Declaration of Veillance (*Surveillance is Half-Truth*)

Steve Mann, Ryan Janzen, Mir Adnan Ali, and Ken Nickerson
Veillance Foundation, 330 Dundas Street West, Toronto, Ontario, Canada M5T 1G5

***Abstract*—A core problem humanity faces today—underlying failing economies and governments, widespread corruption, and systems interoperability disasters—comes from a lack of integrity. We live in a world where organizations seek to know everything about us, yet reveal substantially nothing about themselves. This is a world of hypocrisy, which is the opposite of integrity. Hypocrisy is evident in entities which use surveillance cameras, while simultaneously forbidding others from taking pictures, or wearing a camera, such as a computer-based seeing aid. This combination of watching and concealment establishes a condescending or abusive dynamic. In terms of "Games People Play" from the theory of Transactional Analysis, this is what psychologists call a "We're OK, you're not OK" relationship. In response to these one-sided "(sur)veillance games" our governments and industry leaders impose on us, we propose key principles for information-gathering, reporting, and sensing (*i.e.* "veillance") under control of all individuals — The Declaration of Veillance, Version 1.0.**[1]

> "Why do cars and buildings ALWAYS have the right to wear cameras, but people sometimes don't?"
> — Stephanie, age 7, in response to her father being physically assaulted at a McDonalds in Paris, France, for wearing a computerized seeing aid [1].

I. Introduction

We're surrounded by a rapidly increasing number of sensors [2]. Entire cities are built with cameras in every streetlight [3]. Automatic doors, handwash faucets, and flush toilets that once used "single-pixel" sensors now use higher-resolution cameras and computer vision [4]. Surveillance is widely used without regard to genuine privacy, only Panoptic-privacy [5].

There are two forms of sensing/watching/sight/veillance:

English word	*French word*	*Meaning*
Oversight	**Surveillance**	Watching by the authority
Over	**Sur**	Authority
Under	**Sous**	Individual
Undersight	**Sousveillance**[2]	Watching by individuals

In the context of Transactional Analysis [8], popularized in *Games People Play* [9], we examine the psychologically condescending, one-sided relationship of surveillance being allowed but sousveillance forbidden, compared to more mutually beneficial coveillance [6], where surveillance and sousveillance equiveillantly co-exist ("*veillance juste*", *i.e.* "fair sight").

As cameras are embedded into everyday things and "wearables," it becomes fruitless to try to stop people from recording. Such policies will fail [10], and only burden those who need cameras to see and understand their world. Many kinds of devices can enable veillance, such as a wearable computer with a camera and display. The display allows the unit as a whole to become a realtime *seeing aid*, as opposed to a mere *recording device*. Just as the justice system must allow evidence from both sides, having *veillance* in the hands of both the powerful and the weak serves a human need for truth and understanding, as well as human health and safety[3,4] (Fig. 1).

[1]Join us by emailing veillance@eyetap.org and help draft Version 2.0!

[2]Sousveillance [6][7] is also called "Quantified Self" or "Body Hacking".

[3]*E.g.* Martha Payne, age 9, banned from photographing the poor-nutrition lunches she was served by her school in Scotland, fought back and won.

[4]Photographic monitoring of dietary intake in US Pat. App. 20020198685.

Fig. 1: Establishments often use surveillance while prohibiting sousveillance. Principles of justice are needed, as symbolized by Lamb versus Lion, in "*Equal Before the Law*", a sculpture by Eldon Garnet (photo, Mark Stiegel). When the Lion prohibits the Lamb from recording its own evidence, courts only see the Lion's side of the story—a half-truth.

Courts demand the whole truth, but surveillance is only a half-truth. Surveillance being half-truth becomes apparent once we recognize the hypocrisy of widely-used surveillance, combined with strong prohibitions on personal seeing and memory aids. The opposite of hypocrisy is integrity; thus, this half-truth embodies a lack of integrity.

II. Declaration of Veillance

Veillance freedom is the right for all humans to:

1. **See**, both literally and metaphorically, *i.e.* "sense";
2. **Understand** what they see/sense;
3. **Remember** what they sense (*e.g.* record); and
4. **Share** and describe their memories to others.

