

The Fridge's Brain Sure Ain't the Icebox



Kieron O'Hara • University of Southampton

I've never quite seen Harry Potter as a fount of wisdom in the same way as, say, Kant, Confucius, or Einstein are. And I'm slightly nervous that I will misquote this and be inundated with complaints from Those Who Care about the works of J.K. Rowling. However, when a character called Mr. Weasley opines that one should "never trust anything that can think for itself if you can't see where it keeps its brain," even the Potter skeptic has to admit that he's onto something.

I bring this up because of the emergence of the Internet of Things (IoT). This simple idea – giving physical objects unique identifiers, fitting them with sensors or actuation systems, and then hooking them up to the Net to communicate their data and receive their orders – is being anticipated with relish. Really dumb devices becoming smart via complex networked interaction – intelligence on the cheap. The International Data Corporation reckons that there will be 212 billion such devices by 2020, generating global revenues of US\$8.7 trillion.¹

The hype is easy to satirize.² Believe it or not, more than one person has invented smart underpants.^{3,4} (I have developed my own scenario about these, which is much more interesting than any that have made it into the press, although it raises some of the privacy issues I will discuss later, and is probably not suitable for a family magazine.) For some reason, every "hey-wow" account of the IoT mentions a fridge that tells you when your milk is past its sell-by date. Perhaps the fridge is compulsory. Anyway, I've mentioned it now, so my duty is done.

Beware the Data Monster

There is no doubt that the IoT is coming to a fridge near you. Expect wearables, instrumented bodies,

sensors in the environment and at home, apps to monitor pollution, traffic, and power usage, and trackers on everything in the global supply chain.⁵ The issues for the digital citizen are – of course – privacy and security. The data this blanket coverage will generate, even if it's only a fraction of the anticipated size, will be colossal, and will surely dwarf the big data we're so proud of today. This will be data about absolutely everything – where we go, what we do, how fit we are when we do it, what we switch on, what we buy, who we meet, and what routines we prefer.

The CEO of Volkswagen, Martin Winterkorn, whose contribution to the IoT via the instrumentation of his cars isn't small, has recently warned that even cute little Herbie is becoming a "data monster."⁶ Once we've driven back home, smart meters threaten to be incredibly disclosive. Although data need not stream directly to the utility for billing purposes, it must still go to a neighborhood aggregator that combines and anonymizes it across a geographical area so that the utility can predict future consumption and maintain its pricing model.⁷ Yet these streams tell us an awful lot – household devices' energy-use signatures are quite distinctive, so we can have a good guess at when the microwave went on or how many people had a shower,⁸ and so on, with almost all the devices we can mention.⁹

Worse, a potential security problem arises because the devices are small and individually dumb. We're approaching the anniversary of the first known large-scale IoT cyberattack, uncovered by security firm Proofpoint:

The attack that Proofpoint observed and profiled occurred between December 23, 2013 and January 6, 2014, and featured waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting

enterprises and individuals worldwide. More than 25 percent of the volume was sent by things that were not conventional laptops, desktop computers, or mobile devices; instead, the emails were sent by everyday consumer gadgets such as compromised home-networking routers, connected multimedia centers, televisions, and at least one refrigerator. No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location – and in many cases, the devices had not been subject to a sophisticated compromise; instead, misconfiguration and the use of default passwords left the devices completely exposed on public networks, available for takeover and use.¹⁰

You see? Stabbed in the back by that damned fridge.

If the devices can't be made secure, where in the architecture can security be safely located without imposing costs or creating vulnerabilities?

So What's New?

All this is reasonably well known. Any digital system raises privacy issues simply by furnishing persistent data trails, so it isn't surprising that the IoT needs thinking about.⁹ Julie Brill of the US Federal Communications Commission (FCC) recently mused that without safeguards to protect consumers, sensitive personal data could be used to make decisions about them, and that privacy and trust concerns might well prevent the IoT from reaching its potential.¹¹ This is of note for the digital citizen – the point, finally, of this column – because some of the privacy issues raised are specific to the IoT and especially hard to crack. Part of the reason for this is the IoT's potential ubiquity – how would you avoid it? But partly,

these problems are deep, and conceptually and technologically hard, too. Furthermore, the solutions aren't obvious.

What, then, are these specific issues?

