Dialogue

Wearables and Sur(over)-Veillance, Sous(under)-Veillance, Co(So)-Veillance, and MetaVeillance (Veillance of Veillance) for Health and Well-Being

Steve Mann

University of Toronto, Canada
mann@eyetap.org

Abstract

At the University of Toronto, we're embarking on a bold new initiative to bring together these four disciplines: law, business, engineering, and medicine, through what we call "sousveillant systems"—grassroots systems of "bottom up" facilitation of cross-, trans-, inter-, meta-, and anti-disciplinarity, or, more importantly, cross-, trans-, and inter-passionary efforts. Passion is a better master than discipline (to paraphrase Albert Einstein's "Love is a better master than duty"). Our aim is not to eliminate "big science," "big data," and "big watching" (surveillance), but to complement these things with a balancing force. There will still be "ladder climbers," but we aim to balance these entities and individuals with those who embody the "integrity of authenticity" and to provide a complete picture that is otherwise a half-truth when only the "big" end is present. This generalizes the notion of "open source," where each instance of a system (e.g., computer operating system) contains or can contain its own seeds (e.g., source code). Sousveillant systems are an alternative to the otherwise sterile world of closed-source, specialist silos that are not auditable by end-users (i.e., are only auditable by authorities from "above").

Introduction

Many fields and disciplines, such as law, business, engineering, and medicine, are undergoing a pivotal shift on a quest for a certain kind of integrity that we call the "integrity of authenticity," a transition from centralized "big data" to a more distributed "little data" through tools such as blockchain that embed the "seeds" of a system within each instance of it.

In *Rules for a Flat World*, Gillian Hadfield (2017) writes that law is the subjecting of human conduct to rules made by peers—that law is (or should be) formed among equals, the same way a family living in a log cabin on an island in Lake Ontario makes rules in order to coexist. She calls this "making law without lawyers" (Hadfield 2017: 20).

Traditionally at least, most business schools don't actually conduct business. Ajay Agrawal has challenged this trend by creating an entity within the University of Toronto's Rotman School of Business. This approach, together with other related ideas like crowdfunding (Agrawal, Catalini, and Goldfarb 2014), creates a new world in which business is done, or can be done, by ordinary people of all ages, genders, ethnicities, etc., thus "creating business without businessmen."

Traditionally, many engineering schools are places that don't actually do engineering, but that is also

changing. The “maker” movement is allowing ordinary people to invent, design, and build the technological future; that is, ordinary people “doing engineering without engineers.”

Medicine has traditionally been about “big data,” “big pharma,” etc. However, today our most up-to-date medical record might very well be of our own making through “wearables” (wearable computers).

At the University of Toronto, we’re embarking on a bold new initiative to bring together these four disciplines: law, business, engineering, and medicine, through what we call “sousveillant systems”—grassroots systems of “bottom up” facilitation of cross-, trans-, inter-, meta-, and anti-disciplinarity, or, more importantly, cross-, trans-, and inter-passionary efforts. Passion is a better master than discipline (to paraphrase Albert Einstein’s “Love is a better master than duty”).

Our aim is not to eliminate “big science,” big data,” and “big watching” (surveillance), but to complement these things with a balancing force. There will still be “ladder climbers,” but we aim to balance these entities and individuals with those who embody the “integrity of authenticity” and to provide a complete picture that is otherwise a half-truth when only the “big” end is present.

This generalizes the notion of “open source,” where each instance of a system (e.g., computer operating system) contains or can contain its own seeds (e.g., source code). Sousveillant systems are an alternative to the otherwise sterile world of closed-source, specialist silos that are not auditable by end-users (i.e., are only auditable by authorities from “above”).

Surveillance Facilitates Inequity, Hypocrisy, and Half-Truths

Surveillance (“big watching”) and its associated “big data” are well known and well understood as the purposeful sensing by an entity of greater authority over an entity of lesser authority, e.g., “a watch kept over a... suspect, prisoner, or the like” (dictionary.com, n.d.) or the “close observation of someone, often in order to catch them in wrongdoing” (ourdictionary.com, n.d.).

