KATHERINE ALBRECHT

KATINA MICHAEL

Connected: To Everyone and Everything

The activist group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) was founded in 1999 by Katherine Albrecht. The very same year Kevin Ashton, co-founder and executive director of the then Auto-ID Center at M.I.T., made a presentation to Proctor & Gamble with a title that included the phrase "Internet of Things." According to Ashton, "the most numerous and important routers of all" are people [1], but people have limitations and are not very good at capturing data about objects in the physical world.

By 2001, Ashton's automatic identification vision became a lot clearer. At the Auto-ID Center during a Forrester Executive Strategy Forum he stated: "In nature, identification is a matter of life and death. If you can't identify things, you can't count them, you can't work out whether or not you can eat them, you can't work out whether or not they are friends or foe" [2]. All this was in the context of a discussion with an African tracker, emphasizing how a predator decides to attack a herd of zebra to "singulate," "hunt," and finally to "exhaust" [3].

It is true that the "connectedness" offered by the Internet of Things is extremely powerful, and has tremendous possibility, but as far as people are concerned, there are two fundamental, and potentially fatal, flaws to its vision. The first flaw is that people are *not* "things" but as soon as they are incorporated into the Internet of Things, they *become* things, at least in the eyes of the system. In addition, people potentially become prey as well, as we have seen in recent events – prey for marketers, for overzealous security arms of government, and for a whole lot more.

People are not mere "objects." Placing numbers on individuals and putting them on equal footing with cans of cola and bags of dog food is simply dehumanizing [3]. At one point, Kevin Ashton was planning a book tentatively titled *Soda with Souls* [4], implying that an RFID sensor could imbue inanimate objects with a spiritual essence. Of course the reality is just the reverse, because an underlying trajectory of all these sensors is human beings. Far from numbers enhancing the soul, putting a number onto a person all but denies that persons humanity. The terrible evidence for this is still with us from our not too distant past [5], [6].

The second flaw is that linking objects to subjects *en masse* may someday sound the death knell to our fundamental human right to privacy [7]. Ashton's vision of people becoming the most important "routers" of all indicates this. Routers act like gateways and are devices that forward data packets on between

Digital Object Identifier 10.1109/MTS.2013.2291170
Date of publication: 9 December 2013

networks, which is likely where the "people as sensors" paradigm is headed [8]. Recently, Cisco Systems ratcheted up the original language of the Auto-ID Center's vision. Rather than simply call it the Internet of Things, they now enthuse that we are headed toward an Internet of *Everything*. In light of this, we should perhaps now be considering the Internet of All Things, in other words, the Web of Things and People (WoTaP) [9].

Relationships today are more relevant than ever – that is, truly meaningful human relationships – because of all the clatter of social networks that would try to reduce them to marketing links and data mining insights and other detritus of the machine that is consuming real love between people.

Relationships have become a key currency for all these new technologies – the fuel that makes them run: relationships between people and things, between people and their environment, but especially between people and each other. Social science researchers look at the complex taxonomy of online social networks and shout "hooray," believing that these relationships herald a new era of connectedness [10]. Marketers also shout for joy with dollar signs in their eyes. Witness the recent changes at Google and Facebook for a case in point "now we can connect photos with product endorsements" [11]. Unless we can count people, unless we can number and track them, not only can we not hunt and track them, but we can't monetize them. So-called "smart" technologies and ubiquitous sensors make this easier than ever before.

The changes that have taken place in the 14 years since the Auto-ID Center and CASPIAN were founded represent a profound shift. Rather than shy away from the dehumanizing aspect of numbering and tracking people, instead of opposing it with boycotts and legislation, *we* the "watched," the information prey, have welcomed this technological invasion into our midst like a Trojan horse, bringing surveillance tools into the very inmost private centers of our lives.

This should not surprise us. The agenda has been set by big companies like IBM, which has been referring to a "smart planet" since 2008 [12], [13]. Plans around this smarter planet were already well underway as far back as 2001, when IBM received a patent for the "Person Tracking Unit" (#20020165758 Identification and Tracking of Persons Using RFID-tagged items) [14], and laid the groundwork for visual surveillance through its People Vision research project, now renamed IBM Smart Surveillance System [15].

