Veillance Integrity by Design

A new mantra for CE devices and services.

By Steve Mann

Take a look at your grandparents' radio (Figure 1). What was most remarkable about it was what was "behind the scenes." Take a look at the back. It was probably easily removable, or, more often than not, maybe it didn't even have a back. It was completely open (Figure 2).

OPEN AND TRANSPARENT BY DESIGN

Inside, it probably used user-replaceable parts like "electronic lamps" (vacuum tubes) in sockets so you could easily unplug the parts to replace them. And the radio probably had a list of the parts in it, like in Figure 3(a). You could use parts from almost any manufacturer in another manufacturer's radio because all the parts were interoperable.

Many of these parts were inside transparent glass envelopes. These electronic lamps were like the environmentally recyclable (just metal and glass) light bulbs that many governments have banned in favor of more toxic light bulbs containing mercury and less-recyclable components. You could literally look inside the radio, and even inside these "lamps," and see and understand how everything worked.

Stapled or glued to the inside panel, there was often a schematic diagram [Figure 3(b)]. This "skeleton" outline laid bare all the secrets of the radio's inner workings. To get it, you didn't have to do anything special, like sign up to become a developer. It was there for everyone to see. Whereas most of the lamps (vacuum tubes) were transparent, perhaps by chance, the important thing here is that the manufacturer expended extra special effort toward transparency by including the schematic diagram as well.

FIGURE 1. Consumer electronics with integrity: A 1951 Westinghouse model 1951 6-T-104 table radio.

Whoever bought the radio probably paid cash for it, and the radio manufacturer or vendor probably did not know or collect any personal information about the buyer. The maker and seller of the radio probably didn't even know who the buyer was (although we should note that, in the early days of radio, government licensing was in some ways more stringent). So here we had a situation where the owner of the radio knew everything there was to know about the radio, without revealing anything about himself or herself.

FIGURE 2. An open design with nothing to hide. The radio is open at the back so you can look right in and see all the parts inside it. The "electronic lamps" (vacuum tubes) themselves are transparent so you can see into them as well.

The fact that this radio is not in landfill in a waste dump but instead is still working to this day, 64 years after it was made, is a true testament to its excellent design, ease of use, and ease of repair [1]. Transparency, interoperability, serviceability, and repairability are important aspects in which this radio is more sustainable than most of today's consumer electronics (CE) devices. The world of computing was once also this way too. In 1977, my Apple II computer came with a schematic diagram, parts list, and source code listings of its firmware.

But modern CE lacks these open and transparent design principles. Today, CE is often designed for landfill, in a throw-away society that not only creates garbage but also fails to create the scientists of yesteryear. Being able to understand the world around us helps foster a natural sense of curiosity and inventiveness. A child growing up with a radio like this is more likely to learn about radio and take an interest in things like the pentagrid converter and principles like superheterodyne radio signal reception simply because it is all plainly visible and easy to understand.

Digital Object Identifier 10.1109/MCE.2015.2484879
Date of publication: 16 December 2015

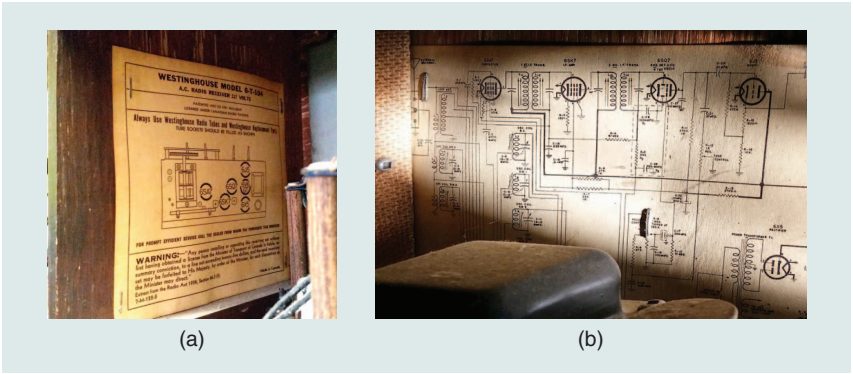

FIGURE 3. A close-up view looking into the open back of Figure 2: (a) on the left side there is a parts list; (b) on the right side there is a schematic diagram that explains how the radio works and teaches its design and principle of operation to anyone who wishes to learn more about the product and how it works.

