II-E.

2Later viewing of the recording may be some form of sousveillance or surveillance, however at the time of capture there is no intention and therefore no sousveillance or surveillance.
support of a criminal investigation, to augment their existing crime-scene artifacts. The authorities are then engaged in surveillance based on $X$, even though $X$ is a direct product of sousveillance.

Conversely, for example, consider the situation that government surveillance artifact $Y$ is leaked, perhaps in support of publicizing government corruption, unjust use of violence, or incompetence. Then, artifact $Y$ is being used for sousveillance – even though the original act producing $Y$ was surveillance.

II. Economics of Sousveillance

Economics, as defined by the Merriam-Webster dictionary, is “a social science concerned chiefly with description and analysis of the production, distribution, and consumption of goods and services”. Due to the corporeal reality of humans, economics can be considered in terms of human action. We define action as purposeful and goal-driven behavior, and not reflexive or instinctual behavior, which is conceptually excluded from the category “action”. Economics, therefore, is a study of human action [17, Ch. 1].

Due to the fundamentally social nature of humans, economics has always been concerned with the actions occurring between parties, which we distinguish here as social action, hence the categorization of economics as a social science.

While the general premise of the high economic value of relationships, and the consequent division of labor and specialization it affords, has been recognized in broad terms for millennia [18, p. 103], more recent work has illustrated the mechanisms humans use to gain both efficient production and use of resources. As we will discuss in greater detail below, in Sec. III, economics profoundly affects the ability of man to perform morally positive actions, because such actions typically require resources, and more generally, prosperity. “Prosperity” in economics typically refers solely to material wealth. However, in this work we use the term in the more general English-language sense that includes wealth, physical health, security of person, emotional well-being, personal growth, and so on. The etymology of prosperity is “good fortune”, but this connotes a degree of fatalism – i.e. prosperity is something that occurs solely by external forces. We consider prosperity in the sense of “flourishing”, that for any individual depends on both correct internally-directed action, and favorable external environmental conditions.

We take as well-established that general prosperity requires specialization of labor [20]. This implies further that group size is critical for material prosperity, since larger groups functioning well can specialize to a much greater degree. To profit from the properties of large group size, the participants must be able to engage in exchange. This necessitates that participants in a large society limit themselves in particular ways, so that emotions such as trust and empathy can be established, and that outcomes such as justice can be expected.

Large-group cooperation, in the form of transactions, is a fundamental requirement for societal prosperity.

A. Sousveillance, trust, and transactions

A trustworthy party is one that will not unfairly exploit vulnerabilities of the other parties in the relationship. The reason trust is important economically is to enable transactions to proceed with a minimum of transaction costs. Trust is linked to identity, and the reputation ascribed to that identity. Examples of the benefits of trust-based transactions in cost and efficiency, dating back over a thousand years, can be found in the ancient Muslim “Hawala” transfer systems [21], [22], [23] and the Jewish Maghribi trader’s coalition [24]. The fact that Hawala money transfers are still used today, and remain less expensive than modern electronic banking systems, provides attestation of the economic advantage of trust-based transactions. An excellent review of trust from an ethical perspective is in [8, p. 308], from which we quote:

“The necessary conditions for a trusting relationship... are:

1) Interdependence: at least one party in a trust relationship must be dependent on at least one other party in order to accomplish a goal.

2) Vulnerability: at least one party in the trust relationship is vulnerable to the opportunistic behavior of another party in the trust relationship.

3) Risk: as a result of this vulnerability, the interests of at least one party in the relationship are at risk.

We can then define a trust relationship as one of interdependence where at least one party is vulnerable to the opportunistic behavior of at least one other party to the relationship but where nonetheless the vulnerable party voluntarily accepts the risks of its vulnerability.”

In the present analysis, we can assume that potentially transacting parties already have some degree of interdependence, hence the attempt to transact. With respect to sousveillance, a sousveiller $A$ has fewer vulnerabilities to the other transaction participant $B$ than if sousveillance is not employed. Then, for each prospective transaction occurring between $A$ and $B$, with $A$ employing sousveillance, there are the following cases:

1) transactions that proceed (or not), but would have (not, resp.) proceeded anyway without sousveillance, i.e. $A$ already trusts $B$; (2) transactions that proceed solely because of sousveillance.

The canonical example is that of the pin makers given by Adam Smith [19]. He documents how a lone unskilled pin-maker might be pleased with an output of 1 pin per day, so that ten independent unskilled pin makers could produce 10 pins per day. However, by dividing the labor among the same ten men, each with a specialized task and station appropriate to the their task, one can expect a typical output of 48,000 pins per day, corresponding to an increase of $4800 \times$ more pins per participant, using the same input materials and laborers.

4Hawala traders operate by accepting cash in local currency, then transmitting the payment order, along with a password, to another trader in the (generally foreign) destination city. The recipient can then pick up the money by presenting the password to the destination trader, usually the next day. The balance between traders is maintained informally, with no promissory instruments exchanged, so these transactions are based entirely on the honor system. Currency exchanges take place at market rates, rather than any official exchange rate. A typical commission fee is 0.2%-0.5%, which is far less than banks charge.

5We assume the “prospective transaction” is in good faith – both parties are voluntarily transacting and expect, ideally, to complete the transaction honestly. This rules out “transactions” such as theft, fraud, and “showrooming”, i.e. examining merchandise without intention to purchase from that seller, only to purchase the same or similar product elsewhere.
sousveillance, and would not have without sousveillance, i.e. due to A’s reduced vulnerabilities by employing sousveillance, mean that A has less reliance on trust and so is more willing to deal with party B; and (3) transactions that are aborted because of sousveillance – since our premise is that A employs sousveillance, this case indicates a rejection by B to engage in a transaction.

Now let us analyze these cases with respect to trust and transactions. In case 1, sousveillance has no impact on trust or transactions. In case 2, sousveillance allows transactions to proceed that would otherwise not be initiated, and so increases the number of transactions. This has the ancillary benefit of allowing a relationship to develop that may lead to the involved parties eventually trusting one another. In case 3, sousveillance has no impact on trust, and reduces transactions. While this appears to be an argument against sousveillance, it actually a direct validation of our thesis that societies that reject sousveillance will be impoverished, relative to those accepting sousveillance.

Therefore, sousveillance employed across many transactions (i.e. at a societal level) enables an increase in the volume of transactions, and so enabling greater specialization and consequently greater prosperity.

Since case 3 illustrates the primary social issue blocking widespread use of sousveillance, as opposed to financial cost issues, or technological issues, let us examine this case in more detail. The refusal to deal in the presence of sousveillance implies a refusal to deal due to a change in the vulnerabilities of the involved parties. Namely, the one employing sousveillance is less vulnerable to the arbitrary authority of the other party, and the authority in fact may be made more vulnerable due to the ability of the sousveiller to obtain recourse from a more powerful entity such as a consumer advocacy bureau, the police, a judge, or public opinion.

One might make an argument based on emotion, that transactions may be aborted solely because the “feelings” of B, for example that A lacks sufficient trust and faith in B as evidenced by the choice to employ sousveillance. Thus, B is in fact reasoning about A’s choice to engage in sousveillance.

Based on experience with the deployment of surveillance, feelings about sousveillance are a function of how often one encounters it. The present author finds widespread surveillance of roads, highways, offices, and shops highly disturbing, inducing a “creepy” feeling. However, with sufficient saturation of surveillance in society, it becomes merely another fact of life to which we adjust. In fact, in the case of the shop-keeper, we can empathize with their position in using technology to prevent theft and identify criminals. We also can recognize the benefit to all shoppers in the form of lower prices. Lastly, we recognize that while surveillance can easily be used as evidence against criminal acts, it is more difficult to use such recordings to implicate innocent individuals, and in fact may exonerate them from claims of wrong-doing.

B. Economic implications of information

We now consider transactions with respect to information available to transacting parties, and the effect of sousveillance in information asymmetries.

In “The Use of Knowledge in Society” [25], Hayek argues that the inherently decentralized nature of economic knowledge, specifically of prices, implies that the fundamental barrier to central economic planning is information. This means, for any real economy, the “price mechanism” summarizes the local information regarding cost, availability, and demand of any good, in such a way that others can reason about their economic decisions in a way that benefits all parties involved. Hayek was the first to clearly elucidate how the price mechanism leads to efficient allocation of resources, across society, by ameliorating the problem of local knowledge. The key insight is that on the whole, participants in any action have more information available to them than any central authority can possibly have. In general, limits of any central authority are cognitive in nature (although the specific bottleneck may be in data collection, collation, bandwidth, storage, processing power, or dissemination of results).

Economic information, i.e. information used in the decision-making process, does not only take the form of prices. For example, honest dealing, quality of service, prompt and complete fulfillment of explicit or implicit contracts, responses to exceptional conditions, and customer support, are all examples of non-price information that may have more influence on prospective buyers and sellers than price alone.