Where this truly becomes interesting (or alarming, depending on your world view) is in plans to link up technologies for tracking and surveillance of people with near total omniscience of their environment. This is the essence of the smart planet, or the "planetary skin," as a partnership between Cisco and NASA R&D has claimed [16]. But while smart planets are supposed to have everything to do with cities, and smart grids, and smart meters, and monitoring bridges, and weather patterns, their real potential is in the feedback mechanisms that pass human-centric data through wireless sensor networks (WSNs). These sensors, sprawled all over our built and natural environment, affixed to people, animals, trees, transport vehicles, lampposts, and eventually *everything*, are designed to send back messages to the cloud and in turn drive smarter analytics. In sharing this data openly, we are promised new efficiencies of scale and a revolution of data-driven innovation.

> We, the information predators and the information prey, must ask who is made smarter and who will ultimately be empowered by these so-called intelligent systems.

Predictive analytics, machine learning, and big data [17] will allegedly give us greater insights than ever before on how we can maximize our limited resources. We are promised a fairer distribution of energy, better emergency warning systems, a reduction in criminal activity, and the power of crowdsourcing to lead us to a better, safer, and more informed world.

What is wrong with this model of advancing our potential humanity? We seem to want not only to quantify the planet, our countries, our cities, our neighbourhoods, but even – and perhaps especially – ourselves! But these are also, as readers of Gilles Deleuze have recognized, *technologies of control* [18].

We now return to the humble frequent shopper card, which, along with the credit card, was the earliest form of a numbering system designed primarily for the monetization of the individual [19]. We claim here that not too many have ever profited from such a scheme, save for the retail companies who issue them [20]. Again, like a Trojan horse, however, these devices have found their way into the wallets and onto the keychains of a majority of consumers in the U.S. and across the industrialized world. Adoption rates of frequent shopper cards stand at nearly 90% of U.S. and U.K. households that have enrolled in at least one, whereas adoption in Australia of the FlyBuys scheme in 2009 was more circumspect with one in four adults registered into the scheme [21]. However, consumers do not knowingly volunteer their personal shopping information to big business and government; they do so unawares [22]. By the time people realize these tools cut both ways, they have already become entrenched, accepted and (*yawn*)

business-as-usual. Of course, that is also the case today with many of the other whiz bang gadgets the data captors would like us to adopt. From search engines and "free" email to smartphone apps and toll transponders, like TVs that watch us and store shelves that take our photos - everything is bugged. Soon they'll be watching the very bread we eat. Oh wait, they already are! Voluntary uberveillance now pervades most of our society [23].

The marketing pitch, of course, is that the quantified movement will herald the solution to the world's problems – and our own individual personal problems. Monitoring our weight and exercise levels, recording our every thought and sniffle, tracing our every movement and location, all promise to make us better, safer, and stronger as we forge a brave new world of data-driven human perfection. Our new ability to quantify the self, to segment the self, to disembody individual parts, and to provide all that data effortlessly is indeed a revolution. But will all that quantification really improve the experience of *living* – of breathing, worshiping, raising children, interacting, marvelling, loving – for those who are being sliced and diced [24]? It is sadly all too true, as Ashton well pointed out, that computers *do* reduce people to bits and bytes: "you can't eat bits, burn them to stay warm or put them in your gas tank" [2]. And you can't love them, either.

We challenge the idea that the Internet of Things will usher in a new era of human health and happiness [25]. This does not mean we do not embrace positive computing initiatives. *We clearly do* – as we are using them to write this paper. The creative genius and pioneering spirit of our innovators and engineers is also not in dispute here. But at the same time we shouldn't be fooled. At its core this perceived utopia contains both a danger and a deadening.

The danger is the very real threat it poses to our safety and privacy [26]. At the end of the day there is very little difference between tracking and surveillance. Remove the watcher, and tracking and surveillance are one and the same thing. We, the information predators and the information prey, must ask who is made smarter and who will ultimately be empowered by these so-called intelligent systems [27]. Whether by radio-frequency identification (RFID), near-field communications (NFC), bar codes (e.g., Quick Response codes), global positioning systems (GPS), or sensors of all types (including for image capture) – someone is watching. What we carry, or even bear, and the data we collect thereby, may be used either to help us, or to cause us irreparable damage [28].

Secondly, it poses a threat to the very things we hold dear and claim to be trying to use it to protect – precisely, our human dignity and our happiness [29]. These are things that cannot be quantified – at least not yet, and we suspect they never will be! These include the light in the eyes of our children, the ineffable beauty of the natural world, the joy of a hug from a friend, the exhilaration of a cold, snowy morning. Blanketing the earth and injecting each other with sensors will do little to enhance these experiences, and would even threaten to do harm.