Thus, these four freedoms correspondingly imply:

1. A seeing aid (sensing aid) should never have restrictions greater than those enforced on recording-only devices. Such restrictions unfairly inhibit the ability to see in realtime;
2. A sensing aid may use computation to help understand the environment, *e.g.* use synthetic synesthesia to highlight hazards, show directions, sense radiation, see radio waves, or sense sensors (*veillametrics*) [16][11][12][18];
3. We must have the inalienable right to record when: *(a)* under threat, *(b)* being detained, *(c)* expected to be held accountable for our actions, and *(d)* for health care, *e.g.* one's own biosignals, mindfiles [13], and memories [14];
4. The right to share one's life experiences, *e.g.* tell one's life story; transmit health data to a physician; transmit for personal safety, to prove an alibi, or to preserve "bemes" [13].

III. Surveillance is a Half-Truth; Veillance is the Whole Truth

We live in a world where journalists and ordinary citizens are arrested for photographing those in authority, and risk being murdered for revealing corruption. On the other hand, embedded journalists with military or police can't be objective, as there is an inherent conflict-of-interest. In this sense they become police or military accomplices, *i.e.* bedfellows ("embedfellows") with their sponsor organization, merely conveying propaganda. Journalists often come under attack, threatened with violence for being honest. Accurately recalling and reporting what we see, is an act of integrity in itself: data integrity coincides with moral integrity. This gives rise to the following observations.

Ordinality: Persons have a stronger right to see than things. Protection of human life (*e.g.* via wearable cameras) must be allowed, wherever protection of things is allowed (*e.g.* merchandise protected by surveillance cameras).

Equiveillance: Persons must have the right to record while being recorded, since if sousveillance is prohibited, surveillance is only a half-truth. In legal proceedings, if either the plaintiff or defendant was prevented from recording evidence of the alleged crime, then the opposing party's recorded evidence should be inadmissable in court.[5] Any party may record, unless a non-recording contract comes into effect:[6]
(i) Party A warrants their recording won't be used against B,
(ii) Then, and only then, Party B agrees to cease recording.

'Smart People': "Since we have...smart lightbulbs, smart toilets, smart elevators, ...why not have 'smart people'—people equipped with information processing hardware?" [15]. People have moral agency; mere "things" do not. *"Veillance By Design"* is reliable, observable, and verifiable—unlike mobile phones leaking data about their users, imaging devices and software detecting "EURion constellations" and refusing to function, or school-issued laptops spying on students in the privacy of their own homes (*Robbins v. Lower Merion School District*). Tools must serve their users first. (Humanistic Intelligence before Machine Learning and Artificial Intelligence.)

Seeing both points-of-view: All modern law is built on the famous Latin phrase: *Audi alteram partem* (literally "hear the other party", usually translated "hear both sides"). Notionally extending this concept from testimony to evidence, we then have *Vide alteram partem* ("see..."). More correctly, we have "***Vide de habitaculo alteram partem***", meaning to see from the other's point-of-view, *i.e.* see both points-of-view.

Making it real: As engineers, scientists, and inventors, our research team is developing *open science* technologies[7], so genuine privacy and veillance can coexist with commerce, politics, and other activities [10].

IV. Ambiguous Vision and "Veillance Games"

As an artistic, scientific, and technological advancement to better understand and quantify vision, *veillametrics* was introduced [11][12], revealing *veillance flux* from cameras, as the cameras' ability-to-see moves and reflects through rooms, buildings and streets [17][18]. The result is an IoV ("*Internet of Veillance*"), including both the IoT (Internet of Things—surveillance), along with "Wearables" (sousveillance).

Our governments and industry leaders hide their surveillance cameras in opaque black hemispherical metal masks behind smoked plexiglass domes so we can't see which way the camera is looking. In response to this dystopian world, we create gaming scenarios where players follow this example: each wears a dark acrylic sphere that completely encapsulates their head to hide which way it is facing, hiding wearable cameras [19]. With this *ambiguous veillance* you try to secretly photograph without getting caught. The game symmetrizes behavioural modification issues raised in Milgram's studies on obedience, Zimbardo's *Stanford Prison Experiment*, and in [20]. You are given a terrometer / lethiometer (www.wearcam.org/eleo/), and a veillance dosimeter [17] that measures and displays your "dose" of veillance flux—how much you are being photographed. You use this knowledge and meta-knowledge of veillance flux to compete for prizes:
- most passively scopophilic (seeking veillance flux); and
- most scopophobic (avoiding veillance flux).

[5] Receipt analogy: When you buy something, you have a right to get a receipt, so both parties have evidence of the transaction. If only one party is allowed to have a copy of the transaction, they can't prosecute the other party.