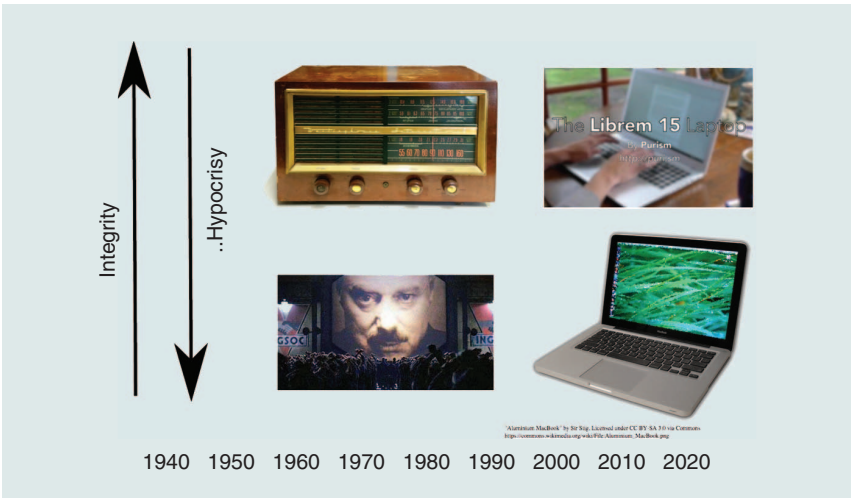

FIGURE 4. CE devices used to transparently reveal their principle of operation, but now devices spy on us while hiding their operating principles. This is a form of hypocrisy. In the late 1940s and early 1950s such hypocrisy was the domain of dystopian science fiction works like the book and movie Nineteen Eighty-Four. The opposite of hypocrisy is integrity. CE products like the Librem laptop computer embody the intergrity that most laptop computers lack.

When you buy something now, not only does the product reveal nothing about itself, but the seller and maker want to know everything about you.

GAMES PEOPLE PLAY

Games people play, you take it or leave it
Things that they say, just don't make it right
If I'm telling you the truth right now, do you believe it?
Games people play in the middle of the night

—"Games People Play,"
Alan Parsons Project, 1980

We can look at this situation in terms of transactional analysis (the "games people play") since the relationship between the surveilled and the surveillors may be thought of as human relationships gone awry. The seller or manufacturer takes on the role of parent, and this causes an inherent clash when an adult enters the space and doesn't want to be an "I'm not okay, and you're okay" child.

Those of us who play the role of child fit perfectly well into the (abusive) relationship the vendor or seller is providing, but those of us who want to think on our own, independently, will clash with this model. This is what psychologists call the "I'm okay, and you're not okay" form of interaction, in which the manufacturer sees others in life as inferior. Thus, surveillance is conducive to abuse.

The best situation is "I'm okay, and you're okay," which can never happen with surveillance. In this way, according to transactional analysis, surveillance is inherently flawed by its very nature. Only veillance can achieve the desirable "I'm okay, you're okay" state of the four possible states in transactional analysis.

INTERNET OF SURVEILLANCE

Author's note: This section and the following sections come from various discussions [2] during the 2013 IEEE International Symposium on Technology and Society (ISTAS, http://veillance.me) and subsequent 9 September 2015 meetup [3] with input from Ryan Janzen, Mir Adnan Ali, and Ken Nickerson.

There is an inherent hypocrisy in CE devices that run closed-source operating systems and are shrouded in secrecy while they also collect increasingly more information about us. What can we do to create a new class of CE devices that embody integrity by design?

Consider the examples shown in Figure 4, two from around 1950 and two from around 2015, i.e., roughly 65 years ago and today. Back then, integrity was the norm. Today, hypocrisy is the norm, with closed-source products being a lot more common than good-quality products like the Librem 15 computer, which embraces integrity by design. We're surrounded by technologies of surveillance and sensing that, by design, are getting harder to understand.

DON'T CENSOR THE SENSING OF SENSORS [4]!

The cameras in toilets, urinals, and faucets, first one-pixel sensors, then 128-pixel or 1,024-pixel sensors, are growing more intelligent (Figure 5) [5]–[8]. Other fixtures like streetlights and appliances are also using built-in, hidden cameras, e.g., outdoor LED lighting and embedded, invisible closed-circuit television [9] and Cisco Smart+Connected City Lighting [10].