The branch of economics called information economics, or the economics of information, is concerned with the unique attributes of information when considered from an economic perspective [26], [27], [28, p. 20]. When one party to a transaction is in possession of relevant information not disclosed to the other party, this situation is referred to as an information asymmetry. In classical economics, information is typically considered in itself enough to enable a decision to be made – thus, if an economic actor (e.g. a consumer, manufacturer, insurer, etc.) is aware of a particular fact, then that information may be immediately used in their decision-making process.

In the context of an information asymmetry (i.e. where sousveillance is typically employed), however, raw information or knowledge of an event by an individual is often insufficient to obtain a desirable outcome. By definition, the sousveillance practitioner is not in a position of authority, and therefore, without verifiable documentary evidence, information reported by the sousveiller to any higher authority may be on its own insufficient to attain their goal and to meet the needs of the sousveiller. Testimony can be challenged by other testimony, and in this situation, the person with greater

---

6 Former San Francisco police commissioner Peter Keane, in a 2011-Mar-15 San Francisco Chronicle article “Why cops lie”, comments: “Police officer perjury in court to justify illegal dope searches is commonplace. One of the dirty little not-so-secret secrets of the criminal justice system is undercover narcotics officers intentionally lying under oath. It is a perversion of the American justice system that strikes directly at the rule of law. Yet it is the routine way of doing business in courtrooms everywhere in America.”
authority has an advantage.\textsuperscript{7}

For available information to be acted upon, whether by a consumer making a purchase or a judge making a ruling, the quality of any information is critical in determining to what degree it affects any decision regarding how to act. Veracity and accuracy cannot always be determined by testimony alone, and when conflicting testimony is presented, often the participant in a position of authority is more trusted. However, if information is timely, organized, and presented with supporting evidence, then the determination of veracity depends less upon the authority of the one testifying.

By the nature of authority there are, in general, fewer parties in authority, than the number of parties not in authority. This is true because if more than one party wishes to enforce their will, conflict arises, and by definition the party with greater authority has an advantage.\textsuperscript{7} Police Lie Under Oath", Michelle Alexander describes some of the perverse economic incentives that lead to these counter-productive practices, such as illegal quotas for the number of arrests police need, to obtain associated rewards, combined with a lack of consequences for professional misconduct.

Sousveillance can play a valuable role in lessening the problem posed by this dilemma, by enabling a reduction in the information asymmetry. For example, a contractor working in a high-risk environment may opt to use sousveillance to reduce his occupational hazard insurance premium. Likewise, a driver may choose to record his own actions to obtain a lower premium on his car insurance.\textsuperscript{8}

C. Opportunism

Opportunism is the taking of unfair advantage of another party. Combating opportunism is arguably the most important factor [30, p. xi] in establishing economic prosperity, at both the micro and macro scales. For opportunism to occur, there typically must be an imbalance in either knowledge or power between the transacting parties. A “golden opportunity” [31] is a situation in which a party can engage in opportunistict behavior without any possibility of getting caught. By reducing exposure to such “golden opportunities”, sousveillance acts to reduce the “attack surface” of potential victims. Some forms of opportunism have already been discussed, for example moral hazard can be considered a form of reneging on a contract. In [30, pp. 30–36] Rose proposes a classification of the different kinds of opportunism into three degrees, which we present here with an examination of the roles sousveillance plays in combatting them.

1) First-degree opportunism: This “involves taking advantage of the imperfect enforceability of contracts”. Examples include reneging on contracts, shirking, and self-dealing. These practices are typically illegal, and so can be legally remediated, if caught. Sousveillance has immediate and obvious applicability to this situation in two respects.

One way sousveillance applies is that enforcement of contracts requires information regarding the execution of the contracted good or service. By engaging in sousveillance, the party executing the contract can verifiably demonstrate that the agreed-upon terms are being met. To give a simple example, consider hiring a house painter, who agrees to sand and clean all surfaces, apply primer, and use three coats of top paint. After the job is completed, it may be difficult for the customer to determine if the correct and agreed-upon process was followed, or if the painter was shirking his contractual obligations. Using sousveillance, the painter can generate hard

\textsuperscript{7}Furthering the argument, in a 2013-Feb-02 New York Times article “Why Police Lie Under Oath”, Michelle Alexander describes some of the perverse economic incentives that lead to these counter-productive practices, such as illegal quotas for the number of arrests police need, to obtain associated rewards, combined with a lack of consequences for professional misconduct.

\textsuperscript{8}Note that if there is no other option available, e.g. having insurance is mandatory, and recordings are mandatory, perhaps because there is only one insurance company in that field, and the recordings are sent directly to them, this becomes surveillance.
evidence that the contract was fulfilled correctly. In this way, sousveillers can mitigate accusations and suspicions of first-degree opportunism.

The other obvious way that sousveillance applies to first-degree opportunism is in the detection of it, and in the identification of the culprits. For example, consider a theft of personal property occurring in a busy and crowded area, with heavy surveillance, such as at a cafe in a shopping complex at lunchtime. Obtaining surveillance recordings is at the discretion of the property managers, and even if available, are likely to cover such a wide field-of-view that the perpetrator may not be identifiable. Sousveillance affords a first-person perspective covering the immediate vicinity of the sousveiller, is immediately available for review and, if necessary, available for submission to either the authorities for investigation, or to appeal to the public for further information about the offender. In this way, sousveillance acts as a mechanism to reduce the cost of justice, since obtaining forensic evidence becomes routine and inexpensive.

2) Second-degree opportunism: This form of opportunism “involves taking advantage of the incompleteness of contracts because most contracts cannot anticipate every possible eventuality”. This form of opportunism is typically legal, so the usual remedy is to cease dealing with the offending party. Routine examples of incomplete contracts are those for employment, which may execute over years or decades. Contracts of any significant duration are generally incomplete, since as Klein [32] notes:

“When a large number of possible contingencies exist regarding future events, the use of the fully contingent complete contract of economic theory is too costly. Transactors use incomplete contracts in these circumstances not only to avoid the significant “ Ink costs” of writing fully contingent contracts, but, more importantly, because incomplete contracts avoid the wasteful search and negotiation costs that otherwise would be borne by transactors... Transactors enter relationships knowing they have left some unlikely contingencies unspecified, recognizing that if such a contingency develops, it will have to be handled after the fact. In addition to avoiding the rent dissipation search and negotiation costs involved in complete contractual specification, contracts are incomplete because of measurement costs.”

Sousveillance can help combat second-degree opportunism in two ways. One is that because it allows the negotiation process to be on record, at very little cost, this gives the transacting parties a basis to reason about the implicit understandings in a contract. With sufficient timestamping for sequencing negotiations, so that later clarifications are accounted for, it is reasonable to expect that any dispute arbiter would accept a sousveillance-based record of negotiation as definitive for determining the interpretation of what was actually agreed to in a contract.

A second way that sousveillance can help is that it enables certain measurements to be routine and inexpensive. In the case of video sousveillance, these are measurements based on visual inspection. This implies that at least some measurement of the executing process can be stated explicitly in contract, thus avoiding incomplete contract specification due to concern about measurement cost, in the applicable domain.

3) Third-degree opportunism: Finally, third-degree opportunism “involves taking advantage of discretion that exists in a relational contract”. A “relational contract” is one in which the explicit terms are very broad, relying heavily on implicit understandings and the discretion of the parties involved. The prototypical situation is that a principal hires an agent to perform some specialized function (e.g. a doctor, lawyer, engineer, or CEO). In the course of carrying out his duties, the agent decides to accept a lower payoff for the principal in exchange for a higher payoff for himself. Then we say that the agent has engaged in third-degree opportunism.

For example, say an unknowledgeable car driver (the principal) takes their vehicle for repair into an auto shop. The mechanic (the agent) then examines the vehicle for problems, and makes his recommendations for repairs. The principal has no way to immediately evaluate the veracity of the agent’s recommendations, and is therefore vulnerable to third-degree opportunism.

In this case, sousveillance can be employed in a similar manner as in first-degree opportunism, but by the principal rather than the agent. In our example, the car owner can convey detailed information of the interaction to another mechanic or other knowledgeable person either at the time of the transaction, or after it is completed, to determine if the mechanic was in fact behaving opportunistically.

4) Sousveillance and the Degrees of Opportunism: In all three degrees of opportunism, sousveillance affords some mechanism for combating the behavior, and in the other direction, can often help a wrongly-accused party to establish their innocence. Of course, sousveillance cannot address all instances of opportunistic behavior, since the root cause is internal to the decision-making process of the offender. The basic mechanism that is common to all cases where sousveillance can be applied, ultimately, is that sousveillance enables accountability. The path to this desirable outcome may take the form of detecting opportunism, identifying the persons responsible for it, or dispelling accusations of opportunism.10

Who would you rather hire to paint your house? Us, who offer a sousveillance video of the process, or our competitors, who don’t?

