Guest Editor's Introduction

Attention Paid Versus Paying Attention in Pervasive Computing

Joseph A. Paradiso
MIT Media Lab

Daniel Siewiorek
Carnegie Mellon University

FROM DREAMS TO DEVICES

Verner Vinge, a noted science fiction author and retired computer science professor known to many of us, wrote a beautiful narrative on the seductive power of technology and knowledge in the preface of his award-winning 1992 novel "A Fire Upon The Deep"—a long-established theme in human lore that goes back at least to Adam and Eve. Ubiquitous sensing has deep roots in its own Tree of Knowledge—going beyond enabling today's applications of convenience, it portends to abstract the notion of presence itself, potentially ushering in a new kind of digital "omniscience."[1] Vinge went on to give us a crushing depiction of life under ubiquitous sensing of several kinds in "Fire's" 1999 prequel "A Deepness in The Sky," then projected the promise, peril, and social change that such capability would provide in the near future with his subsequent 2006 novel "Rainbows End" (thought significant enough to our community for one of Vinge's bridging novellas to be published in IEEE Spectrum in 2004).[2] The wonderful, weird, and worrisome nature of this transformed world (very much enabled by Pervasive Computing) that Prof. Vinge and others envisioned early within speculative fiction is ever more palpable now, as it enters into the mainstream popular debate (e.g., see https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html for a list of relevant articles published in The New York Times from June 2019 to February 2020).

Accordingly, in this Special Issue, we set out to explore this topic as projected into twin demons relating to attention—unwanted attention paid to us versus our own attention being unwittingly diverted—i.e., the danger of living in a Panopticon versus the specter of our personal cognitive resources being fragmented and deleteriously diverted by too many competing digital factions that exploit intimate knowledge of their users (itself informed by ubiquitous sensing).

This is on our turf. It seems like only yesterday when small gatherings at the edge of the computer science/EE academic and research communities interested in HCI, sensors, wireless, and embedded computing met in workshops at our canonical retreats like Semi Ah Moo in Washington or Schloss Dagstuhl in Germany to plot out the future of what we then called, for the most part, Ubiquitous or Pervasive Computing. Inspired by Marc Weiser's seminal vision of less than a decade earlier,[3] we dreamed big, and before appropriate wireless infrastructure and networking paradigms were appropriately in place, we cobbled together our concepts and demos to shine a bit of light into what this now-termed "Internet of Things" world

Digital Object Identifier 10.1109/MPRV.2020.2986903
Date of current version 14 May 2020.

Published by the IEEE Computer Society

would be like. What seemed almost fanciful 20 years ago has become the norm. With low-power wireless options and agile cloud computing now abounding, sensors are indeed getting everywhere, and with advances in machine learning and common sensor posting standards, this ubiquitous data can increasingly be leveraged for nearly infinite purpose. But with our success comes many levels of societal concern—indeed, some in the EE/CS community whose research ushered in these revolutions now seem to lament their role in what we see as detrimental societal consequences.

(UNWANTED) ATTENTION PAID TO US

Surveillance capabilities once accessible in limited ways by law enforcement or intelligence agencies are now potentially endemic, as we are surrounded by microphones and cameras constantly monitored by tireless AIs, we wear or carry GPS tracking devices, and in general, radiate increasing numbers of bits everywhere we go. Turning sensor-laden items off is less of an option - there is not generally an "OFF" switch, and if we manage to power some down, there are already too many smart objects entering our environment to account for. Research has for years explored frameworks to manage privacy[4] and dynamically throttle the quality and quantity of information we leave behind[5,6] or restrict what can be done with it,[7–9] but most have been sandbox implementations in an idealized world, where all players willingly live within a framework that is now quite balkanized and too easily subverted. Like unified password management or payment systems, will we eventually be able to trust a single entity that will pull a dynamic digital curtain around us as we traverse different segments of our lives, spanning devices from Amazon, Apple, Google, Govee, Sengled, Sdeter, Wyze, Wansview, etc., at home, work, transit, and abroad without users having to deal with the details? Our homes and cars already have become multimodal wireless sensor stations—those of us who own a Tesla have eight potentially networked cameras already sitting in our driveway. And how much can we depend on these great gatekeepers to truly honor our notion of privacy—"Who will watch the watchmen?"—indeed, massive and often harmful breaches of data seem to be a catchphrase of our epoch. The legal tension between digital services hoarding personal sensor data versus governments and powerful entities who want access has already surfaced even before recent Alexa subpoenas,[10] and we only see the tip of the iceberg in the illicit battle for it.