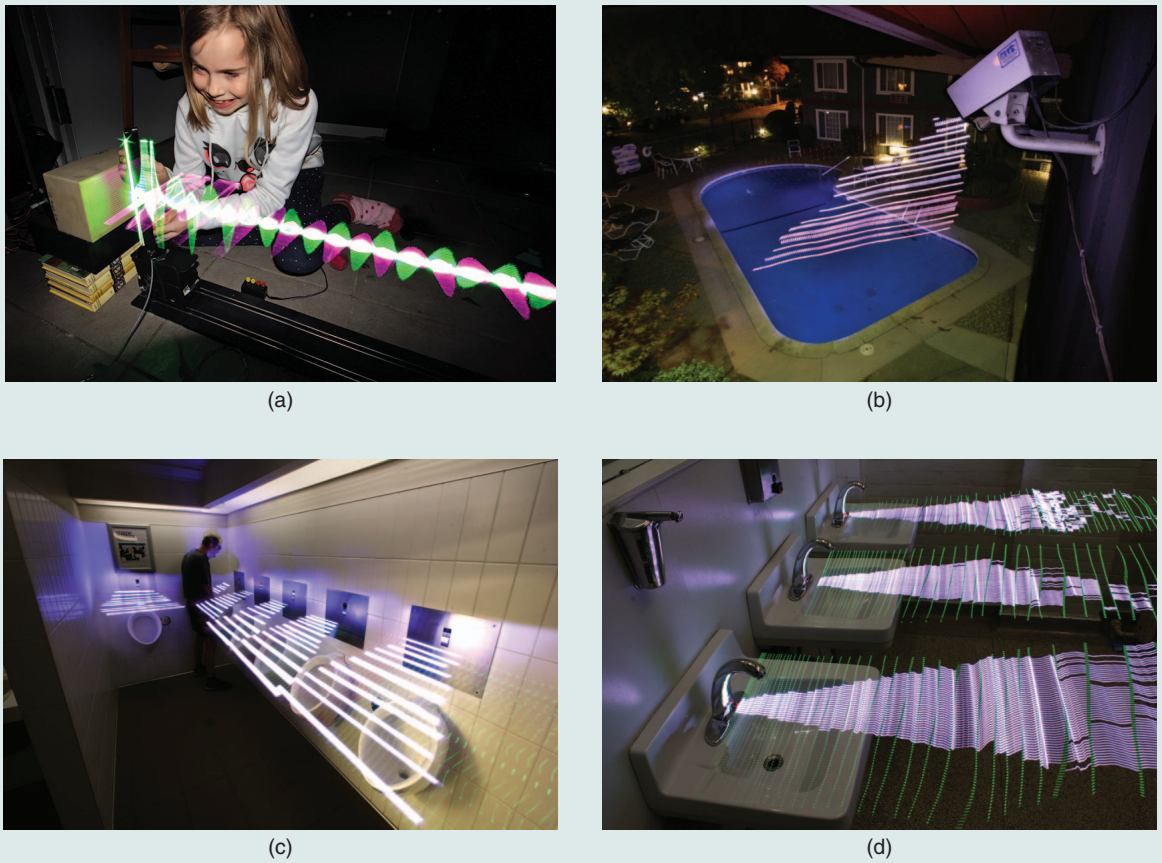

FIGURE 5. (a) Stephanie Mann, age 9, with a metasensing robot she built to see "sitting waves" (like standing waves but not alternating). Metasensing made visible the otherwise invisible electromagnetic wave propagation from a microwave radar-based motion-sensing burglar alarm. Metasensing is the sensing of sensors and their capacity to sense. (b) Liquid surveillance: Seeing a camera's capacity to see. (c) and (d) Surveillance even extends into our public washrooms where sensing devices detect if our hands are present to operate the taps.

SURVEILLANCE IS A HALF-TRUTH; VEILLANCE IS THE WHOLE TRUTH

Daddy, 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 McDonald's [11] in Paris, France, for wearing a computerized seeing aid.

Surveillance and dictatorships are examples of things that are hierarchical or centralized and thus provide only one side of the picture, i.e., the picture as viewed only from the top of the hierarchy. As Kevin Kelly writes in *Out of Control*, democracy and the free market are examples of things that are decentralized and distributed: "the network is nearly synonymous with democracy or the market" [12].

Courts demand the whole truth, but surveillance only provides a half-truth. This half-truth embodies a lack of integrity that becomes most apparent when surveillance is widely used but personal seeing and memory aids are prohibited. We humans are not good at half-truths. Stories have a beginning, middle, and end. Every truth exists within a certain context. When we don't have the full story, things don't make sense. Therefore, surveillance is unsatisfying, unfair, and unjust. We need a veillance that is more fair and just than surveillance. In this day and age, wearable cameras are easy to hide, so it is pointless to try to stop people from secretly recording. Policies against wearing cameras are doomed to fail [13] and only burden those who need camera systems to see and understand their world. I live in the future. I'm facing these issues daily. Soon, you will too.

DECLARATION OF VEILLANCE

Join me in supporting this declaration of your future rights. We should demand the right for the whole truth. Veillance freedom is the right for all humans to see, understand what they see, remember what they see, and be able to describe what they see to others.

- *See*: A seeing aid (e.g., a wearable camera with a wearable display) should never be less allowed than a recording-only device. Otherwise, we have selective enforcement against a seeing aid versus just wearable cameras that don't help people see in real time; likewise with a general-purpose sensory aid.
- *Understand*: A seeing aid can include a networked wearable computer, for sense making, in support of understanding sensory data in real time.
- *Remember*:
  - You have the right to secretly record while under duress or potential threat.

