Equiveillance: The equilibrium between Sur-veillance and Sous-veillance

Steve Mann,
University of Toronto
On the Identity Trail
May 2005

This is the text of the final pre-conference workshop topic, that leads into the Opening Keynote Address (a panel discussion) for Association of Computing Machinery (ACM) Computers, Freedom and Privacy (CFP)

Below I have put forth 10 issues that I hope we can address in the ACM opening keynote address, which will be a panel on equiveillance;
http://wearcam.org/anonequity.htm

Panelists are asked to either challenge (refute), or re-enforce (accept) these 10 predictions of an equiveillant society (see further, below).

I will begin with an introduction to equiveillance in both the abstract and normative sense, and also the practical matters of an equiveillent society, and what I see as the inevitability of equiveillance.

David Brin will respond to these predictions, in a predictive way (i.e. with imagination of what future societies might be like).

Latanya Sweeney will respond to the threats of surveillance and whether equiveillance can keep these threats in check (or whether it merely adds more cameras to the "fire").

Ivan Szekely will respond from the prespective of a state where inequiveillance is rampant, i.e. in the face of individuals lacking rights to access of surveillance data, should they resort to sousveillance of the state? Can equiveillance be a "fuse" or "circuit breaker" to protect us from a totalitarian state?

PREAMBLE: Legal, Ethical, and Existimological Questions associated with Sousveillance and Lifelong Personal Imaging, Video Capture and Incidentalist Imaging in the age of portable wireless technologies.

Surveillance is already the subject of more than 4000 peer reviewed scholarly article references on Citeseer, and is also the subject of an IEEE interntional conference. For a good survey article, see Gavrilla 99, who summarizes surveillance as the art, science, and technologies of "Looking at People". Surveillance is derived from French "sur" (above) and "veiller" (to watch). Typically (though not necessarily) surveillance cameras look down from above, both physically (from high poles) as well as hierarchically (bosses watching employees, citizens watching police, cab drivers photographing passengers, and shopkeepers videotaping shoppers).

Likewise Sousveillance, derived from French "sous" (below) and "veiller" (to watch), is the art, science, and technologies of "People Looking at". Sousveillance does not immediately concern itself with what the people are looking at, any more than surveillance concerns itself with who or what is doing the looking. Instead, sousveillance typically involves small person-centric imaging technologies, whereas surveillance tends to be architecture or enviro-centric (cameras in or on the architecture or environment around us). Sousveillance does not necessarily limit itself to citizens photographing police, shoppers photographing shopkeepers, etc., any more than surveillance limits itself along similar lines. For example, one surveillance camera may be pointed at another, just as one person may sousveill another. Sousveillance therefore expands the range of possibilities, without limitation to the possibility of going both ways in an up-down hierarchy.

With the miniaturization of cameras into portable electronic devices, such as camera phones, there has been an increased awareness of sousveillance (more than 30,000 articles, references, and citations on the word "sousveillance" alone), and we are ready to see a new industry grow around devices that implement sousveillance, together with a new sousveillance services industry.

Here are 10 Hypotheses that I hope we can address in the panel:

---

1. (techlaw). Sousveillance will become a major force and industry, despite initial opposition. Like surveillance, sousveillance technology will outstrip many laws, and will be another example of technology moving forward more quickly than the legal framework that grows around it.
2. (privacy). Over the past 30 years, sousveillance practice has raised many new privacy, legal, and ethical issues, and these issues will become central as the sousveillance industry grows.
3. (incidentalism). Sousveillance of the most pure form, is not merely the carrying around of a hand-held camera, but, rather, must include elements of incidentalist imaging to succeed. For this reason, camera phones, pocket organizers containing

cameras in them, and wristwatch cameras, for example, exhibit an incidentalist imaging effect not experienced with even the very smallest of handheld digital cameras. A device exhibits incidentalist imaging when it can capture images as well as perform at least one other important and socially justifiable function that does not involve capturing images. This "backgrounding" by another socially justifiable function is a technology that is essential for sousveillance to take root in most societies.

