

**Panopticon as a metaphor of the Internet of Things – why not?**  
**But if it were the opposite?**

Recently, the ‘Council on the Internet of Things’ website published an article in Chinese<sup>1</sup> by Yongmou Liu, Associate Professor of Philosophy of Science and Technology, School of Philosophy, Renmin University of China, which is a warning against the danger of the Internet of Things becoming “a domineering tool”. The *Panopticon* is used as a metaphor for describing a “surveillance society” where technology is extensively and routinely used to track and record human activities and movements in ways which are invisible to ordinary people as they are watched and monitored. We can find already today examples of this in the tracking and recording of travel and use of public services, the frequent use of CCTV, the analysis of buying habits and financial transactions, and the workplace monitoring of telephone calls, e-mail and Internet use.

A few days following that publication, I had an interesting e-mail exchange with Rob van Kranenburg on the concept of Panopticon, and this reminded me of his book on the Internet of Things<sup>2</sup>, in which science fiction author David Brin<sup>3</sup> was evoked by Sean Dodson in his Introductory Chapter, to expand on the vision of a City of Trust that would emerge in place of a City of Control:

*“In our future cities (...) instead of a nest of cameras atop each lamppost, lies a near invisible network of wireless frequencies where almost any object and space can be located and monitored, found and logged as easily as an item on eBay or the price of a flight on easyJet (...) The City of Control is a place where the deployment of radio frequency identification tags (RFID) have become not just commonplace but ubiquitous. Objects, spaces and, yes, even people are tagged and given a unique number, just like web addresses are today. Notions of public and private have begun to dissolve; or are rendered irrelevant; notions of property are rapidly being rethought. Security is the defining issue for those who can afford it, but also for those that cannot. Very soon, access to parts of the city is being carved off: allowing the rich and powerful entry where they please and the poor have access where they are lucky. Every item you buy at the supermarket is being tracked and potentially data-mined, lest there be a combination of goods in your basket that the authorities don’t like. Your movements are watched, not by the use of crude cameras (which it transpires were rather poor at fighting crime anyway) but by tags embedded in your gadgets or in your clothes or even under your skin. Transmitted wirelessly and instantly they connect with satellite systems that record your digital footprint endlessly. Everything you buy, every person you meet, every move you make. They could be watching you. (...) The City of Trust on the surface looks very similar to the City of Control. But here the citizens have been given much more control; here*

---

<sup>1</sup> <http://www.theinternetofthings.eu/content/yongmou-liu-totalitarianism-or-democracy-preference-internet-things-and-its-risk-perspective>

<sup>2</sup> Rob van Kranenburg, *The Internet of Things. A critique of ambient technology and the all-seeing network of RFID*. Report prepared by Rob van Kranenburg for the Institute of Network Cultures with contributions by Sean Dodson, 2008.

<sup>33</sup> David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Basic Books, 06/01/1999, ISBN-13: 978-0738201443.

*pervasive systems have been embedded, but offered as an option rather than as a default. You leave your laptop on the train, no problem – with the ‘internet of Things’ you can locate it on a search engine, even arrange for it to be delivered back to your door.”*

Let’s remember what the Panopticon is. The concept designed by British philosopher and social theorist Jeremy Bentham in the late 18<sup>th</sup> century, refers to a type of building where an observer is allowed to observe (-opticon) all (pan-) inmates without them being able to tell whether or not they are being watched. Bentham devoted most of his efforts to developing a design for a Panopticon prison, but the concept is equally applicable to hospitals, schools, and other institutions.

The essential feature of Bentham's design was that the custodians should be able to view the prisoners at all times (including when they were in their cells), but that the prisoners should be unable to see the custodians, and so would never know when they were under surveillance. This goal was extremely difficult to achieve within the constraints of the technology then available, but something close to a realisation of Bentham’s vision became possible through 20<sup>th</sup> century technological developments, especially closed-circuit television (CCTV) cameras.

In the mid-70s, the Panopticon prison design was invoked by French philosopher Michel Foucault as metaphor for modern “disciplinary” societies and their pervasive inclination to observe and normalise. Foucault claimed that all hierarchical structures like the army, prisons, schools, hospitals and factories had evolved through history to resemble Bentham's Panopticon. He suggested that *power* and *knowledge* were interlinked in the Panopticon society – the essence of power itself could be summarised by the ability to “see-without-being-seen,” to have knowledge of the others that the others could never obtain.

Building on Foucault, contemporary essayists often assert that technology has allowed for the gradual and invisible deployment of panoptic structures throughout society. After Brin, Jensen and Draffan<sup>4</sup>, among others, have demonstrated how our society is being pushed towards a panopticon-like state, thanks to the proliferation of surveillance technologies. If we accept that vision of modern society, it comes to mind that the Internet of Things holds the potential of pushing the limits far beyond what has been until now state of the art of such technologies. I believe that person-to-object, object-to-person and object-to-object communications – the Internet of Things – will open up tremendous opportunities for market expansion and business profitability. But more fundamentally, a new proletariat – the *proletariat of objects* – will arise throughout the 21<sup>st</sup> century, taking over from the 18<sup>th</sup> century’s proletariat of peasants, the 19<sup>th</sup> century’s proletariat of workers and the 20<sup>th</sup> century’s proletariat of consumers. The driving force of the economy will no longer be the labour force or the purchasing power but actually the technical standards of the “smart” objects created by the humans. A time could come when the trillions of smart objects interacting with people in a “brave new world” – from *gizmos* to *spimes* to *biots*, according to

---

<sup>4</sup> Derrick Jensen, George Draffan, *Welcome to the Machine: Science, Surveillance, and the Culture of Control*, Thomson Gale, 10/11/2005.