An aspect of the vast and complex space of securing our personal devices is touched on in one of the articles in this issue, "Betrusted: Improving Security Through Physical Partitioning," by Andrew "Bunnie" Huang, which proposes a modular mobile device that restricts its vulnerability to being compromised and discusses extending these ideas to generic IoT systems.

On the other hand, the increase in convenience and capability that our sensors and their associated services contribute to our lives are becoming undeniable and indispensable, and we begin to live in what was posed as a "utopic" digital age in those many now classic concept videos our community produced across many decades.[11] Just to give a few examples, shared cameras have been demonstrated to catch serious criminals,[12] and sensors in our homes, in our pockets and on our wrist reduce energy consumption and keep us fit. Writing this in the time of COVID-19 quarantine, dynamic tracking of phone/user locations,[13,14] as well as data automatically posted from connected thermometers[15] can provide estimates of contagion and disease spread. We are now openly streaming video from an array of Kinects installed across the currently quarantine-vacated MIT Media Lab building (originally for research on interactive pervasive displays[16]) in order to connect the recently-evicted occupants to their former home and maintain a sense of unity. In this case, together with the daily video conferencing we are all doing now, ubiquitous cameras are bringing us together in an era of mass separation.

Notions of privacy have likewise changed across years and generations—we enter a strange, fragile projection of the world David Brin envisioned in his 1998 book "The Transparent Society," where all users too willingly give information away that would have been thought

deeply personal in prior years, although there are hints that this is starting to turn.[17] Meanwhile, context and data fusion engines pull our passively emanated digital detritus together, hence we unwittingly release much more detail than we suspect.[18] The lead author remembers his excitement as a child when first typing his name into a building-sized IBM computer in the early 1960s and saw that it was remembered—now so much about us is latched so deeply into a universe of servers and networks that truly unplugging is a gargantuan effort and commitment.[19]

We are already witnessing very serious fallout from the weaponization of data gleaned from social networks with targeted distortion of truth injected back.[20] The consequences that we are living with now can all become much worse, when powerful bad actors, authoritarian regimes, etc. hack or casually exploit information from distributed sensors for direct harm and threat or even very disturbing aspects of "societal control." Some of this is already happening.[21] Ultimately, this breaks the Transparent Society's symmetry, as there is a tremendous power/data imbalance between individuals versus corporations or governments. Yes, the internet empowers everyone with a megaphone, but we are also seeing that this can be a chaotic amplifier cascading into an easily manipulated mob mentality.

Furthermore, recent advances in microelectronics, MEMS, low power operation, and energy scavenging are enabling ever smaller sensory "bugs" that bad actors can hide in our environment with increasing effectiveness. Can we again "take control" here, be assured that we can escape from being monitored when it suits us, and achieve a lasting trust in our devices? Or will we risk an "Enemy of the State" existence (alluding to the popular 1998 film), living in fear of what the phone in our pocket emanates,[22] what the camera on the corner senses, or what the accelerometer tossed onto our walkway detects? Will future exterminators sweep for electronic as well as organic bugs, if not hybrids?[23] Or will achieving actual privacy be an escalating battle of threat and countermeasure—a mode long familiar to espionage[24] and conceptually explored for decades by artists and critical designers.[25] This is the world in which cybersecurity has lived for decades, and that struggle quickly extends well into everyday physicality.

Addressing the rubric of ubiquitous sensing, another of the articles in this issue, "Quantifying the Politics and Physics of Ubiquitous Sensing Using Velliance Flux," by Ryan Janzen, introduces a framework under which the regions of "view" from different types of installed sensors can be quantified and weighted by factors like resolution, societal impact, and ownership of data. Suggestions are made for ways to measure this "veillance" parameter, and although the practicality of implementing some may be limited, the article launches a vital conversation about defining and quantifying metrics for what sensors actually do in a society.

OUR ATTENTION (UNWITTINGLY) DIVERTED

George Orwell's seminal novel from 1949, "1984" had state-mandated cameras installed in our living rooms, but most of us now willingly put streaming cameras all over our homes. Ubiquitous surveillance, at least in Western Economies, rides on the seductive Trojan Horse of consumer electronics, giving rise to what Zuboff has recently termed "Surveillance Capitalism."[26] It has been long established that there is large economic value coming from our sensors and data—information that can be used to improve our lives, while also binding us into behavior that can work against our best interests. The smart environments that IoT enables will get to know us better than we know ourselves—sure our "digital butlers"[27] can do our bidding without us needing to explicitly tell them everything, but also expose us to unwitting manipulation if they are also governed by other agendas. How will today's overwhelmingly distracting online experience, with ubiquitous websites exploding with all manner of "click bait" to lure us into deep visceral pits, scale to the everywhere immersive experience that pervasive displays and augmented reality glasses promise? Can we avoid garish nightmares, such as portrayed in Keiichi Matsuda's fanciful short "Hyper-Reality" (see http://hyper-reality.co/)?