---

9 Sousveillance may incidentally provide other benefits for a sousveiller. Consider the following advertisement.

10 Accountability for actions implies both negative consequences (punishments) and positive ones (rewards). Sousveillance functions in the same way with respect to laudable moral behaviors, as with reprehensible ones. Thus, by using sousveillance to detect laudable behaviors, and identifying the persons responsible for them, sousveillance also allows those responsible to be rewarded.
D. Bureaucratic terror and sousveillance

The preceding sections of the present work have dealt primarily with voluntary economic transactions that are financial in nature. In this section, however, we consider sousveillance as a mechanism for avoiding undesirable feelings when dealing with bureaucrats, such as helplessness, powerlessness, and ultimately, terror. These transactions may be compelled by legislation, and therefore, as non-voluntary transactions, take on different characteristics than those based on voluntary good faith. In particular, the asymmetries in both authority and information are generally more extreme, and the option to “vote with one’s feet” and find another service provider isn’t available, in general, when transacting with a bureaucracy.

The word “bureaucracy” comes from the French for desk or office, “bureau”, and the Greek for political power, “κράτος” or “kratos” in the Latin alphabet. Terror, from the Latin for “great fear”, is an emotional state of extreme fear. Fear, in general, is a healthy reaction to potential sources of risk. For example, a person may reasonably feel fear when standing near the edge of a high cliff, or when working with a hot stove. Fear acts to help preserve bodily integrity and well-being. When the degree of fear becomes too intense, rather than having a protective function, it leads to paralysis, irrational behavior, and even lashing out. Therefore, let us recognize terror as a kind of unhealthy fear. An inconsistent and disproportionate response from an external interaction can induce this state, even in a healthy person [33, Ch. 1].

1) Bureaucracy: The modern bureaucratic system of administration was championed by writers on management such as Weber, Taylor, and Drucker. One of the key benefits of a bureaucracy, as envisioned by Weber,11 is that rules are as Weber, Taylor, and Drucker. One of the key benefits of bureaucracy – for example, a City Hall, the police, emergency administration was championed by writers on management such as Weber, Taylor, and Drucker. One of the key benefits of a bureaucracy, as envisioned by Weber,11 is that rules are generally more extreme, and the option to “vote with one’s feet” and find another service provider isn’t available, in general, when transacting with a bureaucracy.

He goes on to point out that bureaucracies in the private sector are invariably developed as a consequence of government-granted monopolistic rights, since otherwise there are always alternatives for customers to turn to, forming a natural antidote to bureaucracy. In this section, we specifically examine non-consensual bureaucratic transactions, i.e. with a government bureaucracy – for example, a City Hall, the police, emergency first-responders, courts, or any of the multitude of Administrations, Departments and Ministries of modern nation-states.

2) Depictions of Bureaucracy: Bureaucratic terror is a staple of dystopian novels, such as Franz Kafka’s “The Trial” (1925) and “The Castle” (1922), and Yevgeny Zamyatin’s “We” (1924). Other fictional depictions include Bulgakov’s “The Master and Margarita” (1967) and C.S.Lewis’ “The Screwtape Letters” (1942). A typical description from this genre, from the preface to “The Screwtape Letters”, runs as follows.

“I live in the Managerial Age, in a world of “Admin.” The greatest evil is not now done in those sordid “dens of crime” that Dickens loved to paint. It is not done even in concentration camps and labour camps. In those we see its final result. But it is conceived and ordered (moved, seconded, carried, and minuted) in clean, carpeted, warmed and well-lighted offices, by quiet men with white collars and cut fingernails and smooth-shaven cheeks who do not need to raise their voices. Hence, naturally enough, my symbol for Hell is something like the bureaucracy of a police state or the office of a thoroughly nasty business concern.”

3) Cognitive Limits of Bureaucracy: Even with the best of intentions, bureaucracies in welfare states face the same kind of cognitive barriers that Hayek illustrated with respect to pricing, discussed above in Sec. II-B. As Wagner [36, p. 20] states:

“Expositions of welfare economics typically assume that the analyst possesses knowledge that is in no one’s capacity to possess. A well-intentioned administrator of a corrective state would face a vexing problem because the knowledge he would need to act responsibly and effectively does not exist in any one place, but rather is divided and dispersed among market participants. Such an administrator would seek to achieve patterns of resource utilization that would reflect trades that people would have made had they been able to do so, but by assumption were prevented from making because transaction costs were too high in various ways. A corrective state that would be guided by the principles and formulations of welfare economics would be a state whose duties would exceed its cognitive capacities.”

This means that regardless of the intentions of the bureaucrats, when resource allocations, or higher-order means controlling them, are centralized, then mis-allocation is bound to occur. The issue is fundamental and cognitive in nature, and so while measures may be taken to improve the situation (i.e. make it “not worse”) it appears that it is impossible to make the mis-allocation disappear (i.e. make the situation “better”).

4) Bureaucracy and Power: Bureaucrats have the legal force of their respective governments backing them. This is not quite the same as having power over their euphemistically-named “customers” – those who must contend with the bureaucracy. In “On Violence” by Hannah Arendt [37, p. 239], she delineates “power” as the ability to voluntarily regulate, control, and make decisions in a social context. On the other hand, “violence” indicates a lack of power, and forms a means to gain some of the characteristics of power, and in this way, violence acts as a kind of simulacrum of genuine power. That

---

11 In [34, pp. 956-958], Weber enumerates his six bureaucratic characteristics as: imperial positions, rule-governed decision making, professionalism, chain of command, defined responsibilities, and bounded authority.
is to say, while some “customers” accept the legitimacy of the bureaucracy, and therefore the bureaucracy holds genuine power over them, in other cases the “customer” transacts with the bureaucracy only due to the implicit threat of violence. While in general one may see a bureaucracy as simply an administrative function, insofar as “[a] durable system of government must rest upon an ideology acknowledged by the majority” [17, p. 189], the “customer” is aware at some level that ultimately, every government bureaucracy has recourse to violence, to force acquiescence to their rules.

Those rules are generally in accordance with the public legal code, usually published in a set books, such as the “Code of Federal Regulations” in the USA. However, the actual operation of administrative functions relies on a set of handbooks and guidelines commissioned and published by the bureaucrats themselves. Let us refer to these as the “second set of books” [38]. Without direct access to the “second set of books”, the “customer” has no way of reliably knowing what the outcome of a bureaucratic process will be. This uncertainty creates fear in the “customer”. Depending on the degree of not knowing what to expect (i.e. the “customer” knowing only that they may suffer disproportionate or inconsistent responses, backed by the force of law), this fear can pass beyond the point of “healthy fear” and into the domain of terror.

5) Sousveillance in Bureaucratic Transactions: Sousveillance acts toward alleviating the asymmetry in information and authority inherent in a bureaucratic transaction. One way this occurs, with respect to authority, is that the “customer” is able to share his side of the story, with full documentary evidence rather than mere testimony. This is true for both a bureaucratic transaction itself, and for any events leading to the bureaucratic transaction. Sousveillance allows a sousveiller to share the context of potentially controversial actions, so that both bureaucrats and the public can review the evidence from a first-person perspective.

If a transaction proceeds with a poor outcome, the “customer” may then appeal to higher authorities or the public. Sousveillance functions to provide the sousveiller, who by definition lacks authority in dealing with the bureaucracy, with a simulacrum of authority (see also “swollag”12 in [39]). This reduces the terror in the “customer”, since as a sousveiller the “customer” has evidence to challenge disproportionate bureaucratic responses so that they may not need to suffer them. Another way that sousveillance can improve the situation (i.e. transactional outcome) is with respect to information. As sousveillance becomes more widespread, more recordings of bureaucratic interactions become available for review. Armed with instructional sousveillance video of previous transactions, “customers” can know better what to expect, and are better able to identify inconsistent behavior from the bureaucracy.

In the present work, we focus on video sousveillance for clarity; however, USA’s federal Freedom Of Information Act (FOIA) enables a kind of sousveillance where the artifact produced is a literal copy of “the second set of books”, as well as related case-specific information. These forms of cooperative sousveillance (“Access to Information” acts) have been implemented, in various forms, by many nations (e.g. Canada, France, Norway) as well as many state and provincial legislatures. When successful, this form sousveillance can clearly reduce the information asymmetry between a bureaucracy and its “customer”. This gives insight into the bureaucracy’s operation so that the “customer” can successfully reason about what reactions to expect. We predict FOIA-type laws will continue to spread, since as a form of sousveillance they also give rise to economic efficiency in non-voluntary transactions.

