

Computing Ethics

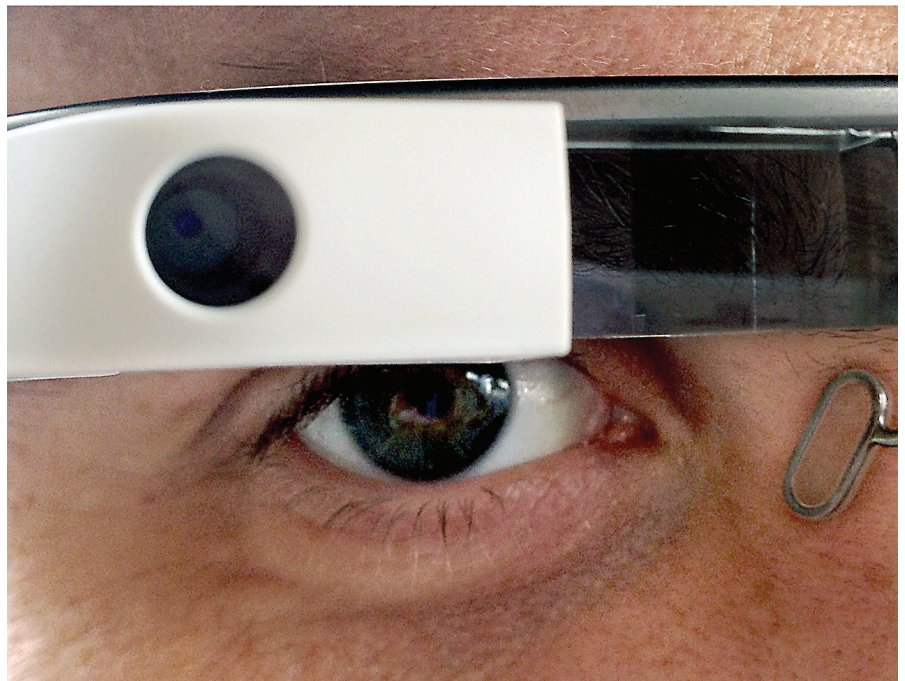
No Limits to Watching?

Considering the ethical questions raised by technologies that are moving from knowing what we are doing (and where) to knowing who we are.

LITTLE BY LITTLE, the introduction of new body-worn technologies is transforming the way people interact with their environment and one another, and perhaps even with themselves. Social and environmental psychology studies of human-technology interaction pose as many questions as answers. We are learning as we go: “learning by doing” through interaction and “learning by being.”⁹ Steve Mann calls this practice existential learning: wearers become photoborgs,³ a type of cyborg (cybernetic organism) whose primary intent is image capture from the domains of the natural and artificial.⁵ This approach elides the distinction between the technology and the human; they coalesce into one.

With each release greater numbers of on-board sensors can collect data about physiological characteristics, record real-time location coordinates, and use embedded cameras to “life-log” events 24x7. Such data, knowingly or unknowingly collected and bandwidth permitting, may be wirelessly sent to a private or public cloud and stored, often for public view and under a creative commons license.² Embedded sensors on wearers can actively gather information about the world and capture details of a personal nature—ours and those of others too. These details can be minor, like embarrassing habits of less than admirable personal hygiene, or major, such as records of sexual peccadilloes or events relevant to court proceedings.

A third party might own the data gathered by these devices or the device



itself. The Google Glass Terms of Service state: “...you may not resell, loan, transfer, or give your device to any other person. If you resell, loan, transfer, or give your device to any other person without Google’s authorization, Google reserves the right to deactivate the device, and neither you nor the unauthorized person using the device will be entitled to any refund, product support, or product warranty.”⁸ Personal information stored on the Internet for ease of access from anywhere at any time raises the possibility of unauthorized access. Most wearable sleep monitors indicate when you are awake, in light sleep, in deep sleep (REM), and calculate the level of efficiency reached between your rest and wake times.⁷

Monitors can tell adults how often they wake up during the night, the duration of sleep, time spent in bed, and times of awakening.⁶ Sleeping patterns convey personal details about individuals, such as insomnia or compulsive obsessive disorder, sexual activity, workaholicism, likely performance in stressful jobs, and other things.