- You have the inalienable right to record while being detained.
- You have the right to record if you are going to be held accountable for your actions.
- You have the right to record for health care, e.g., record your heart [electrocardiogram (ECG) waveform] together with pictures or video to determine environmental factors leading to stress and possible danger.

▼ *Share that memory with others*: You have the right to share your own life experiences, to tell your life story, e.g., to your physician for health monitoring, or for personal safety, to provide an alibi, etc.

ORDINALITY

People should have more right to see than things. Protection of human life (e.g., by wearable cameras) should be allowed wherever things are protected (e.g., by surveillance cameras).

EQUIVEILLANCE [14]

Equiveillance means that you have the right to record while being recorded. Surveillance (oversight) [15] is a half-truth if sousveillance (undersight) is prohibited [16].

VEILLANCE CONTRACT

Inadmissibility of tampered (one-sided) evidence—all parties may record until a nonrecording contract comes into effect: Party A agrees not to use its recordings against Party B. Party B agrees to cease recording. Receipt analogy: when you buy something, you have the right to ask for and receive a receipt, if you want it, so that both parties have a recording (written) of the transaction. If only one party (e.g., the store) is allowed to have a copy of the transaction, that party should not be able to prosecute the other party, who is not allowed to have a copy.

RIGHTS AND RESPONSIBILITIES

To the extent that these rights may incur responsibilities that require new approaches (e.g., maintaining confidentiality and managing impacts on other parties), we wish to be involved in shaping a future where privacy and veillance can coexist with business, commerce, and other activities affected by veillance.

MAKING IT REAL

We're engineers, scientists, and inventors. We want to create a better future through our technologies, like Videscrow, NotRecord, AlibEye, and dTaz.

"IoT" SHOULD MEAN "INTERNET OF TRUTH" AND INTEGRITY

We live in a world where journalists and ordinary citizens are arrested for photographing police and where reporters are murdered for revealing corruption. Embedded journalists with the military or police, e.g., cannot be objective because there is an inherent conflict-of-interest, rendering them subject to merely conveying government propaganda. In this sense, they become police or military shills, i.e., bedfellows ("embedfellows") with the organizations they're reporting on.

True journalists with integrity often come under attack, threatened with violence for being honest. To the extent that we're all journalists in the "Web 3.0" (cyborgspace) era of the Internet, the very act of remembering and reporting what we see sometimes gets us into trouble [17]. See, e.g., [18] and [19] for instances of police limiting the public's right to record.

Cameras are borne by cars (with dashcams), buildings, light posts, and many other objects. In some sense, these inanimate objects have been given the gift of sight.

Acting with integrity means remembering what you did, so you can live your life by certain principles. Criminalizing sight and remembrance is, therefore, a direct blow to integrity. Whom do you call when you see a police officer breaking the law or a corrupt oversight official committing murder? Every government and major corporation employs professional security services and extensive surveillance. But who is watching them?

A PERSONAL NARRATIVE

For more than 40 years (since my childhood in the 1970s), I've been inventing, designing, and building wearable augmented reality camera systems to help me see and understand the world around me. But I find myself under attack for merely wearing a camera or trying to see and comprehend the world. I'm not an activist, but I've unwittingly (and in some sense unwillingly) bumped into the soft underbelly of a rapidly growing monster in our midst.

Back in the early 1990s when I was a student at the Massachusetts Institute of Technology (MIT), the first thing I wanted to do when I got there was swim in the Charles River, but I was warned that the water was dangerous due to pollution from Polaroid Corporation's chemical plant located upstream from MIT [20]. Since I couldn't swim in the river, the next thing I tried was some photography of the Polaroid building, a historical art deco landmark about 1.7 mi upstream from MIT. I was physically assaulted by Polaroid's security guards merely for trying to photograph the building. They seemed to have a lot of surveillance cameras mounted to their building, perhaps to make sure that nobody takes pictures of it. The guards seemed to think that they owned not only their building, but the surrounding public property, claiming that I was not allowed to photograph their building, even if I was on public property.

On my first day of class at MIT, one of my professors (who also worked in Polaroid's vision research laboratory) walked around the class, shooting a close-up picture of each of the students in his class, without any advance warning. I recall covering my face with one of my books, kind of half disturbed and half laughing at the hypocrisy of it all. This experience led me to later formulate the concept of humanistic property [21], i.e., if we're not allowed to photocopy textbooks or take pictures of art works (like Polaroid's art deco building), why should others be allowed to photograph us?

Polaroid was a big supporter of ID cards and surveillance, watching everyone, and helping other large organizations watch everyone. But hardly anyone was watching them. This hypocrisy is nothing new, but it has now grown to a scale that affects everyone, constantly.