E. Summary of Economic Benefits of Sousveillance

Sousveillance can:
• reduce the cost of justice, per Sec. II-C1,
• reduce a sousveiller’s vulnerabilities to other transaction participants, per Sec. II-A,
• reduce transaction costs by limiting “golden opportunities” for opportunism, per Sec. II-C,
• enable transactions that otherwise would not occur, per Sec. II-A,
• provide context for controversial actions, per Sec. II-D5,
• reduce information asymmetry, per Secs. II-B, II-D5,
• discourage negative outcomes and encourage positive ones, per Sec. II-C1,
• enable accountability, per Sec. II-C4, and
• be shown to be inherently distributed, per Sec. II-B.

III. Morality and Sousveillance

In this section we briefly review some general properties of morality, and apply these properties to two kinds of action, namely sousveillance, and forbidding sousveillance. We show that while sousveillance is a descriptive term, not a normative one, the act of forbidding sousveillance may prevent positive moral actions to be taken.

A. Positive and negative moral actions

In general, classes of human action (i.e. verbs) when considered without context, are amoral; this means that mere descriptive terms regarding actions are morally neutral. Morality does not exist in the kind of action itself, which is merely a tool to accomplish an end, and the morality of any particular action can only be rationally considered in-context.

Certain terms used to indicate actions are morally lauded or proscribed in the very definition of the word, such as theft or murder. Thus, these terms for actions are morally normative, in that their application intrinsically praises or condemns persons engaged in those actions. Morally normative terms form an exception to the general rule of human actions being amoral absent context. Consider the moral prohibition: “do not steal”. This indicates that the action indicated simply should not be performed, at all. If the prohibited activity is engaged in, it requires a strong explanation. Conversely, consider the moral exhortation: “be charitable”. The exhortation indicates a moral benefit from being charitable, that is, this action should be

---

12Swollag is to the authorities, what gallows are to the commoners. Swollag is also gallows spelled in reverse.
engaged in when possible – it is not a commandment that this action needs to be carried out at all time (e.g. in lieu of feeding one’s family).\textsuperscript{13}

Moral value judgments of positive moral actions can serve two distinct purposes: one purpose is to help decide which of the many potential positive moral actions available to an individual should be carried out,\textsuperscript{14} and another is to evaluate the degree of success within a particular kind of action.

In [30], Rose argues that any economically successful system of morality must consider negative moral actions universally, from a non-consequentialist perspective (i.e. do no wrong, regardless of the consequences\textsuperscript{15}), whereas positive moral actions must be considered from a consequentialist basis (i.e. each potential action is evaluated by its consequences) in order to select which actions to take. Accepting this foundation implies that we then have a rational basis to determine both the form or kind of positive moral action, by using consequentialist reasoning to compare multiple alternatives, and to determine to what degree should we engage in that positive moral action, again using consequentialism to maximize benefits and minimize costs.

Another point that helps to see the asymmetry between positive and negative moral actions, is that positive moral attributes are often defined as optimums between negative moral attributes – but not the reverse. For example as noted in [8], Aristotle pointed out that “courage” is the optimal balance between recklessness and cowardice, and likewise “generosity” can be considered the optimal balance between stinginess and profligacy. In this way, we can see why for any particular positive moral action, it is impossible to have too much of it, considered by itself – only relative to other potential positive moral actions can such a decision be made.

\textbf{B. Application to Sousveillance}

Having distinguished between the moral values regarding positive moral actions and negative moral actions, an important issue is whether a positive moral action can depend on sousveillance; if so, then an absolute prohibition of sousveillance forms a negative moral action in itself. To establish the non-normative property of sousveillance, let us consider a particular case.

A man engages in sousveillance, and thereby obtains documentary evidence regarding the commission of a crime. Now, with this information, the sousveiller has multiple options, including doing nothing. Other options are presenting the evidence to the victim, the public, or to legal authorities. These

\textsuperscript{13}Theft may be considered morally acceptable to feed one’s family as a one-time event to preserve life, however, this is an example of an exception with justification. Routine theft, even to feed one’s family, ultimately leads to impoverishment on a larger scale for both sellers who must charge more and invest in security, and all other consumers, who must pay more.

\textsuperscript{14}For example, a person helping another may need to decide, should I give this person money, or instead provide encouragement and assistance in gaining employment? Positive moral actions in general require resources which are finite, such as money and time.

\textsuperscript{15}Exceptions can be made, however, they must be specific in nature and not merely appeal to a “greater good” rationalization. See [30, ch. 6-8] for details.

\textsuperscript{16}The best weapon against extortion may be sousveillance; in a sousveillance society (i.e. where sousveillance is widespread), extortion will tend to be discouraged or at least brought to justice in many situations, especially if both parties are conducting sousveillance.
B. The analogy between cryptography and veillance

In Sec. II-A, we briefly considered the social acceptance of sousveillance based on experience with widespread surveillance. However, there is a key and fundamental difference between sousveillance and surveillance: surveillance by definition is reserved for those with authority, whereas sousveillance is not. Since those persons with authority are the ones who, in practice, determine the rules that those without authority submit to, such comparisons between sousveillance and surveillance are limited in their generality. Another approach is required to model this critical aspect of sousveillance.

There is a natural analogy between veillance and cryptography, as shown in Fig. 3. Cryptography, like veillance, may be distinguished by the domain of application, and takes on different characteristics depending on the authority relationships between various parties.

Let us consider an individual as being capable of action, and an action involving multiple persons, called the participants, as a transaction. Now consider a party external to a particular transaction (a third party). Both cryptography and veillance then act to control (restrict or enable dissemination of) information about the transaction.

In commerce, we wish to minimize transaction costs. In the domain of online sales, cryptography contributes to this goal by keeping sensitive payment information out of view from criminals that may wish to use that payment details for their own purchases. Likewise, if an employee wishes to share confidential business plans with a colleague online, encryption is typically used (e.g. a corporate VPN) to again prevent the dissemination of the confidential information – say from their competitors – again contributing to efficiency thereby reducing transaction costs and increasing prosperity.

However, as these two examples of cryptography illustrate, the participants in a cryptography-based transaction must cooperate to accomplish their transaction. If either party is antagonistic to the use of cryptography, then the transaction either doesn’t proceed, or proceeds by other means.

Yet, historically we see examples of antagonists to cryptography, using their authority to mandate controls on the use of it. There is a very clearly analogous situation, as in sousveillance. Referring again to Fig. 3, we see that when parties in positions of authority engage in cryptography (we can refer to this as surcryptography), but at the same time prevent others from using it (i.e. engaging in souscryptography), then the present dynamic of “McVeillance” (surveillance, combined with a prohibition on sousveillance) [40] is replicated in the domain of cryptography, forming a system of “McCryptography”.

McCryptography was in fact the usual state of affairs, until two key events occurred. One was the release of PGP, in particular its source code; and the second event was the creation of the World-wide-web, composed of servers and clients using the HTTP protocol and graphical user interfaces. The first event provided the technological capability, and the second created the economic necessity of cryptography being available for personal use.

1) The legal status of PGP: While governments and large corporations have had access to strong cryptography at least since 1982, when RSA Inc. (now a part of EMC Corp.) made their products available on the market. Later, in 1991, Phil Zimmerman released the first version of PGP, including the source code which was subsequently uploaded to the Usenet message system. The well-known cryptographer Bruce Schneier considered PGP as “the closest you’re likely to get to military-grade encryption.” [41, p. 587]. Usenet by design replicates posts across its global network, so that political dissidents, cypherpunks (free communication activists), peace activists, criminals, and ordinary citizens around the world now had access to cryptography strong enough that it was in practice unbreakable by any adversary, including governments.

Soon after the release of PGP, in February 1993, the author Phil Zimmerman became the target of a federal criminal investigation, and was charged with “exporting munitions without a license” [42, pp. 368–370]. The law at the time considered encryption software using keys greater than 40 bits in length as “munitions”, so the 128-bit scheme used in PGP was classified as such. Zimmerman reacted by reasoning that while software could be classified as munitions (along with firearms and missiles), it had already been legally established that books were protected as free speech. So, he published his source code in the form of a printed book. The case was dropped, so his theory was never tested in court.

2) The Liberalization of Cryptography: Citing economic concerns, the legal control regimes around cryptography were substantially liberalized [43, p. 2.118], not just in USA, but in most of the world, with the exception of France. Even in France, exceptions have been made for precisely the reason we argue that widespread sousveillance is inevitable: economic prosperity. Secure online banking and online shopping for goods and services are “killer apps” for cryptography. No government wishes to drain their coffers by prohibiting technological developments, when they have the potential to dramatically improve economic efficiency. Numerous large
corporations have indeed sprung up around cryptography and data security, far more so than would supported by a purely “crypto-as-munitions” legal regime.Important new use cases (since the mid-1990’s) for cryptography have become routine: VPNs for remote network access to corporate data, whole-disk encryption, secure single-sign-on across a large range of Internet properties from providers such as Google, Yahoo!, and Microsoft, and whole-system cryptography for “cloud computing” encompassing both disk images and all network communications, are a few among the many novel uses of cryptography.