Surveillance often embodies an inherent inequity through the facilitation of the powerful keeping watch over the vulnerable. This inequity sometimes takes the form of a “male gaze,” popularized in Margaret Atwood’s dystopian concept of “UNDER HIS EYE” (Calogero 2004; Patterson and Elliott 2002), and, in particular, a “white, male gaze in the CCTV control room... [that has] a particular bias” (Galič, Timan, and Koops 2017). Surveillance often means that “[p]eople of color, migrants, unpopular religious groups, sexual minorities, the poor, and other oppressed and exploited populations bear a much higher burden of monitoring and tracking than advantaged groups” (Eubanks 2018: 6). Surveillance tends to target predominantly black (Browne 2015), poor (Ferguson 2017), and other vulnerable groups.

Hypocrisy of Surveillance

Surveillance often (but not always) embodies an inherent hypocrisy in the sense that entities conducting surveillance may choose to (and have the capacity to) prohibit other veillances (see Figures 1 and 2).

Figure 1: Three examples of surveillance hypocrisy. Surveillance is the veillance that has the capacity for hypocrisy. That is, it is the veillance that has the authority to watch while prohibiting others from watching. This creates a possible conflict of interest in which one party hoards all of the evidence while attempting to destroy others' capacity to collect evidence. Consider, for example, someone wearing a medical device that helps with visual memory. This device captures their entire life but is unable to see. Thus, the otherwise unbroken record is broken or missing data. When called to testify in court, a person with a memory impairment who normally relies on such a device could argue that the entity of greater authority destroyed the recording by prohibiting it. This creates a possibility of corruption, e.g., a selective retention of evidence that is more favorable to the authority, and a selective degradation (or even complete deletion) of evidence that might support others taking legal action against the authority.

Figure 2: Privacy is often cited as a reason for the hypocrisy of one-sided watching. But this is not true privacy. It is the panoptic privacy as prophesized by Bentham's prison design in which inmates have privacy from each other while being watched by guards. Here, for example, is the counter where we return books at the Terman Engineering Library at Stanford University. The librarian is often absent, so we often photograph the books that we return as they appear lying on the counter. This is so that we have a "visual receipt" showing that we returned the books, even though doing something as practical and necessary as this is against the rules and therefore, perhaps, an act of civil (or other deliberate) disobedience. Photograph by the author.

Precise Definition of Surveillance, etc.

Google translates the English word “oversight” to the French word “surveillance” (see Figure 3).

English:

French/Latin:

Figure 3: Google translates the English word “oversight” into the French word “surveillance.” Analogously, we proffer “undersight” (“sousveillance”), “side-sight” (coveillance or soveillance, i.e., the side-to-side peer-based watching of social networking or neighbourhood watch), and “metavision” (“metaveillance”), which is the watching of watching or sensing of sensors and the sensing of their capacity to sense.

More recently, the words “undersight” and “side-sight” (or “social-networking-sight,” the vision of social-networking) emerged (Mann 2001a).

We tend to use the French/Latin word “surveillance” rather than its English equivalent “oversight” because the English word has two quite different meanings. “Oversight” can mean “surveillance,” or it can mean “an error or omission” (e.g., “It was an oversight on our part”).

Sousveillance, loosely defined as the vulnerable watching the powerful, coveillance (côteveillance or soveillance or sociaveillance or mediaveillance), loosely defined as the side-to-side gaze between peers via social media and the like, and metaveillance, loosely defined as the sensing of sensors and the sensing of their capacity to sense, are relatively recent concepts emerging around the generalized idea of “veillance,” which is defined as purposeful sensing (Janzen and Mann 2014; Reynolds 2011; Bakir 2010; Mann 2002; Ali and Mann 2013; Ganascia 2010; Vertegaal and Shell 2008; Michael and Michael 2012; Bakir 2009; Fernback 2013; Reilly 2015; Cardullo 2014; Ali et al. 2013a; Nolan, Mann, and Wellman 2008; Ali et al. 2013b; Weber 2012a, 2012b; Mortensen 2014; Quessada 2010; Manders 2013; Cammaerts 2015). We shall more precisely define surveillance as follows:

Surveillance is the veillance performed by an entity that has the authority to prohibit other veillances.