The Demands of Security

The IoT will string together many devices that are small, cheap, and simple, and highly heterogeneous. Can we ensure that these devices are clever enough to implement decent security, to prevent problems such as those Proofpoint revealed? Remember that IoT devices' relative simplicity is going to be part of the business model – neither costs nor complexity should be high. Yet security creates its own demands, which will threaten that low-cost model. If the devices can't be made secure,

can't simply withdraw tens or hundreds of billions of devices in the way that a car manufacturer can withdraw faulty tires or petrol tanks.

Accountability

IoT systems are highly distributed, so the data will move around a lot. This is a problem for regulators. Of course all that transport increases the risk of interception, but perhaps more importantly, it's harder to trace where data is and what it's used for. This will make it much more difficult to hold people, companies, and institutions to account for (mis)use of data.

What Is Personal Data?

The simplicity of IoT devices means that the data they produce probably won't be personal data from which someone can be identified. However, the IoT's power stems not from the data in one device but from the network whose aggregated data might well be identifying. This situation, in which personal data isn't collected, is unusual, and data-protection practice might not be fully geared up to it at scale. We must understand the role of behind-the-scenes data collectors, or data brokers, in more detail.¹¹

Consent

In many cases, consent can be implied. No one puts on a pair of smart underpants without consenting to their data processing (let's not think too hard about the circumstances in which that sweeping statement might not be true). However, implied consent isn't a magic bullet in this space. If our normal, everyday environment is instrumented, then the implied consent model for IoT risks making life impossible for those who don't consent to having their data gathered and used. If we withdraw the need for consent, then the boost to our surveillance society will surely be excessive. This is a deeply thorny issue that academics are only now getting their heads around.¹²

where in the architecture can security be safely located without imposing costs or creating vulnerabilities? Will inflexibility have a cost if it's difficult to attach new devices to an existing network?

Future-Proofing

In many IoT scenarios, devices will be in place for several years – for example, embedded in major appliances such as the fridge (whose average lifespan, incidentally, is between 13 and 20 years depending on whether a freezer is included). Security must thus be implemented not only for the present day, but also for future circumstances that will be hard to predict. If hackers undo existing security arrangements, we

People Are in the Loop

People will be at the center of the IoT, bringing along all sorts of vulnerabilities beyond what we can model and predict in the technology (almost all security has this character, that the weaknesses are in the social engineering, not the technological stuff). For instance, I find it significant that the Proofpoint discovery was of an attack dated 23 December – it was over the Christmas period. Did the attack's success come down to many of the devices being Christmas presents, turned on and tested by grateful recipients, leading to a short period where a critical mass of devices was operational before users changed passwords from the defaults? I speculate, but perhaps that was a brief window of vulnerability completely unpredictable from an understanding of technical matters alone.

Who Decides?

These IoT privacy issues are all hard; some require legal thinking (meaning that we will be waiting not only for the slow grind of legislation, but also for courts to set precedents and make judgments about how old law applies to new technologies); others need technological innovation (and then each must ratify the other). Yet the process of sorting out these problems is also bedevilled by the complexities of deciding who should arbitrate. Regulating privacy is a complex matter, and in the particular case of the IoT, it isn't immediately obvious how it should be done. One important conclusion we must draw, however, is that the technology industry, and privacy by design (PbD), must play a prominent role.

Certainly government isn't in a good position to preserve confidence through regulation. Quite apart from the issues of jurisdiction (your fridge is Chinese, you bought it in the US, it's installed in Canada – who tells it what not to do?), government can't

credibly pose, post-Snowden, as a disinterested actor in the regulation of giant quantities of disclosive data. Meanwhile, market privacy solutions are unlikely to provide a quick win. Data has been commoditized and monetized so successfully that its value now dramatically outweighs consumers' market power.

On the other hand, although predictions in this area are necessarily speculative, it seems unlikely that helpful social norms will easily emerge. Use and understanding of technology are diverse and highly fragmented across demographic groups. Furthermore, IoT technology is developing extremely quickly, so the process of social adjustment and understanding might not keep

which implies greater complexity in the devices or the architecture. Security imposes a cost, which might be a particular problem in an area where business models depend on keeping costs down.

It's a tough problem. It's tempting to understand privacy as a type of control – you prevent data or information about yourself from reaching other people. You set rules and then enforce them – and this looks difficult on the IoT. Yet this conception arguably misrepresents how we talk about our privacy, and the ways in which it concerns us.

I would contend that privacy is better understood as a constant

Technology isn't an exogenous force that disrupts or reinforces privacy. It's part of the changing context in which boundaries are negotiated.

pace. We should also bear in mind that the IoT could be largely invisible to most people, who might not feel much pressure to respond to its challenges.