This sequence of events does not imply that the liberalization of cryptography happened automatically, without any conscious thought or effort. On the contrary, there were extensive efforts from advocates, activists, and researchers to educate businesses, the public, and legislators of the importance of cryptography. For example, here are a couple of examples of typical arguments for a liberal cryptography regime, from the early 1990’s.

“Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds.” – John Perry Barlow [46].

“I want a guarantee – with physics and mathematics, not laws – that we can give ourselves real privacy of personal communications.” – John Gilmore, [47].

These quotes are from the early days of the “cypherpunk” movement, when the arguments were more about ideals, rather than economic necessity. Since thought is the hallmark of human action, and thoughts are directed by ideals, the fundamental “rightness” of ordinary people having access to strong cryptography was a necessary precursor to the economic argument.

3) Implications for Sousveillance: In our analogy, cryptography is a kind of inverse of veillance. Both enable control over the information in a transaction, cryptography by giving the option to keep it private, and veillance by giving the option to share it. Referring back to our original definition in Sec. I-C, the key property of veillance is that it produces an artifact that can be moved through time or space.

Sousveillance, like souscryptography, has to date encountered substantial resistance from those in positions of authority. Like souscryptography, as the availability of and economic reliance on sousveillance increases, we expect that economic self-interest will compel those in positions of authority to re-consider their antagonism to sousveillance in light of self-interest, and ultimately self-preservation. As with souscryptography, antagonism towards sousveillance may initially confound using it routinely. However, the increases in economic efficiency, personal safety, and accountability that sousveillance affords are of a like scale, as those afforded by souscryptography.

Therefore, we expect a similar development and deployment path for sousveillance as with souscryptography, with initial resistance but later acceptance, once the overall benefit to all parties is evident. As we’ve seen with souscryptography, this process is not automatic, and requires strong advocates and practitioners to make those benefits evident to the involved parties, and to create a sustainable industry supporting sousveillance.

C. Thought Experiment

Consider two contemporaneous societies. One is pro-sousveillance, A, the other is anti-sousveillance, B. In both A and B, we assume surveillance is at least as common as we see today. And, assuming present technological trends continue with respect to hardware and networking, the technical ability to engage in sousveillance in this scenario comes at a cost comparable to present-day mobile phone use, and therefore is potentially ubiquitous.

In A, we see retail businesses that allow routine sousveillance by customers, enabling easier price comparison and greater personal safety. We also see a range of service-providers that agree to engage in sousveillance so that customers can routinely verify that work was done to the agreed-upon standard. Interactions with representatives of government institutions, such as emergency first-responders, licensing and passport offices, courts, and so on are routinely recorded by their “customers”, to reward those responsible for positive outcomes, and provide feedback to the administration regarding negative ones. The cost of justice is lower than in B, so that bringing opportunists to justice is more likely, and furthermore, those wrongly accused have a documentary evidence with which to defend themselves.

Now in B, where we have a regime similar to that in place today, engaging in sousveillance is technically as straightforward as in A, but the social and legal recognition of the value of sousveillance has not taken place.

Then the key question is, will the people of A move towards B’s position regarding veillance, or will the people of B move toward A’s?

If concerns of privacy come to dominate the discourse, than we would expect surveillance in B to be scaled back, perhaps proportional to the degree of sousveillance possible (which, since we assume B is anti-sousveillance, is close to none at all). Since sousveillance by its nature is most beneficial to those who otherwise lack authority, and provides them with a means of recourse in any dispute, it therefore can appeal to the bulk of society, not just those in positions of authority. However, the genuine economic benefits go to all parties, not merely the ones at the top or bottom of any hierarchy. This means B moves from McVeillance, i.e. surveillance but little sousveillance, to one of equiveillance, where the degree of surveillance is approximately equal to that of sousveillance, even if both are minimal. However, since in reality powerful interests have successfully introduced surveillance, and the practice is entrenched, we see this as

17Strong cryptography is still considered a munition in USA. However, it is reportedly straightforward now for companies to obtain an export license [44], although the cost of $250 per license may be prohibitive for Free Software [45] projects and the like.
unlikely to dissipate. Therefore, B approaches a non-negligible state of equivalence, which is the state of A.

Thus we conclude that people in B, having observed the economic efficiency, personal safety, fairness, and ultimately, the accountability afforded by sousveillance, will move toward adopting the policies of A regarding sousveillance.

V. CONCLUSION

In this work, we have considered the use of sousveillance from an economic perspective. We have enumerated properties of sousveillance with respect to economic transactions. In particular, how sousveillance can reduce asymmetries in information, and how sousveillance can be used to reduce economic opportunism occurring in varying degrees: in the imperfect enforcement of contracts (first degree), with incomplete contracts (second degree), and in the principal-agent problem (third degree). We also discuss bureaucratic (non-voluntary) transactions, and how sousveillance can be used in an institutional setting to promote accountability and positive outcomes. Finally, we consider the development and deployment of sousveillance as analogous to the use of personal cryptography, and argue that similar economic pressures will compel the acceptance of sousveillance. We explore this line of thinking in a thought experiment, and conclude that if social and technological trends in place today continue, the widespread and routine use of sousveillance is inevitable.

REFERENCES

An Information-Bearing Extramissive Formulation of Sensing, to Measure Surveillance and Sousveillance

Ryan Janzen and Steve Mann
Department of Electrical and Computer Engineering, University of Toronto

Abstract—

The word “surveillance” comes from the French word “veillance” which means “watching” and the French prefix “sur”, which means “from above”. Thus “surveillance” means “to watch from above” (e.g. guards watching over prisoners or police watching over a city through a city-wide surveillance camera network). The closest purely English word is “oversight”.

A more recent phenomenon, sousveillance (“undersight”) refers to the less hierarchical and more rhizomic veillance of social networking, distributed cloud-based computing, and body-worn technologies. Sousveillance forms a reciprocal power balance with surveillance, both being understood in the context of not just technology, but also complex human social and political relationships.

In this paper we derive a precise theoretical and mathematical framework to understand, interpret, quantify, and classify “veillance” (“watching”) as to its directionality (i.e. surveillance versus sousveillance).

While veillance can occur in a variety of sensory modalities, such as auditory sur/sousveillance, dataveillance, etc., we will focus especially on optical (visual) veillance. We define new physical concepts: the veillon, the vixel, and the veillance vector field, to provide insight into the measurement and demarcation of surveillance and sousveillance and their interplay.

I. INTRODUCTION

Surveillance is a French word that means “watching” (“veillance”) from above (“sur”). Examples include police watching over citizens, or retail establishments watching over customers. More generally, surveillance includes the observation or recording of an activity by an inanimate object (machine), or by a person not participating in the activity [1][2][3]. Surveillance often consists of cameras affixed to property or 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) [1][4][5][6][7][8]. In this sense, surveillance is typically an action initiated by a property owner.

We use the term veillance, more broadly, to describe a deliberate action of watching, observing or sensing, that does not necessarily originate “from above” (“sur”).

Another form of veillance is sousveillance, which means “to watch from below” [1][2][4][7][9]. The etymology of “sousveillance” derives from the French prefix “sous” meaning “under” or “from below”. For example, whereas surveillance is often done by means of cameras affixed to large entities (e.g. buildings and land), sousveillance is often done by means of cameras borne by small entities (e.g. individual people).

Sousveillance is often associated with grassroots, individualistic activity. It is particularly implemented in conjunction with small mobile devices such as smartphones, electronic seeing-aids, and personal safety devices [1]. Sousveillance has become a significant topic with recent advancements in wearable computing and AR (augmented or augmented reality) [1][4][7][8].

II. DISTINGUISHING AND CLASSIFYING VEILLANCE

This paper presents a theoretical, physical, and mathematical framework for veillance which can be used to precisely measure surveillance and sousveillance as well as to denote their commonality and their distinction.

This framework gives rise to a particular definition of surveillance and sousveillance which we call the “Spatial Jurisdiction” theory. For completeness, we offer several other potential theories of definition, as follows, each forming its own distinction between surveillance and sousveillance. Spatial Jurisdiction theory is the one which lends itself well to precise mathematical measurement and analysis.
• **Spatial Jurisdiction** definition, our main focus, to be defined precisely and mathematically quantified in sections III-A and III-B. In essence, surveillance is the gathering of information from sensors or processes within the user’s property or where the user is in a position of control. Sousveillance gathers information from spatially outside the user’s region of authority, political or forceful control.

• **Mounting** definition: surveillance cameras are “architectonic”, *i.e.* mounted to inanimate objects, such as land (by way of lamp posts or poles) or buildings; sousveillance cameras are “human-centric”, *i.e.* borne by people.