Wearables can also look outward, reconstructing the world with location coordinates,¹¹ current speed traveled and direction, rich high-resolution photographs, and audio capture. Wearers gather data about themselves but also heterogeneous data about fixed and mobile entities, including infrastructure, living things (such as people and animals) and non-living

things (such as vehicles). This is not simply derivable information, such as the “point of interest nearest you is ‘x’ given your position on the Earth’s surface,” but can be interpreted as, “Johnny is traveling at ‘x’ miles per hour and is a little sluggish today on his bike ride compared to yesterday, perhaps because of his late night and his consumption of one glass too many of wine while at the nearby bar.”

These devices can tell us about exceptions to everyday patterns of people in or out of our social networks. Consider the potential for government surveillance beyond the Call Detail Records that caused such controversy for the National Security Agency in 2013. Relentless data capture is uncompromising. Wearers concerned only about whether the device is working as intended might not consider the consequences of unauthorized data collection. They might feel they have purchased the device and are using it to their best ability. Will they consider feelings of fraternity with strangers who do not have access to the same technology? Or will they feel they have every right to put on their wearable device and adapt their body for convenience or personal needs such as maintaining personal security, reducing liability, and increasing life expectancy? Might wearers figure that any problems are the *other* persons’ problems as long as the wearers believe they are not breaking the law? Whether the device is doing what it is supposed to do (for example, work properly), might occlude more meaningful questions of societal consequences from using such devices.

Bystanders are likely to be as oblivious to data collection from wearable devices as they are from data collection of private investigators using covert devices. Yet many people vehemently oppose being a subject of someone else’s recording.¹ The disappearing difference between covert and overt devices makes it possible for surveillance to become so ubiquitous that it is rendered “invisible.” Anything right in front of us and ever present is in our “blind spot,” hardly noticeable because we are enveloped by it like the fog. Novelty wears off over time, industrial/human factor design can help

Relentless data capture is uncompromising.

make things invisible to us, and we undergo conditioning. When surveillance cameras are everywhere, including on our heads and in our lapels, it is no longer surveillance. It is simply the human activity of “watching.”

CCTV cameras are arguably invasive, but we do not protest their use even though people are aware of their presence. What happens when we open the floodgates to constant watching by tiny lifelogging devices? We open ourselves to not just Big Brother, but countless Little Brothers.¹⁵ Corporate or governmental compliance and transparency hide the fact that audiovisual collection of information will come at a cost. Multiple depictions of the same event can be stronger than a single view, and corruption can flourish even in a transparent environment. It can even be corruption on a grander scale. Crowdsourced sousveillance (watching from below)¹² might take place for authenticity or verification, but police with the authority to subpoena data for use in a court of law as direct evidence can use the data to support their “point of view” (POV), irrespective of the fact that “point of eye” (POE) does not always capture the whole truth.^{a,13}

The more data we generate about ourselves, our families, our peers, and even strangers, the greater the potential risk of harm to ourselves and each other. If we lose the ability to control images or statistics about personal or public behaviors how do we make the distinction between becoming a photoborg and becoming the subject matter of a photoborg?

a Hans Holbein’s famous painting *The Ambassadors* (1533) with its patent reference to anamorphosis speaks volumes of the critical distinction between PoE and PoV. Take a look (<http://www.nationalgallery.org.uk/paintings/hans-holbein-the-younger-the-ambassadors>), if you are not already familiar with it. Can you see the skull? The secret lies in in the perspective.