Perhaps leveraging preferences and dynamic models of users can help to offload this, but we already see that being used for further manipulation, with "ads" targeted more directly towards influencing us, or more insidiously, presentation of distorted information or "fake news" in ways personally tailored captivate our attention and increase their effectiveness. Are there means of putting users in true control here, with their precious and limited attentional capability respected and augmented rather than diverted, diminished, and exploited?

This magazine has explored attentional interfaces in the past,[28] but the attention economy develops very quickly and has many dimensions. Two articles in this issue explore facets of measuring and responding to user attention. "Toward Cognitive Load Inference for Attention Management in Ubiquitous Systems," by Pejovic *et al.* concerns measuring user capacity in the physical world, while "How Far Are We From Quantifying Visual Attention in Mobile HCI?" discusses means of measuring user attention to Mobile devices.

LOOKING FORWARD

We stand today at a unique precipice, and the pervasive/ubiquitous computing community gave us a first look at this edge. As an inspirational Peter Hammill lyric quotes, "There is no escape except to go forward"[29]—just like airplanes and cars now need their sensors and computers to function (and for increasing numbers of people living with medical implants, this is also true for their bodies), ubiquitous sensing solutions are already woven too deeply into our society to unplug. Furthermore, most of us would agree that the familiar adage "we ain't seen nuthin' yet" applies here—as technologies that have caused so many issues at arms-length propagate into wearables and eventually implantables, and our brains effectively extend into the cloud via precognitive interfaces, many accepted notions like the nature of presence and the boundaries of individual identity will look quaint. Observing the unforeseen consequences of what our utopian aspirations have already achieved, and despite the intrinsic nonlinear twists in this rapidly arriving future, we need to accelerate innovation on protective-while-enabling societal, ethical, legal, commercial, and even anthropological frameworks, together with the technical solutions that will put us into a better place when we get to the next level.

REFERENCES

1. G. Dublon and J. A. Paradiso, "How a sensor-filled world will change human consciousness," Scientific American, pp. 36–41, Jul. 2014.
2. V. Vinge, "Synthetic serendipity," *IEEE Spectrum*, vol. 41, no. 7, pp. 35–44, Jul. 2004.
3. M. Weiser, "The computer for the 21st century," Scientific American, no. 265, pp. 94–104, 1991.
4. G. Iachello and J. Hong, "End-user privacy in human-computer interaction," *Found. Trends Hum.-Comput. Interact.*, vol. 1, no. 1, pp. 1–137, 2007.
5. N-W. Gong, M. Laibowitz, and J. A. Paradiso, "Dynamic privacy management in pervasive sensor networks," in *Proc. Ambient Intell.*, Oct. 25–29, 2010, pp. 96–106.
6. M. Langheinrich, "Privacy in ubiquitous computing," in Krumm, J. (ed.), *Ubiquitous Computing*. Boca Raton, FL, USA: CRC Press, Sep. 2009.
7. D. J. Weitzner, H. Ableson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information accountability," *Commun. ACM*, vol. 51, no. 6, pp. 82–87, Jun. 2008.
8. A. Pentland, "Reality mining of mobile communications: Toward a new deal on data," in *The Global Information Technology Report 2008-2009: Mobility in a Networked World, World Economic Forum*, S. Dutta and I. Mia, 2009, ch. 1.6, pp. 75–80.
9. J. Lanier, "Jaron lanier fixes the internet," The New York Times, Sep. 23, 2019. [Online]. Available: https://www.nytimes.com/interactive/2019/09/23/opinion/data-privacy-jaron-lanier.html
10. G. Sauer, "A murder case tests Alexa's devotion to your privacy," Wired, Opinion, Feb. 28, 2017.
11. For a list of classic UbiComp-related videos before 2004, see, for example, the listing from Steven Intille's 2003 MIT IAP Class. [Online]. Available: http://web.media.mit.edu/~intille/teaching/ubicomp-videos/ubicomp-videos.htm
12. J. Healey, *Surveillance Cameras and the Boston Marathon Bombing*. El Segundo, CA, USA: LA Times, Apr. 17, 2013.