More succinctly, in the actor-network theory (ANT) sense (Munro 2009), akin to other anthropomorphisms like “information wants to be free” (Giles 2007; Stewart 1987):

Surveillance is the veillance that has the capacity to forbid other veillances.

In this way, surveillance may be *defined* in terms of its increased capacity for hypocrisy (in the veillance sense)—as the “official” veillance of a governing, ruling, regnant, sovereign, leading, commanding, or controlling entity. Implicit here is that this authority manifests itself in ways that include the capacity to allow or prohibit sensing.

Surveillance is thus the veillance of the state or other institutions, syndicates, or cartels that can (but do not necessarily or do not always) exert the prohibition of other veillances.

We also must acknowledge that the boundary between state and non-state organizations is becoming blurred, and that the boundary between environment (surroundings) and the existential “invernmnet” (e.g., one’s own personal wearables) (Mann et al. 2014: 9) is also being blurred. For example, police body cameras

problematize the otherwise clear boundary between one's own personal space and the surrounding space of other authorities.

Particularly, the simple fact that a technology is wearable does not necessarily make it an entirely sousveillant technology. For example, we can imagine edge-cases such as a new police recruit being monitored by a corrupt police chief who forces the new recruit to wear a camera system or an employee forced to wear a camera system that helps a boss keep the worker obedient and subservient or deters the worker from union or whistleblowing activities.

Even in situations where a police officer chooses to wear a camera system, there is still a potential conflict of interest in the curation of recordings both at the officer level and at the organizational level. At the officer level, the officer might cover the camera, aim it advantageously, or ensure it is not running while police misconduct ensues. At the organizational level, the organization may let an individual officer "fall" as a result of video that shows the individual officer committing an act of wrongdoing, but the organization may be willing to destroy evidence to protect itself as a whole.

Therefore, "wearables" and "sousveillance," although closely related, are not synonymous.

Let us thus define one kind of sousveillance in the ANT sense (Munro 2009):

Hierarchical sousveillance is theveillance that does not have the capacity to forbid or allow itself or other veillances.

In this way, sousveillance may be (but is not necessarily) an act of civil disobedience against surveillance (or its purveyors), i.e., sousveillance does not necessarily seek permission for its conduct. It is still useful to define participatory sousveillance as follows:

(Participatory) Sousveillance is the recording of an activity by a participant in the activity.

This is usually done by personal technologies or "bringing cameras from the lamp posts and ceilings, down to eye-level" (Mann, Nolan, and Wellman 2003: 620), which may then give us coveillance.

Sousveillance Disclaimer

Those of us who study sousveillance also acknowledge that veillances can shift, that the sousveillance of self-sensing can be turned into a tool for surveillance (Hulsey and Reeves 2014; Ritsema van Eck 2019) and that the lines can be further blurred when citizen sousveillance also serves law enforcement (Reeves 2012). Joseph Brandim Howson (2018) also introduces concepts like supra-veillance, peer-veillance, and sur-sousveillance. We make no claims that sousveillance is guaranteed to help the vulnerable or that it will be sure to stop or mitigate the oppressive nature of surveillance. In fact, we don't even claim that it is always part of the solution. It might sometimes even become part of the problem. But we do believe that the plurality of veillances will facilitate more diversity in the discussions surrounding the otherwise one-sided discussions onveillance.

Surveillance and "Big Data" are Half-Truths

Surveillance tells only one side of a multi-sided story, and thus surveillance is a half-truth without other veillances (Mann et al. 2015). Likewise, "big data" is a half-truth without "little-data" (e.g., distributed blockchain), and, in some sense, technologies like blockchain allow for the creation of sousveillant systems in which auditability can come from below, not just from above (i.e., the vulnerable can audit the powerful without getting the permission, consent, or "buy-in" of the powerful) (Catalini and Gans 2016).

Equiveillance, the Balance between Sur and Sous-veillance

Equiveillance is the balance or equilibrium between surveillance and sousveillance. Equivalent systems are systems that give rise to equity, diversity, inclusion, fairness, and justice (Weber 2012a, 2012b; Mann 2005;

Kerr and Mann 2006; Mann and Ferenbok 2013). Thus, the veillances are nuanced and politicized in many ways, but the core concepts are useful and necessary to help us understand the complex political landscape in which we live.