• **Ladder** definition: Surveillance is possible only by persons in high positions of authority; sousveillance is carried out by persons in low positions of authority.

• **Authority Exclusivity** definition: Surveillance is the veillon which prohibits other veillances; sousveillance is the veillon which is agnostic toward other veillances;

• **Participant** definition: Surveillance is the capture or recording of an activity by a non-participant in the activity; sousveillance is the capture or recording of an activity by a participant in the activity;

• **Large Entity / Small Entity** definition: Surveillance is practiced by large organizations, corporations or governments; sousveillance by small entities or individuals.

III. **Quantifying Veillance: Vixels, Veillance Vector Field, and Spatial Jurisdiction Theory**

This section will provide the theoretical background used to develop a physical quantification of veillance, and as well to distinguish and measure surveillance and sousveillance in the context of Spatial Jurisdiction theory.

While being ubiquitous, electronic veillance takes on many different forms, differing by hardware device, resolution, placement, jurisdictional control, intended purpose, and actual destination of the data.

We aim to provide a simple measurement of surveillance and sousveillance in a physical space.

Surveillance and sousveillance carry sociological and political connotations, and are understood in the context of human relationships. A mathematical accounting of veillance would benefit first by a more general understanding of “watching”, by taking the “sur” out of surveillance and “sous” out of sousveillance. Veillance itself is an action of deliberate observation, regardless of motive, political affiliation, or societal empowerment or disempowerment. We aim to measure veillance neutrally. While veillance can occur in a variety of sensory modalities, we will focus especially on optical veillance.

Typically in optics, light is traced along its pathway from its source, such as a light bulb, laser, or the sun, to its final destination before being absorbed, following along the path of any reflections, refractions or diffractions along the way. Ray tracing accounts for light along its pathway.

For veillance, though, we will trace light ray pathways in the reverse direction to account for optical observation. This reversal was found in the ancient *extramission theory* described by Plato and Ptolemy, of light consisting of rays from the eyes [10][11]. Ray tracing in computer graphics also makes use of reverse-traced light, to render an artificial scene as if it took place in a virtual space.

However, we seek to formulate extramission in real, physical space. In terms of particles, this is analogous to photons vs. “darksoms”, *i.e.* particles of light vs. a lack of light which flows in the reverse direction to the actual light. Electric charges have a similar analogy: electrons vs. holes. An electron is a carrier of negative electric charge or current, whereas a hole is the absence of an electron: a positively-charged, non-existent, virtual carrier of positive current. Holes were proposed in 1931 by Heisenberg and Dirac and have become well-established in the field of semiconductor physics. More recently, in the case of optics, “darksoms” were proposed (initially in jest) as the absence or inverse flow of a photon [12]. Darksoms (or strictly-Latin, “scotons”) are to photons as holes are to electrons. See Table I. (Darksoms have limitations in relativistic situations or astronomical distances, in that they violate causality when they reverse time-of-flight from transmission to reception. However, in most useful everyday situations on Earth, time-of-flight and relativistic effects are negligible.)

More significantly, in the case of veillance, darkoms have a key disadvantage: Even if darkoms are emitted by a camera, they still cannot account for veillance, or the *ability* to see, because a flow of darkons is dependent on the flow of photons. The ability to see should not rise and fall in proportion to the amount of light hitting a sensor pixel, because that pixel’s *purpose* is to sense the presence or absence of light. By merely pointing a camera at an object, that action alone does not cause the object to emit light. Therefore, the darkon does not fully account for veillance.
We propose a “veillon”, a new entity that accounts for observation, combined with the propagation properties of light.

We define a veillon as one quantum of veillance (for one time-sample from one pixel) which is emitted from a camera and radiates in reverse-time, to enforce causality. A veillon propagates away from the camera, following reflections according to optical properties, independent of whether light is present or not, and independent of the quantity of light received by a pixel sensor. A veillon is emitted by the camera at the time each sample is read, for each pixel.

We also define a vixel, as a spatial region that encloses the extent of observed space, controlling one pixel, or more generally, one linearly independent scalar observation signal. For a camera, a vixel is the volumetric region corresponding to one pixel in the image. (Fig. 1)

Measuring the amount of veillance in a room, or on a street, is the goal of this discussion. First, we examine a camera itself.

Veillance emitted from a digital still-image camera can be measured by the number of pixels multiplied by the bit depth of each pixel.

After the emission of veillons from a camera, the veillons can be blurred or scattered, and degeneracy can occur. For example, pointing a camera at a translucent window, which blurs all the pixels together, reduces the useful information-bearing content to fewer vixels, or as little as one vixel.

“Weveillance rate”, \( r_V \), therefore, for a video camera, is:

\[
V = r_F PB/D
\]

measured in bits/second, where \( r_F \) is the frame rate, \( P \) is the number of pixels in each frame, \( B \) is the bit depth of each pixel, and \( D \) is the degeneracy of each pixel if pixels are blurred, i.e. the number of dependent pixels controlled by each vixel. \( P/D \) gives the number of linearly independent pixels, if the optical setup causes uniqueness to be lost between the pixels. Degeneracy will be discussed further in Section IV and Figs. 5(d, e).

Vixel rays (represented along the centroid of vixels) are illustrated in Fig. 1. Vixel rays are analogous to magnetic or electric field lines, and represent the direction of veillance propagation, but without covering the entire 3-dimensional spatial extent of the vixel. As with magnetic or electric field lines, the closer together adjacent vixel rays are, the greater the concentration of pixel resolution at that point.

Therefore, “veillance intensity”, \( \tilde{V} \) is a vector field that can be defined at every point in space, with its magnitude equal to the density of veillance rays, and its direction everywhere tangential to the veillance rays. Rather than rays (lines with one start point), we now have vectors defined for every point in space. See Fig. 4.

Considering video streaming, this vector field becomes a veillance intensity bit-rate field, \( \Phi_V \), with units: [bits/m²/s].

Measuring veillance crossing an arbitrary surface can be done using “veillance flux”:

\[
\Phi_V = \int_{\Psi} \tilde{V}(\hat{r}) \cdot d\hat{S}
\]

Veillance rays are converted to the veillance intensity field, \( \tilde{V} \), at position \( \hat{r} \). A dot product is composed with normal vectors to the surface, \( d\hat{S} \), whose magnitude is proportional to the area of each infinitesimal portion of the surface \( \Psi \). Veillance flux is measured in [vixels].

More generally, in the case of more than one vixel with reflections or more than one camera, vixels may overlap. The veillance field becomes a vector set field, \( \{\tilde{V}\}(\hat{r}) \), i.e. each
point in space has more than one vector, which do not simply superpose by vector addition because they are associated with different sensors. The veillance flux becomes:

$$\Phi_V = \sum_i \int \{ \vec{V_i}(\vec{r}) \} \cdot dS$$  \hspace{1cm} (3)

A. The Spatial Jurisdiction Theory of Veillance

Surveillance is often thought of in terms of 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) [1][4]–[8]. In this sense, surveillance is typically an action initiated by a property owner.

Conversely, sousveillance typically occurs when photographing one’s surroundings beyond the scope of one’s property, such as when an individual takes photos in a public park, or uses a wearable electronic seeing-aid on public property or within another person’s private property.

B. Jurisdiction Hypersurfaces, for Quantifying Veillance

Using property lines (or more generally, multidimensional surfaces or hypersurfaces) to demarcate between surveillance and sousveillance provides an interesting discussion. By this demarcation, if an individual sets up a camera inside a building s/he owns, and if the vixels are contained within a surface in 3 dimensions enclosing the building’s property, one would be performing surveillance. However, if the camera is pointed to outside the property, onto a public street or to property across the street, the veillace flux through the jurisdiction surface counts as sousveillance.

On a political scale, a king or feudal ruler might conduct surveillance over his peasants, on the streets or inside their houses—everywhere inside his kingdom. That is, his kingdom is his “property”, encompassing many individuals’ properties. For the king, surveillance’s demarcation encompasses a larger area than for the peasants, who might individually keep watch inside or outside their own homes (surveillance v.s. sousveillance). On the other hand, using a telescope to watch outside the kingdom walls, in case a neighbouring kingdom attacks, would be sousveillance from the king’s perspective.

Following this pattern, surveillance and sousveillance are demarcated over progressively larger layers of surfaces, depending on which boundary the veilleur has power, control, or ownership over.

More generally, a “region of authority” is a better descriptor than property because it covers cases when surveillance or sousveillance are enforced in a region, legally or by physical force, and not simply by property ownership. A government can conduct surveillance within their national borders, since the entire national territory falls under a legal, military, communicatory, and economic control of that government, i.e. the jurisdiction, or region of authority, of that government.