HANDLING THE HYPOCRISY

While governments and large corporations want to know everything about us, they reveal very little about themselves. Their workings are often shrouded in secrecy. Ordinary people are placed under ever-increasing surveillance. At the same time, those who are conducting the surveillance—and polluting our air and water

supplies and otherwise placing us in danger—use threats, intimidation, bribery, and surveillance itself to avoid scrutiny and to scrutinize those who scrutinize them. In this way, surveillance allows parties in power to keep any opposition in check.

Edward Snowden revealed that governments in the Anglosphere [22] are placing their own citizens under surveillance, watching nearly everything we do. And secret evidence is increasingly used in a range of legal proceedings in the United States, the United Kingdom, and Canada, meaning that cases are being decided on the basis of "evidence" that lacks the benefit of counsel to challenge or question that evidence.

This hypocrisy—watching you while prohibiting you from watching them—threatens your physical safety, socioeconomic stability, the integrity of health care, and the very foundations of a fair, just, and stable society. The surveillance industry embraces and embodies this kind of hypocrisy: watching us while remaining hidden from being watched. Many establishments that record us prohibit us from recording them (Figure 6).

The opposite of hypocrisy is integrity. Surveillance without integrity only creates temporary stability and temporary security from low-level street crime. Such surveillance does not protect against larger crimes and corruption and, in fact, may actually be the cause of it (see the discussion of ladder theory in [23] and [24]).

Those in positions of power or authority over us—e.g., politicians, police, and clergy—are often people very much like us: most are good, but a few of them are "bad apples." How do you protect yourself from a few bad apples? Police, for example, are more likely to be on the side of other police and security professionals in any dispute that may arise.

Sensors such as surveillance cameras are all around us to protect merchandise, buildings, and other property. The surveillance is constant, and the surveillors never have to ask our permission. One way we can protect ourselves is to put sensors on our bodies to monitor our own health, wellness, and the surrounding environment.

Those who require us to ask permission before recording our own bodies (including our senses) place us in danger and raise

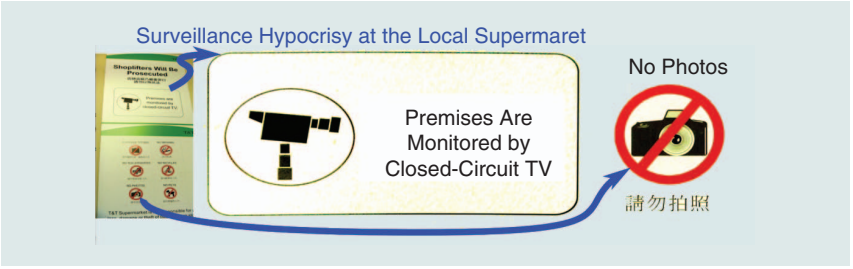

FIGURE 6. Surveillance hypocrisy at the local supermarket!

FIGURE 7. HEADome interactive art sculptures (S. Mann, 2013).

health-care costs for our society. If we have to ask permission to put sensors on our own bodies, the result will be an inability to protect ourselves from danger, health risks, and even our own failing eyesight (as can be done with a computerized seeing aid) as well as from others (e.g., as might be needed to defend ourselves in a court of law or prove our own story of what happened).

To bring balance, fairness, and stability to society, I propose the Veillance Contract: people should be able to make their own recording while they are being recorded. If a telemarketer calls you and says, "This call may be recorded for quality control and training purposes," the word "may" can be taken at both of its meanings, i.e., the call could be recorded and also you could record the call too, if you like. Just as you get to keep a copy of any contract you sign, you have a right to record any transaction in the same medium (text, audio, video, etc.) as the other party. If a person is denied this ability, then recordings of him or her should not be able to be used against him or her. We must be able to uphold this Veillance Contract to protect ourselves from recordings being used out of context [25].

If we don't follow the Veillance Contract, here's the horrible world we all might need to live in, walking around like space aliens:

Security by example—Our government and industry leaders watch us through cameras hidden in dark spherical domes with dark shrouds inside, so we can't see which way the cameras are facing. Imagine how absurd the world would be if we followed their example and walked around with dark globes over our faces so nobody (including them) could see which way our heads were facing (Figure 7).

GENERAL PRINCIPLES, TENETS, AXIOMS, AND POSTULATES OF THE VEILLANCE FOUNDATION

PEOPLE MUST BE ALLOWED TO SEE AND UNDERSTAND THEIR WORLD

Our eyesight and memory can fade with age. Just as hearing aids have become

computerized, our seeing aids (eyeglasses) and memory aids are becoming computerized. Will people be physically assaulted for wearing or using such seeing and memory aids? Consider the range of applications—from the completely blind, who record their day and have others help them later "remember" what they saw (or guide them remotely from a live transmission), to those of us who simply need a seeing aid that works like a simple magnifier, image stabilizer, or visual memory aid [26] in real time.