Metaveillance, Sensing Sensors, and Sensing their Capacity to Sense

Perhaps the most pure and simple-to-define veillance is metaveillance—the sensing of sensors and the sensing of their capacity to sense—as we can regard this as a simple problem of pure mathematics and physics (Mann 2016).

Wearables, Health, and Well-Being through Sousveillance: Bringing Integrity to Health Care

Not long ago, it was difficult or impossible for us, as patients, to access our own health records. Many of us can remember being told that we were not allowed to see or get a copy of our own X-rays (today's proprietary systems don't make things any easier).

We were expected to strip completely naked and reveal everything about ourselves for examination, yet we were often not allowed to access any of the data about ourselves.

This was at a time when it was standard practice to require first-year students to take off all of their clothes and be photographed completely naked from front, rear, and side views in front of a giant sheet of graph paper, allegedly to check for scoliosis or other spinal or posture defects, but there was a secret agenda with a secret purpose—surveillance (Rosenbaum 1995).

Professor Beth Linker wrote: “These photos served as big data.... Body discipline used to happen because other people were monitoring your posture. There is far more self-monitoring in the 21st century” (qtd. in Unger Baillie 2018: para. 17).

There is an inherent hypocrisy in a healthcare system that wants to know everything about us but reveal nothing—to see but not be seen. The opposite of hypocrisy is integrity. Those of us interested in health sousveillance seek to bring integrity to healthcare, such as by putting data into the hands of the individuals that the data came from.

Wearables as Sousveillant Systems: QSS

In response to the one-sided watching (surveillance) built into most healthcare systems of the time, I decided during my childhood in the 1970s to invent a machine that would collect health information like electrocardiograms and electroencephalograms and provide real-time biofeedback (e.g., to see one's own heart's waveform while jogging). I named this system “Quantimetric Self-Sensing” (QSS) and presented it to Kevin Kelly in July 1996. Subsequently, Kelly called it “Quantified Self” (QS) (Kelly 1996, 2017: 336) (see Figure 4).

Figure 4: My Quantimetric Self-Sensing (QSS) system. Left: A 1996 sensing vest and eyewear measured and processed respiration, ECG (electrocardiogram), EEG (electroencephalogram), EMG (electromyogram), GSR (galvanic skin response), audio and video of the surroundings, and many other signals. This system was presented to Kevin Kelly at the WiReD offices in San Francisco, where he called it “Quantified Self.” Right: miniaturization of the apparatus resulted in the world’s first smartwatch in 1998, featured in *Linux Journal*, July 2000.

The idea of QSS is that the most up-to-date medical record is on one’s own body. We own our own data (hopefully, notwithstanding some very unfair “terms of service” agreements with large powerful organizations) and may grant permission to our physicians to obtain our data, not the other way around!

We call this principle subjectright (Mann 2001a, 2001b), denoted as © akin to copyright denoted as ©.

Health Sousveillance: Wearables and Systems for Taking Health into our Own Hands

Health sousveillance is a bold new engineering, medicine, law, and business initiative aimed at empowering individuals with technologies like wearables that let them access, understand, and use their own health data in new ways.

It is based on three key principles:

1. **Subject rights:** We have a right to access any information, such as medical images, recordings, etc., about ourselves. We have a right to share this information with others of our choosing, e.g., our doctor or others who might help advise us on our health (Mann 2001a, 2001b).
2. **Auditability:** We have a right to understand how our health data are captured, encoded, processed, transmitted, stored, etc. This requires free (“libre”) open-source systems that are auditable by end-users or those that they choose to appoint. We have a right to designate others of our choosing to assist us in understanding our own health data.
3. **Right to record:** Wearables empower people to capture their own data about themselves and things that affect them and their health. Individuals shall always have the right to capture, process, record, and share their own data about their own health. We can record our brainwaves well enough that we can actually reconstruct pictures of people we meet, causing the eye itself to function as a camera (Mann et al. 2019) and helping people suffering from prosopagnosia to remember names and faces (see Figure 5) (Mann 1996). There must always be a fundamental right to sousveillance.

Hippocratic Oath 3.0: “Primum non nocere” (“Do no harm”):

1. Denying subject access does harm (e.g., the inability to get the best healthcare);
2. Closed-source does harm (the inability to audit, etc.);
3. Preventing a person from recording their own health data does harm.