Calendar of Events

November 17–20

Web Intelligence and Intelligent Agent Technology Conference
Atlanta, GA,
Sponsored: SIGART,
Contact: Yi Pan,
Email: yipan@gsu.edu

November 17–21

SC Conference on High Performance Computing, Networking, Storage and Analysis
Denver, CO,
Sponsored: SIGARCH, SIGHPC,
Contact: William D. Gropp,
Email: wgropp@illinois.edu,
Phone: 217.244.6720

November 18–21

The International Conference on Computer-Aided Design
San Jose, CA,
Sponsored: SIGDA,
Contact: Joerg Henkel,
Email: henkel@kit.edu

November 21–22

Twelfth ACM Workshop on Hot Topics in Networks
College Park, MD,
Sponsored: SIGCOMM,
Contact: Dave Levin,
Email: dml@cs.umd.edu

November 26–28

The 6th International Conference on Security of Information and Networks
Aksaray, Turkey,
Contact: Atilla Elçi,
Email: atilla.elci@gmail.com

December 2–5

International Conference on Utility and Cloud Computing
Dresden, Germany,
Sponsored: SIGARCH,
Contact: Rajhurnar Buyya,
Email: raj@cs.mu.oz.au

December 7–10

Information and Communication Technologies and Development
Cape Town, South Africa,
Sponsored: SIGCAS,
Contact: Gary Marsden,
Email: gaz@cs.uct.ac.za

December 7–11

The 46th Annual IEEE/ACM International Symposium on Microarchitecture
Davis, CA,
Sponsored: SIGMICRO,
Contact: Matthew Farrens,
Email: farrens@cs.ucdavis.edu

There is a stark asymmetry between those who use wearables and those that do not. There is much confusion over whether sousveillance¹² is ethical or unethical. The possible perils from lifelogging devices that capture the world around them are only now getting attention.⁴ To what extent is it ethical to create the records of the lives of others without prior consent or cognizance? Maker or hacker communities—"prosumers" and "producers"—create personalized devices for their own consumption and become trailblazers for what is possible. But they do not speak for everyone. What is initially made to serve individual needs often is commercialized for mass consumption.

Data from others can generate a great deal of money. Consider the story of Henrietta Lacks, a poor black tobacco farmer whom scientists named "HeLa."¹⁴ According to Rebecca Skloot, HeLa's cells were "taken without her knowledge in 1951" and became a vital medical tool "for developing the polio vaccine, cloning, gene mapping, in vitro fertilization, and more."¹⁴ Until this year, when the family came to a mutually satisfactory arrangement with the NIH, HeLa cells were "bought and sold by the billions," without compensation or acknowledgment. Who profits from wearable devices? The company that owns the device or the data? The wearer? The person in the field of view? Historical evidence suggests it will likely be everyone else but the user wearing the device or the citizen in the field of view. Marcus Wigan and Roger Clarke suggest a private data commons as a potential way forward in this big data enterprise.¹⁶

Widespread diffusion and data manipulation can require more than an ordinary consumer decision about use and acceptance. Trust and adoption are key to societal conversations that will shape guidelines and regulations about what is and is not acceptable with respect to wearable computing. At what stage of the game are the "rules" to be determined and by whom?


New technologies can bring wonderful benefits, but also disputed, unintended, and sometimes hidden consequences. Technologies should aid and sustain humankind, but we

Wearable devices create moral and ethical challenges, especially if they are widely used.

cannot limit technologies to just positive applications. We should not claim benefits without admitting to the risks and costs. Wearable devices create moral and ethical challenges, especially if they are widely used. We must look beyond findings from previous studies of emerging technologies because new technologies often help create new socio-technological contexts. We cannot afford unreflective adoption. "Play" can have real repercussions. The novelty, fun, and "wow" factors wear off and we are left with the fallout. We must be vigilant in our new playhouse, and not negate the importance of moral or ethical standards alongside market values.

Philosophers have contemplated the question of technology and its impact on society. Martin Heidegger, Ivan Illich, Jacques Ellul, and those of the Frankfurt School, have argued that the worst outcome from technology gone wrong is dehumanization of the individual and the loss of dignity, resulting in a "standardized subject of brute self-preservation."¹⁰ A fundamental insight of such literature is that technology has not only to do with building: it is also a *social process*. Any social process resulting in unreflective adoption of technological marvels is profoundly deficient. More is not always better, and the latest is not always the greatest.