PEOPLE ARE WORTH MORE THAN THINGS (SUCH AS MERCHANDISE)

To the extent that certain counterveilling forces, such as privacy, are required to limit veillance, it should never be the case that merchandise or that which is in plain sight (e.g., retail business) is given a higher value than human life and health. If cars and buildings can "see," then so should people (e.g., with a seeing aid at least as capable as those of cars and buildings). And we must not create a world where things know everything about us and reveal nothing about themselves. We must change the Internet of Things (IoT) to the Internet of Open Things or the Internet of Integrity.

VEILLANCE WITH INTEGRITY BRINGS SAFETY

Since wearing a computational seeing or memory aid can result in physical assault, there needs to be a way for the seeing aid to capture evidence of the assault, especially when the assault is perpetrated by owners of surveillance cameras, where there is an inherent conflict of interest (e.g., in an establishment where surveillance is used but recordings might be deleted by the perpetrators).

VEILLANCE WITH INTEGRITY HELPS ESTABLISH FACTS

Rapidly expanding one-sided surveillance leaves us vulnerable to false accusations and suspicion from surveillance taken out of context. We need to have the right and ability to exonerate ourselves from false accusations or suspicion. For example, if we're going to be held responsible for our actions, we should be able to create an alibi, e.g., through systems such as AlibEye.

The AlibEye System is just one of the many projects the Veillance Foundation will undertake to help build a world of integrity. People need to be able to defend themselves and argue their own case, with their own data, not just random data from other parties, or people lose mastery over their own lives. As we age, our memory fails us. And what if we were to suffer a head injury—a "black box" life recorder might help us solve the mystery of its cause and identify a perpetrator.

Imagine being called to the witness stand in a court of law and being asked, "Where were you on the night of 16 July 2015?," to which you might have to answer "Your honor, I was forbidden from remembering" or "My memories were deleted." (See the section "Veillance Contract.") The Veillance Foundation will create such life recorder systems (capturing physiological signals plus surrounding contextual information such as video) for improved health care and safety. Maintaining the integrity of the body (health) through veillance will bring about a pivotal transformation in personal health and safety.

MAPPING VEILLANCE INTEGRITY: THE INTEGROMETER

There are many gray areas, e.g., in the world of private property. A shopkeeper can legally install cameras in his store and legally forbid you from recording. We aim to create a hypocrisy/integrity map that lists establishments in terms of their willingness to accommodate people's need to see and remember what they have seen. We propose a ranking system like the star system for rating hotels and movies (maybe one to five integral signs to rank integrity).

YOU HAVE A RIGHT TO RECORD WHILE BEING DETAINED ON PRIVATE PROPERTY

Imagine you were unlawfully detained and physically assaulted by department store employees and, due to a head injury, had trouble remembering what happened. Moreover, imagine that your video was deleted by the shopkeepers, making it more difficult for you to make your case in court.

Let us examine a specific situation where the case can be clearly made in favor of recording. Presently, rules about recording on private property, such as retail establishments, are enforced through the Trespass to Property Act (Canada) or Trespass Based on Activities (United States). If shopkeepers see you disobeying their "no photos" or "no cameras" rule, they can ask you to leave (they can't legally delete any of your recordings or assault you), and, if you refuse to leave, they can call the police and charge you with trespassing.

One area on which the foundation wants to focus is a situation where a person is detained under a false shoplifting accusation. We argue that a person cannot be trespassing while at the same time being detained. Since the person cannot be trespassing, we argue that he or she cannot be prohibited from recording. It follows, therefore, that people detained on private property cannot be prohibited from recording during the time that they are being detained. We feel this is an important axiom of which the world should be made aware.

The Veillance Foundation is undertaking the development of the field of metaveillance (veillance of veillance—i.e., watching the watching and sensing of sensing) [28], [29]. Metaveillance reveals the otherwise hidden world of sensors, from high-pixel-count surveillance cameras to low-pixel-count cameras used in washroom sensors (e.g., pixel counts as low as 128 pixels), as illustrated previously.

INTEROPERABILITY AND ACCOUNTABILITY REQUIRE UNDERSIGHT

With the closed-source model, we don't know what's in "things." So we need the right to tinker and understand how these things work. The Veillance Foundation will create standards of integrity for the IoT [30]: things should no longer be allowed to "know" everything about us and reveal nothing about themselves. We need to create a world of data self-ownership that supports concepts like subject rights ("I belong to me") [31], where our medical records are stored on our wearable computing device under our control [32], not on a big company's or government's server under its control.

This will require new approaches to interoperability—not merely breaking

down the "silos" among disciplines, but also smashing through the one-way valves in each of these silos that soak up data without releasing it. Instead of big data knowing everything about us, we need "little data" such as our medical records stored on our own wearable computers, along with open-source data formats for this new kind of interoperability and undersight. A society with only oversight (surveillance) is linear rather than circular and, therefore, can never be truly sustainable without undersight (sousveillance).