Conclusions

“Wearables” (wearable computers) have the ability to empower all of us, including the vulnerable, to capture ourselves and the world around us in a way that can bring a new kind of integrity to healthcare, business, law, and engineering. Accordingly, I, along with others who study sousveillance, propose “sousveillant systems” as systems that contain the seeds of their own essence and eliminate the silos between disciplines and the false boundary between developer and user. Sousveillant systems are auditable by end users without requiring the end users to ask special permission or apply to be a special class of person (e.g., “developer,” “auditor,” “scientist,” or “doctor,” etc.). In particular, we propose the idea that individuals can and should be able to be keepers of their own medical history on a miniature, low-cost, blockchain-based wearable computer system that contains the “seeds” of all the algorithms and encoding necessary to understand the data.

Figure 5: ElectroVisuoGram (EVG) is an image recorded from the human brain, causing the human eye itself to function as a camera (Mann et al. 2019).

References

- Agrawal, Ajay, Christian Catalini, and Avi Goldfarb. 2014. Some Simple Economics of Crowdfunding. *Innovation Policy and the Economy* 14 (1): 63–97.
- Ali, Mir Adnan, and Steve Mann. 2013. The Inevitability of the Transition from a Surveillance-Society to a Veillance-Society: Moral and Economic Grounding for Sousveillance. In *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing Augmented Reality in Everyday Life*, Toronto, ON, June 27–29, 243–254. <https://doi.org/10.1109/ISTAS.2013.6613126>.
- Ali, Mir Adnan, Jonathan Polak Nachumow, Jocelyn A Srigley, Colin D. Furness, Sebastian Mann, and Michael Gardam. 2013a. Measuring the Effect of Sousveillance in Increasing Socially Desirable Behaviour. In *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing Augmented Reality in Everyday Life*, Toronto, ON, June 27–29, 266–267. <https://doi.org/10.1109/ISTAS.2013.6613128>.
- Ali, Mir Adnan, Tao Ai, Akshay Gill, Jose Emilio, Kalin Ovtcharov, and Sebastian Mann. 2013b. Comparametric HDR (High Dynamic Range) Imaging for Digital Eye Glass, Wearable Cameras, and Sousveillance. In *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing Augmented Reality in Everyday Life*, Toronto, ON, June 27–29, 107–114. <https://doi.org/10.1109/ISTAS.2013.6613108>.
- Bakir, Vian. 2009. Tele-technologies, Control, and Sousveillance: Saddam Hussein—De-deification and the Beast. *Popular Communication* 7 (1): 7–16.
- . 2010. *Sousveillance, Media and Strategic Political Communication*. New York, NY: Continuum.