4. (accidentalism). Cameraphones, cameraPDAs, and wristcameras have brought sousveillance to a new level. The next major level is that which affords the user deniability for the intentionality of image capture. This feature may be implemented by a random or automated image capture, or by allowing others to remotely initiate image capture. In this way image capture becomes accidental, and this accidentalism affords the user with a strategic ambiguity when asked such questions as "are you taking pictures of me now"?
5. (nonwillfulness). Accidentalism will be taken to a new level when it can be a requirement of a role player, such as a clerk. Just as surveillance is hierarchical, thus creating an industry that can defend itself from criticism (e.g. "don't ask me why there's a surveillance camera in my store, I only work here"), sousveillance will also rise to this same level of deniability. Accidentalism by itself might be regarded as willful blindness. But when combined with, for example, a requirement to participate in sousveillance (e.g. sousveillance technology might, for example, become part of a clerk's uniform) accidentalism becomes nonwillful blindness.
6. (nonwillful blindness). Various forms of continuous incidentalist imaging will give rise to an industry behind products and services for continuous sousveillance. Continuous sousveillance will make sousveillance the norm, rather than the exception, for at least some individuals in society.
7. (protection). Unlike surveillance, sousveillance will require a strong legal framework for its protection, and not just its limitation. Along these lines, certain legal protections will be required to ensure access to those who depend on sousveillance.
8. (disabled). These legal protections will first emerge in the form of assistance to the disabled...
9. (differently abled). The space of those considered to be disabled will gradually expand, over time, as the technological threshold falls and the sousveillance industry grows.
10. (other benefits). These legal protections will expand, to encompass other legitimate and reasonable uses of sousveillance, such as artistic and technosocial inquiry, photojournalism, and collection of evidence.

Fundamental questions: The Mark of Authentication

Should people be able to buy or sell without the Mark of Authentication, i.e. should people be able to buy or sell without permission from anyone else? Can not a transaction be a private matter between two entities?

Is it reasonable or ethical to support the concept of a mandatory sales tax, or any other form of intervention into the right of two parties to privately engage in exchange of goods or services?

What does it mean to buy or sell?

If it is illegal to buy or sell without the Mark of Authentication (i.e. to illegal to buy or sell without permission from some other entity), then what forms of interaction remain legal?

There has been a recent trend to commodify everything from simply getting information (subscription based services) to the exchange of ideas. Even communication and interacation with others has been commodified. For example, if you want to just check the weather, you end up logging into some service. Public payphones are replaced with authenticated cellphones. Clock towers are replaced with authenticated time servers. To be able to know the time of day then becomes a commercial transaction. For example, the clock in my cellphone will not work if it can't get "service" (authenticate). Is communication (such as exchange of ideas) a form of commerce?

In a world where thoughts and ideas and communications are governed by micropayments, to define most activity as commerce, what should remain legally outside the scope of commerce?

If people help each other (i.e. farmers getting together for a barn raising) is that tax evasion? Should they all go to jail if they don't accept the Mark of Authentication?

If it appears that mandatory sales tax (permission-based buying and selling) leads to an eradication of anonymous transactions, what other forms of society, if any, could exist?

What about electronic toll collection, i.e. the need to engage in commerce in order to cross a bridge, or camp somewhere. Many public parks and even forests have a "fee station", i.e. a need to pay in order to move from one place to another. The global economy has actually built more borders rather than eradicate existing borders. Whether crossing a border, crossing a bridge, entering a forest, going for a swim, or taking a walk in a park, as these become commercial transactions, we need to accept the Mark of Authentication.

Is it possible for a non-commerce society to exist in practice? Would it be attacked by the commerce-based society's armies?

Is commerce necessary to the well being or functioning of a society? Even if it is not, how could a non-commerce society exist in the face of attack by disgruntled tax collectors?

If we're willing to accept the necessity of surveillance, i.e. the end of anonymity and privacy, should we build in a form of sousveillance as well? Should we simply give up privacy without also giving up secrecy. Why should, or should, individuals have to give up their privacy while organizations are allowed to keep their secrecy?

What mechanisms could be used to prevent one or more secretive organizations from corruption in building the surveillance networks?

Should there be some form of ``safety valve'' that allows the surveillance netork to ``break'' if it becomes too corrupt?

If so, how should this ``safety valve'' be constructed? Should it be built so that the surveillance network loses its secrecy, or so that it loses its effectiveness. That is, should the safety valve reveal the perpetrators of corrupt surveillance, or should it simply reduce the efficacy of the surveillance so that people can conduct anonymous interaction when the system becomes corrupt?

Or do we prefer the temporary safety of a Liquiface at the Oceana Beach Resort?