See Figs. 5, 6, 7, 8. The region of authority is illustrated in Fig. 6, both in a property sense, and in a corporeal (body) sense. The region of authority is a closed 2-dimensional surface in 3-dimensional space.

Surveillance and sousveillance can thus be immediately quantified by veillance flux crossing this boundary (surface),
Veillance in one region of authority is the total of the veillance flux crossing into a boundary from outside (Fig. 5(b)), plus any sources of veillance emitted by cameras inside:

\[ r_{v,R} = \Phi_{v,IN,\Psi_R} T F B + e_{v,R} \]

\[ = \sum_{\text{outside}} \iint_{\Psi_R} \max(-\vec{v}_R(\vec{r}) \cdot d\vec{S}, 0) + \sum_{\text{inside}} e_{v,c} \quad (4) \]

Veillance rate, \( r_{v,R} \), in a region \( R \) (such as a room) is thus composed of the veillance flux impinging the boundary \( \Psi_R \) and veillance rate emitted \( e_{v,c} \) for each camera \( c \) inside. The integral is modified to reflect how the property border is a closed two-dimensional surface.

Sousveillance can be quantified by the amount of non-absorbed veillance leaving the region of authority (whether a property line or a region of authority around the human body):

\[ r_{sousv.,R} = \Phi_{v,\Psi_R} T F B = \sum_{\text{inside}} \iint_{\Psi_R} \vec{v}_R(\vec{r}) \cdot d\vec{S} \quad (5) \]

This becomes the “sousveillance rate” in [bits/s].

C. Real-life scenarios

For example, in Fig. 8(a) two cameras are mounted in a taxi cab, one facing backwards to place the passengers under surveillance, and another camera facing forwards to record what happens through the windshield. The latter is referred to as an “onboard camera” or “dashboard camera” or “dashcam”. If the passenger-monitoring camera is only 50% blocked by the passenger and interior of the car, then 50% of the vixels escape out the back window contributing to the sousveillance of the front-facing camera, and if both cameras are standard high-definition 1080p with 24-bit colour at 30 frames/s, the sousveillance rate (viewing the surroundings of the taxi) would be quantified as:

\[ r_{sousv.,\text{Taxi}} = (\frac{1}{2} + 1)(24\text{bits/pixel} \cdot 30\text{frames/s}) \times 1920 \times 1080(\text{pixels/frame}) \approx 2.2\text{Gbit/s} \quad (6) \]

leading to a simple result in [bits/s]. Veillance within a room, building, property or political jurisdiction can be measured using this method.

Veillance in one region of authority is the total of the veillance flux crossing into a boundary from outside (Fig. 5(b)), plus any sources of veillance emitted by cameras inside:

\[ r_{v,R} = \Phi_{v,IN,\Psi_R} T F B + e_{v,R} \]

\[ = \sum_{\text{outside}} \iint_{\Psi_R} \max(-\vec{v}_R(\vec{r}) \cdot d\vec{S}, 0) + \sum_{\text{inside}} e_{v,c} \quad (4) \]

Veillance rate, \( r_{v,R} \), in a region \( R \) (such as a room) is thus composed of the veillance flux impinging the boundary \( \Psi_R \) and veillance rate emitted \( e_{v,c} \) for each camera \( c \) inside. The integral is modified to reflect how the property border is a closed two-dimensional surface.

Sousveillance can be quantified by the amount of non-absorbed veillance leaving the region of authority (whether a property line or a region of authority around the human body):

\[ r_{sousv.,R} = \Phi_{v,\Psi_R} T F B = \sum_{\text{inside}} \iint_{\Psi_R} \vec{v}_R(\vec{r}) \cdot d\vec{S} \quad (5) \]

This becomes the “sousveillance rate” in [bits/s].

with the calculation simplified by Gauss’ divergence theorem, thus creating a measure of the amount of sousveillance emitted by the taxi. This superposition analysis could thus be performed in a variety of scenarios, from earth to space (Fig. 8(b) if the geometry is known.

IV. Degeneracy and Uniqueness of Reflected, Scattered or Blurred Vixels

Veillance flux and a veillance field were proposed so far, and can be thought of as an aggregate spatial integral of bidirectional reflectance distribution functions (BRDF). Earlier, we reversed the direction in which light is normally understood, so we could develop an information-bearing concept of light sensing.
If a camera is pointed at subject matter, the original number of vixels falling on the subject matter may be greater than the number of independent vixels reflected off the subject matter.

For example, if a security camera is pointed exclusively at a stack of cardboard boxes on one side of a room, and meanwhile a burgler is moving on the opposite side of the room, only a small amount of visual information will be available in the vixels falling on the boxes. (i.e. It will likely not be possible to reconstruct the burglar’s face just by viewing the boxes, unless the boxes were made of reflective glass instead of cardboard, leading to full vixel reflection.) In the limit of texture roughness, there may be only one effective reflected vixel from each flat face of a box. That is, for a perfectly rough surface, the only extraneous information may be “whether the lights are on” (and how bright), which is all that can be conveyed in one vixel of information.

That is, the reflected veillance from the subject matter may have degeneracy. Degeneracy is used akin to the quantum mechanics term, where one state-observation can be caused by multiple possible states. [13]

With degenerate vixel reflection, diffusion or scattering, multiple possible light sources cannot be distinguished because they activate the same dependent set of pixels. As a result, a smaller number of effective vixels are reflected, in such a situation of degeneracy. In the extreme, if all pixels are illuminated simultaneously by all light sources, the result is only one effective vixel of veillance.

One fine point: Even if only one effective vixel is reflected, diffused or scattered, a shadow or projection falling on the subject matter from elsewhere can still cause much more than one vixel of information to be “seen” by the camera, because the shadow or projection is able to independently illuminate multiple vixels directly falling on the subject matter being viewed, before they become scattered. However, after those vixels continue on after passing the subject matter, and become scattered or diffused, the number of effective vixels from the camera “seen” by looking at or through the subject matter is then reduced in the spatial region where those vixels travel next.

We quantify vixel degeneracy in the following section.

V. LASER SCANNING VIXEL PRINCIPAL COMPONENT DENSITY ANALYSIS

To put this theoretical expression into practice, we devised a method for experimentally measuring veillance, in the form of effective vixels per square metre.

We used principal component analysis (PCA) to identify the number of salient linearly independent (non-degenerate) pixel vectors activated by light from a surface area on an object — that is, loosely speaking, the amount of information expressed in the veillance impinging an object’s surface.

We used a laser to scan across the surface of an object or set of objects, while capturing a sequence of images from one or more cameras in the room, viewing that subject matter. We chose the size of the laser beam (approx. 1 mm) to cover an area smaller than one vixel (given the camera’s distance away), to avoid trivial activations of multiple pixels due to its

![Fig. 9. Testing vixels via an external projected light source such as a laser. Top row: a large illuminated area on an object demonstrates the opposite test from what we want: It shows which pixels are activated by illuminating an area. Conversely, we want to find the density or number of information-bearing effective vixels falling on an object, or impinging a surface. (e.g. property) We first must find the cross-dependency of each vixel, i.e. vixel degeneracy. Bottom row: The illumination area is effectively reduced to smaller than one pixel (by making the camera more distant, or using a finer laser beam). The laser dot is traced across a horizontal track around the object. Degeneracy occurs from reflection on the floor and on a mirror, where there is an ambiguity in determining the “system state” from the image alone.

thickness (Fig. 9ab). As a result, we could isolate and identify the various multiple reflections in a room or scene coming from other objects, caused by that light source point (Fig. 9cd).

The camera image vectors from all light source stimuli were background-subtracted, accentuated nonlinearly as \( f^4(x, y)_{\text{CAM}} \) to cause the high-intensity laser stimulus to dominate over camera noise, and then fed into PCA to identify the number of non-degenerate vixels, and in particular the non-degenerate vixels per unit area of the subject matter’s surface, not per unit area from the camera’s perspective.

For each surface segment, \( S_m \), it would be a long process to individually illuminate and test every single point on the surface in two dimensions. However, if we have an isotropic cross-dependency of vixels, we can scan along two orthogonal tracks \( T_1 \) and \( T_2 \). The number of significant PCA components, \( \Omega\{T_1\} \) and \( \Omega\{T_2\} \) are found separately for each track. We can then estimate the extrapolated number of significant PCA components (significant eigenvalues) for the entire surface as:

\[
\tilde{\Omega}\{S_1\} = \Omega\{T_1\} \cdot \Omega\{T_2\}
\]  

\( \tilde{\Omega}\{S_1\} \) gives the estimated number of effective vixels impinging the surface — that is, the effective veillance flux (\( \Phi_{VE} \)).
For the average effective veillance flux density (veillance intensity), in [vixels/m²], we divide by the surface area:

\[ \nabla_{VE} = \frac{\Phi_{VE}}{S_1} = \frac{\tilde{\Omega}(S_1)}{S_1} \]  

(8)

The veillance rate (effective) for the object’s surface [bits/s], simply uses the bit depth of the camera, \( \tilde{B} \) (number of bits for each pixel), and frame rate, \( r_F \):

\[ \nabla_{VE} = r_F \cdot \tilde{B} \cdot \Phi_{VE} = r_F \tilde{B}\tilde{\Omega}(S_1) \]  

(9)

Thus, we measure \( \tilde{\Omega}(S_n) \) to quantify the amount of veillance sensing, using the process of “Laser scanning vixel principal component density analysis” which requires:

- **Sufficient number of images/frames**: Sufficient images (or video frames) are needed in the experiment to independently test each hypothesized vixel. Otherwise, the PCA components will saturate at the number of video frames. That is, sufficiently many images/video frames are needed to give each potential effective vixel the opportunity to be expressed in a linearly independent vector of pixels.