- Brandim Howson, Joseph. 2018. New Modes of Watching from the Favela. Presented at the *VII Oxbridge Conference on Brazilian Studies*, October 6. St Antony's College, University of Oxford. Oxford, United Kingdom.
- Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
- Calogero, Rachel M. 2004. A Test of Objectification Theory: The Effect of the Male Gaze on Appearance Concerns in College Women. *Psychology of Women Quarterly* 28 (1): 16–21.
- Cammaerts, Bart. 2015. Social Media and Activism. In *The International Encyclopedia of Digital Communication and Society*, edited by Robin Mansell and Peng Hwa Ang, 1–8. Hoboken, NJ: Wiley.
- Cardullo, Paolo. 2014. Sniffing the City: Issues of Sousveillance in Inner City London. *Visual Studies* 29 (3): 285–293.
- Catalini, Christian, and Joshua S. Gans. 2016. Some Simple Economics of the Blockchain. Working Paper 22952. Cambridge, MA: National Bureau of Economic Research. <https://www.nber.org/papers/w22952.pdf>.
- Dictionary.com. N.d. Surveillance. *Dictionary.com*. <https://www.dictionary.com/browse/surveillance> [accessed January 16, 2020].
- Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.
- Ferguson, Andrew Guthrie. 2017. *Big Data Policing: Surveillance, Race, and Law Enforcement*. New York, NY: New York University Press.
- Fernback, Jan. 2013. Sousveillance: Communities of Resistance to the Surveillance Environment. *Telematics and Informatics* 30 (1): 11–21.
- Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. 2017. Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology* 30 (1): 9–37.
- Ganascia, Jean-Gabriel. 2010. The Generalized Sousveillance Society. *Social Science Information* 49 (3): 489–507.
- Giles, Jim. 2007. Comment: Information Wants to be Free. *New Scientist* 195 (2622): 22–23.
- Hadfield, Gillian K. 2017. *Rules for a Flat World: Why Humans Invented Law and How to Reinvent it for a Complex Global Economy*. Oxford, UK: Oxford University Press.
- Hulsey, Nathan, and Joshua Reeves. 2014. The Gift that Keeps on Giving: Google, Ingress, and the Gift of Surveillance. *Surveillance & Society* 12 (3): 389–400.
- Janzen, Ryan, and Steve Mann. 2014. Veillance Flux, Vixels, Veillons: An Information-Bearing Extramissive Formulation of Sensing, to Measure Surveillance and Sousveillance. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, Toronto, ON, May 5–8, 1–10. <https://doi.org/10.1109/CCECE.2014.6901060>.
- Kelly, Kevin. 1996. Personal communication. San Francisco, California (WiReD office).
- . 2017. *The Inevitable: Understanding the 12 Technological Forces that Shape Our Future*. New York: Penguin.
- Kerr, Ian, and Steve Mann. 2006. Over and Under the Valences of Veillance – Exploring Equiveillance. *blog*on*nymity*, January. <http://wearcam.org/anonequiveillance.htm> [accessed May 13, 2020].
- Manders, Corey. 2013. Moving Surveillance Techniques to Sousveillance: Towards Equiveillance Using Wearable Computing. In *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing Augmented Reality in Everyday Life*, Toronto, ON, June 27–29, 19–19. <https://doi.org/10.1109/ISTAS.2013.6613097>.
- Mann, Steve. 1996. Wearable, Tetherless Computer-Mediated Reality: WearCam as a Wearable Face-Recognizer, and Other Applications for the Disabled. In *AAAI Technical Report FS-96-05*, MIT, February 2. Menlo Park, CA: AAAI Press.
- . 2001a. Keynote: Perspective on Subjectrights: 7 Important New Concepts. In *8th CACR Information Security Workshop & 2nd Annual Privacy and Security Workshop: The Human Face of Privacy Technology*, Toronto, ON, November 1–2, 1–7. Bloomington, IN: Center for Applied Cybersecurity Research.
- . 2001b. Subjectright. *The Journal of Medical Knowledge Management, Physician's Computing Chronicle* 6 (2): 8–9.
- . 2002. Sousveillance, Not Just Surveillance, in Response to Terrorism. *Metal and Flesh* 6 (1): 1–8.
- . 2005. Equiveillance: The Equilibrium between Sur-veillance and Sous-veillance. Presented at *The Fifteenth Conference on Computers, Freedom and Privacy*, Seattle, WA, April 12–15. New York, NY: Association of Computing Machinery.
- . 2016. Surveillance, Sousveillance, and Metaveillance. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, Las Vegas, NV, June 26–July 1, 1408–1417. <https://doi.org/10.1109/CVPRW.2016.117>.
- Mann, Steve, and Joseph Ferenbok. 2013. New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World. *Surveillance & Society* 11 (1/2): 18–34.
- Mann, Steve, Jason Nolan, and Barry Wellman. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1 (3): 331–355.
- Mann, Steve, Ryan Janzen, Tao Ai, Seyed Nima Yasrebi, Jad Kawwa, and Mir Adnan Ali. 2014. Toposculpting: Computational Lightpainting and Wearable Computational Photography for Abakographic User Interfaces. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, Toronto, ON, May 5–8, 1–10. <https://doi.org/10.1109/CCECE.2014.6901118>.
- Mann, Steve, Ryan Janzen, Mir Adnan Ali, and Ken Nickerson. 2015. Declaration of Veillance (Surveillance is Half-Truth). In *2015 IEEE Games Entertainment Media Conference (GEM)*, Toronto, ON, October 14–16, 1–2. <https://doi.org/10.1109/GEM.2015.7377257>.
- Mann, Steve, Kyle E. Mathewson, Jeremy Stairs, Cayden Pierce, Jesse Hernandez, Derek Lam, Georges Kanaan, Luke Piette, Humza Khokhar, and Christina Mann. 2019. The Human Eye as a Camera. In *2019 IEEE International Conference on e-Health Networking, Application & Services (HealthCom)*, Bogotá, Colombia, October 14–16, 1–8. <https://doi.org/1109/HealthCom46333.2019.9009592>.
- Michael, Katina, and M.G. Michael. 2012. Sousveillance and Point of View Technologies in Law Enforcement: An Overview. In *The Sixth Workshop on the Social Implications of National Security: Sousveillance and Point of View Technologies in Law Enforcement (An Overview)*, Sydney, NSW, February 22. Sydney: The University of Sydney. <https://works.bepress.com/kmichael/252/>.