Bruce Sterling's typology –will bring about their own revolution, rise up in revolt, herd the human race into Panopticon prisons, and punish those humans least able to respect their laws and jargon and to rid themselves of the specifically human characteristics which hold them at a distance from the centre of social activity. Human behaviour could be deterministically governed by processes outside human control, i.e. processes governed by technologies such as smart cameras, peer-to-peer surveillance networks, remote biometric identification, very short wavelength radio waves, Trusted Computing and Digital Rights Management, cognitive radio, remote interrogation of RFID “dust”, chemical analysers, and data mining. The pressure to adopt these technologies springs from the current political discourse as nations struggle to confront ill-defined threats. The perception that we live in a dangerous world grows and so grows also the social call for safety.

By comforting a form of government characterised by omniscient surveillance and mechanical law enforcement, the Internet of Things would make that humans will lose control over sensing and actuating objects. Let's imagine if the data from all social networks were combined with all the location data, call and SMS records for all mobile phones; then let's imagine combining all that data with data from retailer databases, credit agencies, voter registration records, real estate transactions, and so on. If all today's fragments of data were put together to form a coherent whole, this would create a powerful Panopticon society. The chance of such a society is high as the world is getting increasingly global and interconnected.

Furthermore, surveillance technologies will increasingly be “managed” by individuals themselves – the “threat” may actually come from ourselves. Using various technologies, such as GPS-enabled smartphones, we are beginning to measure ourselves in granular detail – how long we sleep, where we drive, what we breathe, what we eat, how we spend our time. We are storing these data casually, somewhere in the “cloud,” and giving third-parties broad access. There are more and more people using a wearable sensor that tracks their movement 24 hours a day to produce a record of their steps taken, their calories burned, and even the quality of their sleep; data is wirelessly uploaded to the Web so that they can monitor their activity and compare it with that of their friends.<sup>5</sup> This practice of self-surveillance will obviously decrease information privacy in quite challenging ways.

But is the Panopticon the metaphor of what we want for the Internet of Things? I had this discussion by e-mail with Rob van Kranenburg and of course we immediately agreed that it is not. There is no inevitability of a Panopticon dismal scenario; the future is not written yet. We feel it as a moral obligation to contemplate a bright scenario, one in which the Internet of Things will be designed to develop new usages that will empower individuals, not control them.

Here follows what Rob van Kranenburg wrote to me:

*“The Internet of Things is not destined to be ‘The Matrix’! However, given our knowledge and practical experience of history, the drivers for control and surveillance in governance*

---

<sup>5</sup> See for instance: Gary Wolf, *The Data-Driven Life*, The New York Times, 04/26/2010.

*systems and the military origins of the Internet and most digital services and applications, it is not illegitimate that this metaphor is brought forward. The Internet seems to bring possibilities and encourage practices for sharing and collaboration, open source solutions deep down in the protocols and competition on services and applications, and new alliances between old oppositions. Can the Internet of Things build on top of these developments? For this to happen we need to be consciously critical but positive about the potentials we are building now with lone entrepreneurs, SMEs, dozens of IoT platform contenders coming out of big industry as well as small bedrooms. So we need to find out what could be the opposite of Panopticon!”*

Said differently, what could be the metaphor of a free society where individuals are endowed with the capability to exploit their talents and realise their dreams, where social groups stand together, and where organisations adopt an ethical conduct? If we accept that Panopticon can be the metaphor for the surveillance society, the City of Control, the human enslaved by his objects, what could be the opposite concept for the freedom society, the City of Trust, the empowered individual?

If you share our analysis and the challenge that we’ve set for ourselves, please feel free to send your ideas to [info@theinternetofthings.eu](mailto:info@theinternetofthings.eu) with ‘New Year Contest’ in the header. In the jury:

- Gérald Santucci, Head of Unit “Networked Enterprise and RFID”, DG Information Society and Media, European Commission
- Rob van Kranenburg, co-author with Christian Nold of *Situated Technologies Pamphlets 8: The Internet of People for a Post-Oil World* (Situated Technologies Pamphlet 8)
- Francesca Bria is currently a PhD Researcher at Imperial College Business School
- Alex Bassi, Acting (for Hitachi, Ltd) as Technical Coordinator for the FP7 EU project "IoT-A"
- Alexander Gluhak is senior researcher at the University of Surrey, and technical manager of the SENSEI project
- Natacha Roussel, founder independant artist at *Experientiae electricae*