Charlie Chaplin's culturally significant film *Modern Times* (1936) shows the iconic Little Tramp caught up in the cogs of a giant machine. The unintended consequences of modern and efficient industrialization are clear. Chaplin's classic builds on Fritz Lang's futuristic film *Metropolis* (1926), which depicts a mechanized

underground city in a dystopian society. Both films left indelible marks as prescient summaries of what was to follow. When technology becomes a final cause for its own sake, teleology and technology become confused. The old saw that "The person with the most toys wins," reflects this. What about the rest of us? 

References

1. Abbas, R., Michael, K., Michael, M.G. and Aloudat, A. Emerging forms of covert surveillance using GPS-enabled devices. *Journal of Cases on Information Technology* 13, 2 (2011), 19–33.
2. Creative Commons: Attribution 2.0 Generic, n.d. <http://creativecommons.org/licenses/by/2.0/>.
3. Electrical and Computer Engineering, ECE1766 Final Course Project. *Wearcam.org* (1998) <http://www.wearcam.org/students.htm>.
4. ENISA. To log or not to log?: Risks and benefits of emerging life-logging applications. *European Network and Information Security Agency*. (2011) <http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/life-logging-risk-assessment/to-log-or-not-to-log-risks-and-benefits-of-emerging-life-logging-applications>.
5. Gray, C. H. Cyborgs, Aufmerksamkeit and Aesthetik [transl. Cyborgs, Attention, & Aesthetics]. *Kunstforum* (Dec.–Jan. 1998); <http://www.chrisablesgray.org/CyborgCitizen/kunst.html>.
6. Henry, A. Best sleep tracking gadget or app? (2013); <http://lifehack.com/5992653/best-sleep-tracking-gadget-or-app>.
7. Henry, A. Sleep time alarm clock for android watches your sleep cycles, wakes you gently (2012); <http://lifehack.com/5942519/sleep-time-alarm-clock-for-android-watches-your-sleep-cycles-wakes-you-gently>.
8. Kravets, D. and Baldwin, R. Google is forbidding users from reselling, loaning glass eyewear. *Wired: Gadget Lab* (Apr. 17, 2013); <http://www.wired.com/gadgetlab/2013/04/google-glass-resales/>.
9. Mann, S. Learn by being: Thirty years of cyborg existology. *The International Handbook of Virtual Learning Environments* (2006), 1571–1592.
10. Marcuse, H. Social implications of technology. *Readings in the Philosophy of Technology* 5, 71 D.M. Kaplan, Ed., 2009.
11. Michael, K. and Clarke, R. Location and tracking of mobile devices: Überveillance stalks the streets. *Computer Law and Security Review* 29, 2 (Feb. 2013), 216–228.
12. Michael, K. and Michael, M.G. Sousveillance and the social implications of point of view technologies in the law enforcement sector. In *Proceedings of the 6th Workshop on the Social Implications of National Security*. Sydney, NSW, Australia, 2012; <http://works.bepress.com/krmichael/249>.
13. Michael, K. and Miller, K.W. Big data: New opportunities and new challenges. *IEEE Computer* 46, 6 (2013), 22–24.
14. Skloot, R. *The Immortal Life of Henrietta Lacks*. Crown, New York, 2011; <http://rebeccaskloot.com/the-immortal-life/>.
15. Weil, J. Forget big brother. Little brother is the real threat. (Sept. 22, 2010); <http://www.thenextgreatgeneration.com/2010/11/forget-big-brother-little-brother-is-the-real-threat/>.
16. Wigan, M.R. and Clarke, R. Big data's big unintended consequences. *Computer* 46, 6 (June 2013), 46–53.

Katina Michael (katina@uow.edu.au) is an associate professor in the Faculty of Engineering and Information Sciences at the University of Wollongong, NSW, Australia.

MG Michael (mgm@uow.edu.au) is an honorary associate professor in the School of Information Systems and Technology at the University of Wollongong, NSW, Australia.

The authors thank Rachelle Hollander and John King for their observations and insightful comments that helped make this column more robust.

Copyright held by Author/Owner(s).