- Mortensen, Mette. 2014. Who is Surveilling Whom? Negotiations of Surveillance and Sousveillance in Relation to Wikileaks' Release of the Gun Camera Tape Collateral Murder. *Photographies* 7 (1): 23–37.
- Munro, Roland. 2009. Actor-Network Theory. In *The SAGE Handbook of Power*, edited by Stewart R. Clegg and Mark Haugaard, 125–39. London: Sage Publications.
- Nolan, Jason, Steve Mann, and Barry Wellman. 2008. Sousveillance: Wearable and Digital Tools in Surveilled Environments. In *Small Tech: The Culture of Digital Tools*, edited by Byron Hawk, David M. Rieder, and Ollie Oviedo, 179–198. Minneapolis, MN: University of Minnesota Press.
- Patterson, Maurice, and Richard Elliott. 2002. Negotiating Masculinities: Advertising and the Inversion of the Male Gaze. *Consumption, Markets and Culture* 5 (3): 231–249.
- Quessada, Dominique. 2010. De la sousveillance. *Multitudes* 1: 54–59.
- Reeves, Joshua. 2012. If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility. *Surveillance & Society* 10 (3/4): 235–248.
- Reilly, Paul. 2015. Every Little Helps? YouTube, Sousveillance and the “Anti-tesco” Riot in Stokes Croft. *New Media & Society* 17 (5): 755–771.
- Reynolds, Carson. 2011. Negative Sousveillance. In *Proceedings of the First International Conference of the International Association for Computing and Philosophy (IACAP11)*, Aarhus, Denmark, July 4–6, 306–309. Münster, DE: Verlagshaus Monsenstein und Vannerdat OHG.
- Ritsema van Eck, Gerard Jan. 2019. Emergency Calls with a Photo Attached: The Effects of Urging Citizens to use Their Smartphones for Surveillance. In *Surveillance, Privacy, and Public Space*, edited by Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops, 157–178. Abingdon, UK: Routledge.
- Rosenbaum, Ron. 1995. The Great Ivy League Nude Posture Photo Scandal. *New York Times Magazine*, January 15, 28.
- Stewart, Brand. 1987. *The Media Lab: Inventing the future at MIT*. New York: Viking Penguin.
- Unger Baillie, Katherine. 2018. Examining 20th-Century America's Obsession with Poor Posture, a Forgotten “Epidemic.” *Penn Today*, June 7. <https://penntoday.upenn.edu/news/examining-20th-century-americas-obsession-poor-posture-forgotten-epidemic> [accessed May 13, 2020].
- Vertegaal, Roel, and Jeffrey S. Shell. 2008. Attentive User Interfaces: Surveillance and Sousveillance of Gaze-Aware Objects. *Social Science Information* 47 (3): 275–298.
- Weber, Karsten. 2012a. Google Glasses: Surveillance, Sousveillance, Equiveillance. In *5th International Conference on Information Law and Ethics*, Corfu, Greece, June 29–30, 1–3. <http://dx.doi.org/10.2139/ssrn.2095355>.
- . 2012b. Surveillance, Sousveillance, Equiveillance: Google Glasses. Social Science Research Network, July 1: 1–3.
- Yourdictionary.com. N.d. Surveillance. *Yourdictionary.com*. <https://www.yourdictionary.com/surveillance> [accessed January 16, 2020].