We should not don rose colored glasses (or Google glasses, for that matter) thinking all this technology will lead us to a better, happier world. Independent of how clever machines will soon become, it's hard to truly believe that a world governed by automata would be better than one with a rhythm and agenda set by people – democratized, functioning organically from the bottom up rather than systematically from the top down. While technology promises to put the power into all of our hands, it has a tendency to wind up as a one way, top-down control street (like aerial drones, and the NSA's prism surveillance program, to name just two examples).

The Internet of Things may well lead to a "better" and "smarter" planet, but we challenge the notion that we as human beings will be improved as a result [30]. The regular you's and me's may think we're in charge of our shopper cards and our mobile apps and our smart fridges – but they all feed into the same voracious machine – the global brain. The contents of that brain may be comprised of our data, and bits of our lives, but let's not fool ourselves, it's not ours. It belongs to Google, and IBM, and Cisco Systems, and the NSA, and the TSA, and the global MegaCorp that owns your local supermarket. If you don't believe us, just try removing "your" data from their database. We have rich myths about such things as Greeks bearing gifts. We need a new mythology – a new myth – about the people who sought total control over themselves, and wound up having none.

Author Information

Katherine Albrecht is an executive with the private search engine StartPage. She is also the founder and director of CASPIAN.

Katina Michael is an associate professor in the School of Information Systems and Technology at the University of Wollongong, NSW, Australia.

Acknowledgment

The title of this paper was inspired by Eric Bibb's *Troubadour Live* single titled: "Connected" which was produced in 2011 (https://myspace.com/ericbibb/music/song/connected-81491541-89777198).

References

[1] K. Ashton, "That 'Internet of Things' Thing: In the real world, things matter more than ideas," *RFID J.*, June 22, 2009: http://www.rfidjournal.com/articles/view?4986#sthash.NsRaiwEl.dpuf.