Human safety beach resort lounges might offer interaction through tamperproof computer consoles, consisting of interactive water jets in granite or marble slabs, with displays safely behind thick bulletproof glass. Not that the bulletproof glass would really be necessary since inhabitants would be naked, free of guns, or box cutters. This would be a software only world, all hardware being done only by soldiers. At the safe beach resort, there would be no objects with which to jam up the liquiface, and the only thing the terrorists could do would be to urinate or defecate or spit food particles into the liquiface holes, in which case, a self cleaning action could take place, by increase in water column from 2'' w.c. to maybe 33' (10m) w.c.. Authentication and keystroke monitoring of course would keep the soldiers safe from beach resort hackers. A noware sweatshop at the beach resort? All ideas would be welcome as long as they don't threaten the stability of the human safety utopia, however temporarily it would remain utopic.

Wildlife versus Livestock

Wildlife is free to pass through borders without authentication. Birds can fly from one country to another without a passport.

Lifestock must bear the Mark of Authentication in order to pass through borders. Cattle and sheep must be branded, marked, or submit to a biometric database before they are allowed to pass across a border.

Members of the wildlife community are free to help each other, and to form mutually beneficial relationships.

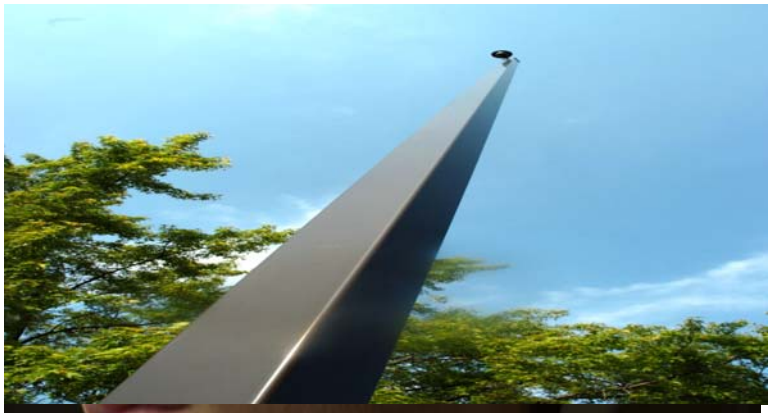
Members of the livestock community are only free to help each other but only if they also offer a portion of that help to their master. In order to facilitate the aforementioned "only if", all manner of help shall be quantized through an organizational mechanism known as "commerce".

```
Baa, Baa, Shee-eople
(Sing to your children, to the tune of Baa, Baa, Black Sheep)

Baa baa shee-eople,
Have you any cash?
Yes sir, yes sir, three bag stash.
One for my country,
One for my state;
And one for the little boy
With a high tax rate.
--S. Mann, 2004
```

Equiveillance in the new deconomy

Equiveillance is the balance (equilibrium) between surveillance and sousveillance.



Consider, for example, a balance between the left and right columns in the table below:

A comparison between surveillance and sousveillance

Surveillance	Sousveillance
God's eye view from above. (Authority watching from on-high.)	Human's eye view. ("Down-to-earth.")
Cameras usually mounted on high poles, up on ceiling, etc..	Cameras down at ground-level, e.g. at human eye-level.
Architecture-centered (e.g. cameras usually mounted on or in structures).	Human-centered (e.g. cameras carried or worn by, or on, people).
Recordings made by authorities, remote security staff, etc..	Recordings of an activity made by a participant in the activity.
Note that in most states it's illegal to record a phone conversation of which you are not a party. Perhaps the same would apply to an audiovisual recording of somebody else's conversation.	In most states it's legal to record a phone conversation of which you are a party. Perhaps the same would apply to an audiovisual recording of your own conversations, i.e. conversations in which you are a party.
Recordings are usually kept in secret.	Recordings are often made public e.g., on the World Wide Web.
Process usually shrouded in secrecy.	Process, technology, etc., are usually public, open source, etc..
Panoptic origins, as described by Foucault, originally in the context of a prison in which prisoners were isolated from each other but visible at all times by guards. Surveillance tends to isolate individuals from one another while setting forth a one-way visibility to authority figures.	Community-based origins, e.g. a personal electronic diary, made public on the World Wide Web. Sousveillance tends to bring together individuals, e.g. it tends to make a large city function more like a small town, with the pitfalls of gossip, but also the benefits of a sense of community participation.
Privacy violation may go un-noticed, or un-checked. Tends to not be self-correcting.	Privacy violation is usually immediately evident. Tends to be self-correcting.
There can be tendency to coverup corruption or illegal activity.	Honest mistakes tend to be exposed before growing into a coverup.
It's hard to have a heart-to-heart conversation with a lamp post, on top of which is mounted a surveillance camera.	At least there's a chance you can talk to the person behind the sousveillance camera.
There is no privacy. Get used to it!	There is no secrecy. Get used to it!