13. J. Dylag, "A new app would say if you've crossed paths with someone who is infected," *MIT Technol. Rev.*, Mar. 17, 2020. [Online]. Available: https://www.technologyreview.com/s/615372/coronavirus-infection-tests-app-pandemic-location-privacy/?set=615328&set=615328
14. S. Wodinsky, *Hong Kong Introduces Invasive Location-Tracking Bracelets, Promises They're Not That Invasive*. Gizmodo, Mar. 19, 2020. [Online]. Available: https://gizmodo.com/hong-kong-introduces-invasive-location-tracking-bracele-1842414923
15. D. G. McNeil Jr., "Restrictions are slowing corona virus infections, New Data Suggest," The New York Times, Mar. 30, 2020. [Online]. Available: https://www.nytimes.com/2020/03/30/health/coronavirus-restrictions-fevers.html
16. N. Gillian, S. Pfenninger, S. Russell, and J. A. Paradiso, "Gestures everywhere: A multimodal sensor fusion and analysis framework for pervasive displays," in *Proc. ACM Int. Symp. Pervasive Displays*, Jun. 2014, pp. 98–103.
17. J. Beck, "People are changing the way they use social media," The Atlantic, Jun. 7, 2018. [Online]. Available: https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/
18. S. A. Thompson and C. Warzel, "Twelve million phones, one dataset, zero privacy," The New York Times, Dec. 19, 2019.
19. N. Popper, "How a bitcoin evangelist made himself vanish, in 15 (Not So Easy) steps," The New York Times, Mar. 12, 2019.
20. N. Confessore, "Cambridge Analytica and Facebook: The scandal and the fallout so far," The New York Times, Apr. 4, 2018.
21. P. Mozur and A. Krolik, "A surveillance net blankets china's cities, giving police vast powers," The New York Times, Dec. 17, 2019.
22. A. Greenberg, "Snowden designs a device to warn if your iphone's radios are snitching," Wired, Security Section, Jul. 21, 2018.
23. H. Pimentel, "Cyborg insect drones: research, risks, and governance," UC Davis Environmental Law Report, Dec. 1, 2017. [Online]. Available: https://law.ucdavis.edu/centers/environmental/files/2018-Spring-papers/Cyber-Insect-Drones-Heraclio-Pimentel-Jr.–Fall-2017.pdf
24. E. Hazletine, *The Spy in Moscow Station*. New York, NY, USA: Thomas Dunne Books, 2019.
25. K. Hill, "Activate this 'bracelet of silence,' and Alexa can't eavesdrop," The New York Times, Feb. 14, 2020.
26. S. Zuboff, "The age of surveillance capitalism – the fight for a human future at the new frontier of power," PublicAffairs, New York, 2019.
27. N. Negroponte, *Being Digital*. New York, NY, USA: Alfred A. Knopf, Inc., 1995.
28. A. Ferscha, J. Paradiso, and R. Whitaker, "Attention management in pervasive computing," *IEEE Pervasive Comput. Mag.*, vol. 13, no. 1, pp. 19–21, Jan.–Mar. 2014.
29. Recording: "Lemmings (including Cog)," from the LP *Pawn Hearts* by Van der Graaf Generator, Charisma Records, London UK, 1971.

Joe Paradiso is the Alexander W. Dreyfoos (1954) Professor in Media Arts and Sciences at the MIT Media Lab, where he directs the Responsive Environments group and serves as the associate academic head. He received the Ph.D. degree in Physics from MIT in 1981 and the BSEE degree from Tufts University in 1977, and joined the Media Lab in 1994 after developing spacecraft control and diverse sensor systems at Draper Laboratory and high-energy physics detectors at ETH Zurich and CERN Geneva. Much of his current research explores how sensor networks augment and mediate human experience, interaction and perception. He is a senior member of the IEEE and AIAA and is a member of the APS and Sigma Xi. Contact him at joep@media.mit.edu.

Daniel P. Siewiorek is the Buhl University Professor of Electrical and Computer Engineering and Computer Science at Carnegie Mellon University. He has designed or been involved with the design of nine multiprocessor systems and has been a key contributor to the dependability design of over two dozen commercial computing systems. He leads an interdisciplinary team that has designed and constructed over 20 mobile computing systems. He is a Fellow of IEEE, ACM, and AAAS and is a member of the National Academy of Engineering. Contact him at dps@cs.cmu.edu.