[2] K. Ashton, "Kevin Ashton, Auto-ID Center, at Forrester Executive Strategy Forum," videotape, Nov. 7–9, 2001, quoted in K. Albrecht and L. McIntyre, *Spychips*. Nelson Current, 2005, p. 208.
[3] K. Albrecht. "RFID tag - You're it," *Scientific American*, September 2008, pp. 72–77.
[4] Mr. Kevin Ashton, *ZoomInfo*, Jan. 8, 2013; http://www.zoominfo.com/p/Kevin-Ashton/4435917.
[5] P. Levi, *The Drowned and the Saved*. New York, NY: Vintage, 1989, p. 94f.
[6] A. Solzhenitsyn, *The Gulag Archipelago (1918–56)*. Harvill Press, p. 346f.
[7] K. Albrecht, "RFID: The doomsday scenario," in *RFID: Applications, Security, and Privacy*, S. Garfinkel and B. Rosenberg, Eds. NJ, U.S.A.: Addison Wesley, 2006, pp. 259–273.
[8] M.F. Goodchild, "Citizens as sensors: the world of volunteered geography," *Geo J.*, 2007, pp. 69, 211–221.
[9] K. Michael, G. Roussos, G.Q. Huang, R. Gadh, A. Chattopadhyay, S. Prabhu, and P. Chu. "Planetary-scale RFID services in an age of uberveillance," *Proc. IEEE*, vol. 98, no. 9, pp. 1663-1671, 2010; http://works.bepress.com/kmichael/186.
[10] M.G. Michael and K. Michael, "Privacy- the times they are a-changin'," *IEEE Technology & Society Mag.,* vol. 31, no. 4, pp. 20-21, 2012.
[11] Google. Terms of Service update, *Google: Policies and Principles*, Oct. 11, 2013; http://www.google.com/policies/terms/changes/.
[12] IBM, *Smarter Planet*; http://www.ibm.com/smarterplanet/, accessed Oct. 16, 2013.
[13] A. Kamanetz, "IBM's 'Smarter Planet' initiative to be announced today, *Fast Company*, Nov. 6, 2008; http://www.fastcompany.com/1071950/ibms-smart-planet-initiative-be-announced-today-you-heard-it-here-first, accessed Oct. 16, 2013.
[14] K. Albrecht and L. McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*. TN, U.S.A.: Nelson Current, 2005, pp. 32–35.
[15] K. Michael and M.G. Michael, "Converging and coexisting systems towards smart surveillance," *Awareness Mag.*, June 19, 2012; http://www.awareness-mag.eu/view.php?article=003989-2012-06-19&category=Networks+%26+Infrastructure.
[16] PSI. "PSI: About us (History)," *Planetary Skin Institute;* http://www.planetaryskin.org/about-us/history, accessed Oct. 16, 2013.
[17] K. Michael and K.W. Miller. "Big data: New opportunities and new challenges," *IEEE Computer*, vol. 46, no. 6, pp. 22–24, 2013.
[18] M. Poster and D. Savat, Eds., *Deleuze and New Technology*. Edinburgh, U.K.: Edinburgh Univ. Press, 2009, p.120.
[19] K. Albrecht, "Supermarket cards: The tip of the retail surveillance iceberg," *Denver Univ. Law Rev.,* pp. 534–539, 558–565, 2002.
[20] K. Michael, "The land of milk and money," *The Drum*, Sept. 25, 2013; http://www.abc.net.au/news/2013-09-25/michael-the-land-of-milk-and-money/4980102.
[21] C. Williams, *Research - Unley Business Loyalty Card Program*, Business and Economic Development, http://www.unley.sa.gov.au/webdata/resources/files/USLT_Item_21_Att1.pdf.
[22] K. Albrecht, "Supermarket 'loyalty' cards and consumer privacy education: An examination into consumer knowledge about cards' data collection function," D.Ed. thesis, Harvard Univ., 2006.
[23] M.G. Michael and K. Michael, "Towards a state of uberveillance," *IEEE Technology & Society Mag.*, vol. 29, no. 2, pp. 9–16, 2010.
[24] M. Eldred, "Technology, technique, interplay: Questioning Die Fragenach der Technik," *IEEE Technology & Society Mag.*, vol. 33, no. 2, pp. 13–21, 2013.
[25] K. Pretz, "Exploring the Impact of the Internet of Things: A new IEEE group is taking on the quest to connect everything," *The Institute*, Oct. 7, 2013, http://theinstitute.ieee.org/technology-focus/technology-topic/exploring-the-impact-of-the-internet-of-things.
[26] K. Albrecht, "Keynote address: RFID and Privacy," in *Proc. RFID Privacy Workshop*, MIT Media Labs, Nov. 15, 2003; http://www.media.mit.edu/events/workshop-rfid.html, accessed Oct. 16, 2013.
[27] P. Gautier, "Interview with Michel Quesnel about the book: *Internet des Objets, Internet mais en mieux* (*Internet of Things, a better Internet?)* by P. Gautier and L. Gonzales," Afnor Ed., 2001); http://www.i-o-t.org/post/Interview_with_Michel_Quesnel_Internet-of-Things.
[28] M.G. Michael and K. Michael. "The fall-out from emerging technologies: On matters of surveillance, social networks and suicide," *IEEE Technology & Society Mag.*, vol. 30, no. 3, pp. 15–18, 2011.
[29] R. Capurro, M. Eldred, and D. Nagel, *Digital Whoness: Identity, Privacy & Freedom in the Cyberworld*, Germany, ontos verlag, 2013.
[30] P.-P. Verbeek. *Moralizing Technology: Understanding and Designing the Morality of Things.* Chicago, IL: Univ. of Chicago Press, 2011.

Announcing Three New *T&S Magazine* Associate Editors

Beginning January 1, 2014, *T&S* welcomes three new Associate Editors:

Katherine Albrecht, Ed.D is an internationally recognized privacy expert with a Doctorate in Human Development and Psychology from the Harvard University Graduate School of Education, Cambridge, MA. She also received a Masters in Education from Harvard, in Technology, Innovation, and Education, and she holds an undergraduate degree in Business Administration and International Marketing from the University of Southern California.

Khanjan Mehta is the Founding Director of the Humanitarian Engineering and Social Entrepreneurship (HESE) Program and Assistant Professor of Engineering Design at Penn State University.

Xi Chen, Ph.D., is a full professor in the School of Business at Nanjing University, China. Previously, he has been a Visiting Scholar of the Michael G. Foster School of Business at the University of Washington, U.S.A..

Additional information will appear in the Spring 2014 issue of *T&S*.

Digital Object Identifier 10.1109/MTS.2013.2293072
Date of publication: 9 December 2013