When combined with computers, we get ubiquitous computing ("ubiqcomp") or pervasive computing ("pervcomp"). Ubiq./perv. comp. tend to rely on cooperation of the infrastructure in the environments around us.	When combined with computers, we get wearable computing. ("wearcomp"). Wearcomp usually doesn't require the cooperation of any infrastructure in the environments around us.
With surveillant-computing, the locus of control tends to be with the authorities.	With sousveillant-computing, it is possible for the locus of control to be more distributed.

Eventually, we will probably end up with a combination of ubiq/pervcomp (surcomp/souscomp) and wearcomp (sousveillant-computing). There will eventually be some kind of equilibrium ("equivellance") between surveilance and sousveillance. We will wear or carry some but not all of the technology. Obviously we don't wear big batteries to run head-mounted lights, so there are some elements like shelter, lighting, electrical wiring, and plumbing (except for diapers which are wearable restrooms) that are best-served by the architecture. But new emerging technologies of miniaturization will shift the equiveillance (sur/sous equilibrium) a little more from architecture of buildings to human-scale architecure. I believe that the "heavy currents" like the 600 Amp 3phase service that comes into our building will stay in the architecture, whereas the "light currents" (informatic electrical signals) will move more and more onto and into the body. Thus the shift in equiveillance will be primarily informatic, encompassing also personal information like lifelong video capture "cyborglog" personal diaries.

Problems with inequiveillance

In the aftermath of inequiveillance, we must consider not just the Axes (of Evil), but also the point where the axes meet (called the Origin, i.e. Origin of Evil). In labeling others as evil, we must also keep our own house clean, and visible. Otherwise inequiveillance, which is the true Origin of Evil, is likely to result.

As a society, have we replaced community with reputation capital and money? To the extent that fame and fortune are fungible, and are thus two sides of the same coin, with surveillance, we no longer live in a small town where neigbors work together for a community.

A goal of sousveillance is to bring back that sense of small town community, in contrast to profiling and surveillance. Sousveillance (cyborglogging, etc.) tends to be distributed and less organized, or at least less hierarchical, and thus conducive to a small community in which individuals trust one another. Surveillance, on the other hand, as with profiling, often operates in secret, in the context of larger peer-anonymous communities, thus breeding mistrust, which itself breeds more surveillance, as a vicious

cycle. Not to forget, of course, the lack of inverse visibility that can lead to corruption of politicians who use secrecy to hide theft of public monies, and the like, in a surveillance-only society.

Understanding inequiveillance requires us to understand and appreciate that notions of secrecy are very different from notions of privacy, and that if we are to give up privacy, then we must and should also give up secrecy. Conversely as long as secrecy exists, so too should privacy.

As a corrolary to equiveillance, it should be reasonable for a person to keep their own record of their life experience, at least during times when they are under surveillance, so that each person can construct their own account of their own activity. To interfere with a person's own cyborglog would be to willfully destroy evidence that that person might need in the defence or prosecution of legal action. Therefore one who attempts to destroy or inhibit sousveillance should, at the very least, fall under the same kind of suspicion as one who inhibits surveillance.

References

- Continuous lifelong capture of personal experience with EyeTap, ACM Multimedia 2004, CARPE, pp1-21 (lead article), http://wearcam.org/carpe/carpe.pdf
- ``Sousveillance: Inverse Surveillance in Multimedia Imaging" Proceedings of ACM Multimedia 2004, pp620-627. http://wearcam.org/acmmm2004sousveillance/mann.pdf
- "Existential Technology," Leonardo 36:1, 2004 Leonardo Award for Excellence http://mitpress2.mit.edu/e-journals/Leonardo/isast/awards2004excellence.html
- Sousveillance, not just surveillance, in response to terrorism, Metal and Flesh (Chair et Métal, CM06, 01 Mar 2002.
- Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer, Steve Mann with Hal Niedzviecki ISBN: 0385658257 (Hardcover), Random House Inc., 304 pages, 2001.
- this paper is at http://wearcam.org/anonequity.htm

Acknowledgements

The author would like to acknowledge the support and help of Ian Kerr, University of Ottawa, the anonequity project and SSHRC.

In revising this article, the author is grateful for some good suggestions made by Dr. Stefanos Pantagis.