WHAT WE NEED AND WHAT WE CAN OFFER

The examples given here lead to the conclusion that policymakers, public and private, are not equipped with the understanding required to see the inherent hypocrisy and injustice in conducting surveillance while at the same time denying others the ability to "look back." Unless an effort is made to counter the rise of pervasive and unaccountable one-way surveillance, the problem will only grow. The basic right to collect evidence to defend oneself from allegations of wrongdoing is at risk, and this puts the legitimacy of governments and other organizations that allow this to occur at risk as well.

This situation compels us to act, to create a Veillance Foundation: an organization dedicated to providing the technologies, understanding, and expertise required to bring fairness and accountability to the collection and recording of sensory data; to influence public policy; and to develop technologies and standards for integrity, comprehensibility, and interoperability.

We're looking for anyone who understands and cares about these issues and who wishes to contribute, intellectually, technically (engineering and architecting the future of wearables and the IoT), financially, or otherwise. In particular, we seek lateral thinkers who see what is at stake here. Our objective is to invent, design, and build the technologies, their etiquette, surrounding connections, community, policies, and expertise in veillance and, thereby, shape society and the future. Join us by e-mailing veillance@eyetap.org.

SUMMARY

The purpose of the Veillance Foundation is to bring together people interested in the decriminalization of truthfulness, honesty, integrity, health and safety, privacy, remembrance, humanistic intelligence, and scientific understanding of our world, both natural and human-made. Our goal is to develop technologies and business practices around basic principles of honesty, integrity, health and safety, privacy, remembrance, humanistic intelligence, and open-scientific discourse.

KEY CONCEPTS

- Surveillance (oversight) [15] and sousveillance (undersight) (Figure 8) [16].
- Surveillance, sousveillance, coveillance, and dataveillance [33].
- Intelligent veillance and the sensularity (sensory singularity) [34].
- Sousveillance is defined as "wearing and implanting various sensors, effectors, and multimedia computation to redefine personal space and modify sensory perception computationally…'Black box' life recorder... transmission of synchronized timestamped ECG data allows a remote physician to observe not only the electrical heart activity but also the visual environment, which may provide clues as to environmental causes of ECG irregularities such as arrhythmia" [35]. Sousveillance is thus useful for total health monitoring [36]–[38].
- Sousveillance, as a field of research, has expanded greatly, and, recently, it has been given new names like *lifelogging*, *quantified self*, *self-quantifying*, *self-quantification*, *personal imaging*, *personal informatics*, *personal sensing*, *self-tracking*, *self-analytics*, *autoveillance*, *self-(sur/sous)veillance*, *body hacking*, and *personal media analytics*. We need unified terminology, frameworks, and concepts to bring all these recent developments together and make sure they remain sousveillance and don't become surveillance.
- Sousveillance and political communication [39].
- Security and suicurity [40], [41].
- Health and safety.
- Priveillance (privacy and veillance) [42].
- Trust: trust is a two-way street. (We can't trust those who don't trust us.)
- Open source and open science: technologies, projects, contributions, and deliverables.
- The Veillance Contract [25].
- Axiom 1: You can't be said to be trespassing while being detained [27]
- Goods and services that uphold the ideals of the Veillance Foundation
  - dTaz (open-source personal safety device)
  - AlibEye (honesty vest, etc.)
  - nLux
  - Videscrow.
- Affiliations and outreach: conferences and collaborations, e.g., an annual event continuing in the tradition of our first veillance conference, ISTAS 2013.
- Inventions and breakthroughs in veillance.
- Optimum instanity [43].
- Cyborgspace (Web. 3.0) as alternative to mainstream media [44]–[46].

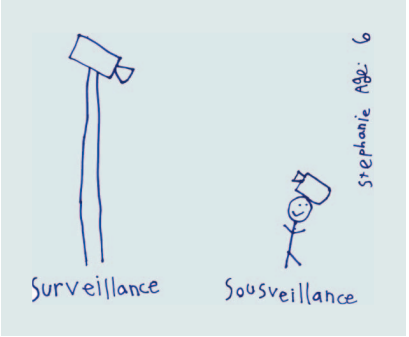

FIGURE 8. Surveillance versus Sousveillance from Stephanie (age 6).

