Internet of things: the greatest mass surveillance infrastructure ever?

Julia Powles

The word “thing”, in Old English, means a meeting or assembly. In the epic poem Beowulf, the eponymous hero declares he’ll “alone hold a thing” with the monster Grendel, who is terrorising the Danes in the great hall of Heorot. Beowulf uses “thing” euphemistically – it is a meeting that immediately descends into a fight.

The Icelandic parliament is still called Althing (Alþingi). But over the ages, “things” have gradually evolved from meetings to matter. Today, we primarily use the term “thing” to refer to objects. Even in this sense, however, things are still core to our political and social lives.

An appreciation that things have always been about community and politics, whether literally, or through the creation and respect of systems of private property, provides a useful backdrop to the recent book, Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up, by writer and professor of communication, Philip N Howard.

Howard’s thesis is that the much-hyped internet of things - the expanding network of connected devices throughout our homes, bodies, streets and communities - heralds a new political age he calls “Pax Technica”.

This pax will not be dominated by any one state, Howard argues, but by “a special kind of stability in global politics, revealing a pact between big technology firms and government”. The categories of democracy and dictatorship will fall. In their place, he claims, will be data-driven socio-technocracies, built on the intensive reporting of our behaviours, habits, tastes and beliefs, seamlessly transmitted by the devices we use, carry and interact with. We won’t need to express our political preferences and needs: our white goods and driverless cars will express them for us.

‘The most powerful political tool ever created’

Howard is excited by this vision; excited by two decades of work with communities empowered by social media; excited by the possibility to reinsert what he sees as civic counterpower into device networks. I am not excited by it – I am terrified, and let me explain why.

The arc of Howard’s argument is that an open, interoperable, global network means that “every dictator will face embarrassing videos he cannot block and outrage he cannot respond to”, and every region in crisis or transition will involve “people using digital media to try to improve their conditions, to build new organisations, and to craft new institutional arrangements”.

The consequence, he submits, is “the most powerful political tool ever created”.

More tension

This is Powles elaborating Howard’s ideas, setting them up for her critique, so she can make her intervention
Howard adopts a playbook that is indistinguishable from the freedom-to-connect narrative fronted by US big tech and government – the valorisation of openness, interoperability, and disruptive innovation by private companies; the demonisation of repressive regimes; and a superficial view of political economy, international relations, and institutional corruption.

The argument is bolstered with an impressive array of case studies of citizen-led activism and coordination through mobile phones and social media. Inspiring stuff, certainly, but far from fully-worked examples of stable, enduring, empowering governance.

Howard fails to get out of the gates on the internet of things. Apart from general handwaving to big data-enabled improvements in health, energy, environment and finance, he provides no convincing argument for the huge corporate and governmental data heist that will be enabled by networking everything in our physical environment, from our toasters to our coffee machines to our town squares. He claims that device networks will solve collective action problems, but there is little to show how this connectivity will empower the citizenry, as opposed to creating the greatest mass surveillance infrastructure ever conceived.

Howard acknowledges the dangers of surveillance, but he offers no opt-out. His solution to nefarious parties obtaining data is to just give out more data - to civic groups that he blithely assumes will organise and operate in the public good.

In this, he appears a convert to the church of big data; the computational theocracy. “Data will help us track good trends, monitor bad behaviour, and make reasoned decisions”, Howard claims. The world’s problems are all soluble, in other words, if only we have ever-more data and handfuls of networked citizen-analysts, thrown amongst the vast machine of corporate and governmental data-miners.

Worryingly, Howard offers no challenge to the proposition that networked things will all communicate, seemingly by default, with “the original manufacturer, the information services we subscribe to, national security agencies, contractors, cloud computing services, and anyone else who has broken into, or been allowed into, the data stream”.

A nebulous trade-off
And the reason we ought to accept this unpalatable, feudal state of affairs? The lures of big data, and the venerated openness of the network. Your toaster is hackable, yes (as may be the rest of these smoking guns in your city), but at the same time, in a nebulous trade-off, with “dictators dying off and the data trail of bad behaviour growing, the biggest dirty networks are on the brink of collapse”. And when the “modern state fails, the internet of things will provide governance”, Howard asserts, unconvincingly.
By tracking us in intensive and intrusive ways – not only in our homes, but in our vehicles and bodies – data-driven devices can nudge, manipulate and mould our behaviours, habits and preferences, limit our autonomy, and bring quantification, segregation and discrimination to what is currently a political economy held together by social fuzziness.

This fuzziness assists us individually – because we have control over who has, and importantly who does not have, personal information about us. But it is also important socially, unless we want to turn into an intensely individualistic, segmented, micro-financialised network of semi-autonomous, tethered beings.

We deserve a smarter solution that offers more than empty marketing rhetoric for “open”, “inclusive” monopolistic big tech business models.

At worst, it’s a terrifying blueprint for the end of politics, depoliticising our engagement with “things”, characterising the objects and relations that furnish our lives as “loss leaders for data flows” – data flows that offer nothing for us, and everything for a staggering, uncontrolled array of corporate and governmental actors.