[6] Both parties may record the statement of the contract, since it may be oral.

[7] Videscrow, Priveillance, NotRecord, AlibEye, and dTaz, to adichotomize: Copyright v. Subjectright; Security v. Suicurity; Sur- v. Sous-veillance.

V. Oversight is half-truth without undersight

Society must reject one-sided evidence where an opposing party's evidence has been destroyed or forbidden. We must reject: (1) subjugation of human sensing; (2) cartels on cognition; (3) monopolies on memory; and (4) hegemonies on history. Regardless of whether or not we need assistive devices to help, in daily life humans need to: (1) see and sense properly, (2) understand our surroundings, (3) remember what we see/sense, and (4) share what has happened with others. Public or private entities that record you, while requiring you to ask permission before you use your own camera or other sensory aid, are hypocrites, abetting the half-truths of evidence spoliation, and putting health and safety at risk. Courts demand the whole truth, but evidence obtained through a lack of veillance equality is a half-truth, and must be inadmissible.

Join the Veillance Foundation and help put an end to half-truths, by emailing us at **veillance@eyetap.org**.

References

[1] S. Mann, "McVeillance," *www.webcitation.org/6Cb7y7KRb*, 2012.

[2] D. Cardwell, "At Newark Airport, the lights are on, and theyre watching you," *New York Times*, 2014 Feb. 17.

[3] F. Spielman, "Infrastructure Trust launches plan to overhaul Chicago's outdoor lights," *Chicago Sun-Times*, 2015 September 17.

[4] J. Iott and A. C. Nelson, "CCD camera element used as actuation detector for electrical plumbing products," *Can. Pat. 2602560*, 2012 Apr. 24; see also WO 2012043663 and US Pats. 6671890 and 8162236.

[5] Staff reporters, "Cameras can stay in Talisman's locker room, says [privacy] commissioner," *CBC News*, 2007 Mar. 22, Acc. 2015.

[6] S. Mann, J. Nolan, and B. Wellman, "Sousveillance..." *Surveillance & Society*, vol. 1, no. 3, pp. 331–355, 2003.

[7] V. Bakir, *Sousveillance, media and strategic political communication: Iraq, USA, UK*. Continuum International Publishing Group, 2010.

[8] E. Berne, *Games People Play*. Penguin, 1964.

[9] T. Harris, *I'm OK–You're OK*. Harper Perennial, 2004.

[10] M. A. Ali and S. Mann, "The inevitability of the transition from a surveillance-society to a veillance-society," in *Technology and Society (ISTAS), 2013 IEEE International Symposium on*, 2013, pp. 243–254.

[11] R. Janzen and S. Mann, "Veillance flux, vixels, veillons: An information-bearing extramissive formulation of sensing, to measure surveillance and sousveillance," *Proc. IEEE CCECE*, May 4-7 2014.

[12] R. Janzen, S. N. Yasrebi, A. J. Bose, A. Subramanian, and S. Mann, "Walking through sight: Seeing the ability to see, in a 3-D augmediated reality environment," *Proc. IEEE GEM*, pp. 313–4, 2014.

[13] M. Rothblatt, *Virtually Human: The Promise—and the Peril—of Digital Immortality*. Macmillan, 2014.

[14] ——, "Alzheimer's cognitive enabler," 2010, Canada Patent 2737183.

[15] S. Mann, "Introduction: On the bandwagon or beyond wearable computing?" *Personal Technologies*, vol. 1, no. 4, pp. 203–207, 1997.

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

[17] R. Janzen and S. Mann, "Veillance dosimeter, inspired by body-worn radiation dosimeters, to measure exposure to inverse light," *Proc. IEEE GEM*, pp. 267–9, 2014.

[18] S. Mann, R. Janzen, S. Feiner, J. Hansen, S. Harner, S. Baldassi, and M. A. Ali, "Wearable computing, 3d aug* reality, photographic/videographic gesture sensing, and veillance," in *Proc. ACM Tangible and Embedded Interaction (TEI2015)*, 2015, pp. 497–500.

[19] S. Mann, "Personal safety devices enable "suicurity"," *Technology and Society, IEEE*, vol. 33, no. 2, pp. 14–22, 2014.

[20] M. A. Ali, J. P. Nachumow, J. Srigley, C. D. Furness, S. Mann *et al.*, "Measuring the effect of sousveillance in increasing socially desirable behaviour," in *IEEE Tech. and Society (ISTAS)*, 2013, pp. 266–267.