REFERENCES

[1] K. Wiens, "The right to repair," *IEEE Consumer Electron. Mag.*, vol. 4, no. 4, pp. 123–135, Oct. 2015.
[2] [Online]. Available: http://wearcam.org/veillance.htm
[3] [Online]. Available: http://www.eyetap.org/WearCamWWTO.htm
[4] [Online]. Available: http://wearcam.org/veilluminescence.htm
[5] "CCD camera element used as actuation detector for electrical plumbing products," Canadian patent 2602560.
[6] Japanese patent WO 2012043663.
[7] U.S. patent 6671890.
[8] U.S. patent 8162236.
[9] OWLS safety and security systems. [Online]. Available: http://www.owls-ag.com/englisch/OWLS_Security_and_Lighting_Solutions/OWLS_Security_Systems.html

(continued on page 143)

2016 IEEE Consumer Electronics Society Board of Governors

Digital Object Identifier 10.1109/MCE.2015.2485020

Soapbox *(continued from page 39)*

[10] Cisco Smart+Connected City Lighting. [Online]. Available: http://www.cisco.com/web/strategy/smart_connected_communities/city-lighting.html
[11] S. Mann. Physical assault by McDonald's for wearing digital eye glass. [Online]. Available: http://wearcam.org/mcdonalds/
[12] K. Kelly. *Out of Control*. [Online]. Available: http://kk.org/mt-files/outofcontrol/ch2-g.html
[13] [Online]. Available: http://www.eyetap.org/papers/docs/IEEE_ISTAS13_Veillance2_Ali_Mann.pdf
[14] [Online]. Available: https://en.wikipedia.org/wiki/Equiveillance
[15] [Online]. Available: http://www.etymonline.com/index.php?term=surveillance
[16] [Online]. Available: https://en.wikipedia.org/wiki/Sousveillance
[17] [Online]. Available: http://bigstory.ap.org/36a09a369deb487585b89d52f4a1c2e9&utm
[18] Boston police commissioner hoping to criminalize the recording of cops in public. [Online]. Available: http://photographyisnotacrime.com/2015/08/boston-police-commissioner-hoping-to-criminalize-the-recording-of-cops-in-public/
[19] Cop draws gun on resident for filming police from his own driveway. [Online]. Available: http://countercurrentnews.com/2015/08/cop-brandishing-menacing-filming-police-from-driveway/
[20] [Online]. Available: http://dailyfreepress.com/2004/03/02/cleaning-that-dirty-water/
[21] [Online]. Available: http://wearcam.org/hpla.htm
[22] [Online]. Available: https://en.wikipedia.org/wiki/Five_Eyes
[23] [Online]. Available: http://wearcam.org/veillance/veillance.pdf
[24] [Online]. Available: http://uberveillance.com/blog/2011/1/3/professor-steve-manns-ladder-theory-understanding-sousveilla.html
[25] [Online]. Available: https://www.youtube.com/watch?t=149&v=z82Zavh-NhI
[26] [Online]. Available: http://wearcam.org/vmp.pdf
[27] [Online]. Available: http://eyetap.org/papers/docs/freeglass.pdf
[28] [Online]. Available: http://www.cv-foundation.org/openaccess/content_cvpr_workshops_2014/W17/papers/Mann_The_Sightfield_Visualizing_2014_CVPR_paper.pdf
[29] [Online]. Available: http://www.eyetap.org/docs/Veillametrics_JanzenMann2014.pdf
[30] [Online]. Available: http://wearcam.org/veillanceIoT.htm
[31] [Online]. Available: http://wearcam.org/id.htm
[32] [Online]. Available: http://www.locusmag.com/Perspectives/2015/09/cory-doctorow-what-if-people-were-sensors-not-things-to-be-sensed/
[33] [Online]. Available: http://www.ischool.berkeley.edu/courses/i290-sscd
[34] Minsky et al. (2013) [Online]. Available: http://eyetap.org/papers/docs/IEEE_ISTAS13_Sensularity_Minsky_etal.pdf
[35] [Online]. Available: http://www.eyetap.org/papers/docs/acmmm2004sousveillance_p620-mann.pdf
[36] [Online]. Available: https://upload.wikimedia.org/wikipedia/commons/b/b9/QuantimetricSelfSensingPrototypeMann1996inset.jpg
[37] [Online]. Available: http://wearcam.org/textbook.htm
[38] [Online]. Available: http://www.wseas.org/multimedia/journals/communications/2015/a605704-592.pdf
[39] [Online]. Available: http://www.amazon.com/Sousveillance-Media-Strategic-Political-Communication/dp/0826430090
[40] [Online]. Available: http://wearcam.org/suicurity.pdf
[41] [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6824309
[42] [Online]. Available: http://wearcam.org/Veillance_and_transparency_CfP.htm
[43] [Online]. Available: https://theblueprint.com/stories/steve-mann/
[44] [Online]. Available: http://www.eyetap.org/papers/docs/glogger.pdf
[45] [Online]. Available: https://tspace.library.utoronto.ca/handle/1807/24600
[46] [Online]. Available: http://www.globalresearch.ca/the-illusion-of-choice-ninety-per-cent-of-american-media-controlled-by-six-corporations/5472690