- **Small test point**: The illumination test point is sufficiently small to spatially access individual physical vixels where they fall on the object’s surface. Otherwise, cross-illumination of independent vixels occurs, similarly to low SNR (signal-to-noise ratio), leading to an artificially low \( \Omega \).

See the process in Fig. 10, 11, 12. For example, when a 160x120 pixel surveillance camera was set up in a room, we tested the veillance striking the surface of a door. The veillance on the door surface was measured at 1877 effective
vixels per square metre, and the metric reduced in effective vixels per square metre when we placed various translucent materials between the camera and the door.

This process is distinct from measuring plenoptic functions, and BRDF (bidirectional reflectance distribution function) [14], because we are not finding the effect of light rays from arbitrary directions in illuminating subject matter (as used in computer graphics and animation), but instead are finding the effect of information on each point of an object’s surface, on each pixel of a camera. Furthermore, we are going beyond a simple input-output mapping, to determine a level of degeneracy in the detected vision of subject matter.

VI. VIXELS IN OTHER SENSING MODALITIES

The concept of vixels also applies to other types of sensors. A building’s temperature-control system might have two temperature sensors, in two separate rooms, creating two vixels of veillance in the building. Those two vixels may overlap slightly based on thermal diffusion between the two rooms. (equivalent to a blurring function in a camera)

In some cases, air or any other fluid can take on a more complex, dynamic motion (either laminar or turbulent motion), such as outdoors in the wind.

In fluid dynamics, the analogue of veillance rays in a fluid flow would be streaklines, as opposed to streamlines and pathlines. Veillance can take place when measuring temperature, chemical content, colour, etc. of the air, or any other fluid, sensing material that has flowed from another location according to laminar or turbulent flow.

For example, an atmospheric pollution sensor set up outdoors would perform veillance with one vixel; the vixel is a region extending outward from the sensor in an irregular or regular conical shape, according to the wind source. If the wind is blowing towards the sensor from the South-East, coming from London, then the sensor is performing veillance on London with one vixel of resolution.

Streaklines follow fluid flow according to each fluid element in time-reversed flow, time-reversed from the intersection with a particular point in space. The difference between streamlines, streaklines and pathlines is subtle [15], and it is interesting that there is a direct analogue to veillance.

VII. HDR (HIGH DYNAMIC RANGE) SENSING, CDR (COMPOSITE DYNAMIC RANGE) SENSING

We developed a method for sensing multiple dynamic ranges simultaneously [16] and an algorithm for compositing dynamic ranges of a waveform [17] into a combined high dynamic range. This initial work was designed for audio, as well as time-varying signals above and below the frequency range of human hearing.

Two configurations of this system, for simultaneous HDR sensing and CDR compositing, are:

<table>
<thead>
<tr>
<th>1 sensor feeds $M \geq 2$ ADCs</th>
<th>1 physical vixel (identical effective vixel)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M \geq 2$ sensors feed $M$ ADCs</td>
<td>Effective vixels: ranging from 1...M Desirably 1 effective vixel</td>
</tr>
</tbody>
</table>

In the latter case, it is desirable for the sensors to be co-located or sensitive to the same spatial location. If the sensors are not perfectly co-located in an acoustic field, acoustic waves will be slightly out of phase or attenuated from one sensor to the next. This discrepancy can be quantified in terms of effective vixels. For two sensor signals $x_1$ and $x_2$, we can define the number of effective vixels as:

$$v_E = 2 - |\rho_{1,2}| = 2 - \frac{|E[(x_1 - \mu_1)(x_2 - \mu_2)]|}{\sigma_1\sigma_2} \quad (10)$$

using the Pearson correlation coefficient $\rho_{1,2}$, where $\mu_1$, $\mu_2$, $\sigma_1$ and $\sigma_2$ are the mean and standard deviations of $x_1$ and $x_2$, respectively, and $E$ denotes expectation. Here, $v_E$ ranges from 1 to 2 vixels.

Empirically, we can test the cross-correlation:

$$v_E = 2 - \frac{\sum_{n=1}^{N} (x_1(n) - \bar{x}_1) (x_2(n) - \bar{x}_2)}{\sum_{n=1}^{N} (x_1(n) - \bar{x}_1)^2 \sum_{n=1}^{N} (x_2(n) - \bar{x}_2)^2} \quad (11)$$

This method requires a test measurement of the sensors in their linear regime, below saturation. This can be evaluated in a temporarily restricted dynamic range, smaller than the full capability of CDR/HDR sensing. More generally, for $M > 1$ inputs, the number of vixels can be empirically estimated using the PCA method described previously, i.e. estimating $v_E$ from $\Omega$.

A. CDR sampling for aircraft pitot sensors

We extended CDR/HDR audio by creating a system to combine the dynamic ranges of pitot airspeed sensors as used in aircraft. This novel system uses 2 vixels, for application on a typical aircraft with a speed sensor mounted on either side of the cockpit. These two vixels are correlated during ordinary forward-facing aircraft motion, when the forward motion dominates over the atmospheric turbulent flowfield. In this limit, the effective vixel count approaches 1.

We built one configuration using pitot sensors having different dynamic ranges, and another with two identical pitot tubes, to create resilience against icing conditions where one or both of the sensors may become partly blocked by ice. We devised an algorithm to dynamically detect and adapt to the drifting dynamic range responses of the sensors, if one of them becomes partly blocked or compromised.

This is an example of a novel “dynamic adaptive CDR/HDR” or “drifting-exposure CDR/HDR” system which adapts its assessment of the relationship between sensor exposure response functions, and the relationship between input dynamic ranges, while the sensor response functions drift in a stochastic manner over time.

VIII. HIR (HIGH IMPEDANCE RANGE) SENSING, CIR (COMPOSITE IMPEDANCE RANGE) SENSING

In this work, we introduce a sensing system which forms a composite signal over a wide range of acoustic or electric impedances. Impedance governs how waves propagate through
Imped., Acoustic

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Imped., Acoustic</th>
<th>Sensitive to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>geophone</td>
<td>high ((z = p/v))</td>
<td>vibr. in solid matter</td>
</tr>
<tr>
<td>hydrophone</td>
<td>medium</td>
<td>vibr. in liquid matter</td>
</tr>
<tr>
<td>microphone</td>
<td>low</td>
<td>vibr. in gaseous matter</td>
</tr>
</tbody>
</table>

Each sensor \(m\) has a transfer function \(H_m(f)\) describing its response in the frequency domain. The number of effective vixels can be defined by scanning this spectral response, and for two sensors, co-located and immersed in the same medium, \(v_E\) can be defined analogously to the correlation coefficient:

\[
v_E = 2 - \frac{\int (H_1(f) - \Pi_1)(H_2(f) - \Pi_2)df}{\int |H_1(f) - \Pi_1|^2 df \int |H_2(f) - \Pi_2|^2 df}
\]

Applications of HIR and CIR sampling include:

- Sensing sound generation/propagation in multiphase media, with a measuring instrument intended to contact a variety of media in different states-of-matter, or in which the phase is not known in advance;
- Sensing sound in chemical processes where a fluid’s chemical composition may vary across a continuum of acoustic impedances.

IX. Conclusions

We have developed a simple physical and mathematical framework for quantifying veillance, in terms of vixels, veillance intensity field, and veillance flux, which, when crossing borders (surfaces) of authority, can measure the relative amounts of surveillance and sousveillance. We have extended this concept to new sensing systems: composite dynamic range sensing and composite impedance range sensing. In summary, we have suggested that veillance can be a precisely measurable phenomenon, both by physical properties and by its social context.

---

1For acoustic signals, impedance governs the ratio of pressure to velocity in a wave. For electric signals, impedance in a medium governs the ratio of voltage to current. This follows the definition of characteristic acoustic impedance as \(z_0 = \rho_0c_0\) using \(\rho_0\) as density and \(c_0\) as the speed of sound in the medium, which creates an analogy of pressure to voltage and velocity to current.