This leaves PbD solutions to play a leading role. However, even this isn't a silver bullet, because they will add complexity and possibly undo the IoT's low-cost business model. For example, consider a smart meter. One of its functions is to convey billing information to the utility. As we've seen, the live datastream would be extremely disclosive. An obvious solution exists – the utility doesn't need the live stream for billing, so the meter could aggregate the output of several days or weeks and send it periodically.⁷ But aggregation implies storage, which implies the need for extra security measures,

effort to negotiate the boundaries of ourselves and our personal spaces (literally and metaphorically) with our peers. We perceive benefits from being visible to our networks, and to other entities such as our governments or our employers, and at the same time wish to restrict that visibility to preserve a private space for action, subversion, relaxation, contemplation, reflection, or intimacy. Similarly, our networks and governments wish us to be visible so that they might maximize benefits to themselves and their members, yet also have interests in limiting the amount conveyed, for reasons of propriety (too much information!), to avoid information overload, and also to protect citizens, preserve trust, and support the democratic process. Real and ideal boundaries change

with context, reflecting tensions within our divergent goal set (and between our goals and our networks' goals).

Hence we both push and pull at the boundaries around ourselves, while being similarly pushed and pulled by our networks. This is a constant process of negotiation and compromise. It won't reach equilibrium, and we can't describe or delimit it with simple sets of rules determining how data may or may not flow. Technology isn't an exogenous force that disrupts or reinforces privacy. It's part of the changing context in which boundaries are negotiated (for example, it affects what data can be gathered about an individual without permission, what benefits accrue to the individual, who can potentially get access to a disclosure, who can be effectively held accountable for data usage, and the relative value of a disclosure to an individual compared to his or her network). This picture of privacy as a dynamic, perpetual process is inspired by writers such as Irwin Altman^{13,14} and Helen Nissenbaum,¹⁵ and by the venerable but expressive common law concept of "reasonable expectations of privacy."

If we're lucky, preferences and interests converge to produce norms, or allow us to draft uncontroversial rules. As I say, I wouldn't be optimistic that they'll do this for the IoT.

The lesson, then, of this understanding of privacy is that data-protection authorities shouldn't try to micromanage dataflow to defuse privacy as an issue. Rather, we need room for our privacy negotiations to take place, and confidence in the process (that is, that negotiations will be in good faith). This should involve as much transparency as is feasible, PbD, and a sensitive set of safeguards drafted by government, civil society, and industry representatives who aren't bedazzled by the big numbers in the consultants' literature.¹¹ Lack

or loss of trust is a major cost of badly adapted systems, but one currently absorbed by society rather than the institutions that caused it. The IoT's size, comprehensiveness, and ubiquity threaten to make these costs very high indeed. □


Acknowledgments

This work is supported under SOCIAM: The Theory and Practice of Social Machines, funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/J017728/1.

References

1. C. MacGillivray, V. Turner, and D. Lund, *Worldwide Internet of Things 2013-2020 Forecast: Billions of Things, Trillions of Dollars*, IDC, Oct. 2013; www.idc.com/getdoc.jsp?containerId=243661.
2. J. Naughton, "The Internet of Things: It's a Really Big Deal," *The Observer*, 15 June 2014.
3. M. Hickey, "Smart Underpants Share How You're Feeling," *CNet*, 12 June 2010; www.cnet.com/news/smart-underpants-share-how-youre-feeling/.
4. M. Castillo, "Underwear Uses Electric Shock to Prevent Bed Sores," *CBS News*, 12 Oct. 2012; www.cbsnews.com/news/underwear-uses-electric-shock-to-prevent-bed-sores/.
5. J. Anderson and L. Rainie, *Digital Life in 2025: The Internet of Things Will Thrive By 2025*, Pew Research Center, 2014; www.pewinternet.org/2014/05/14/internet-of-things/.
6. J. Bacon, "All Brands Should Heed VW's 'Data Monster' Warning," *Marketing Week*, 11 Mar. 2014; www.marketingweek.co.uk/disciplines/data/-/crm/-/loyalty/all-brands-should-heed-vws-data-monster-warning/4009745. article.
7. S. Wicker and R. Thomas, "A Privacy-Aware Architecture for Demand Response Systems," *Proc. 44th Hawaii Int'l Conf. Systems Science* (HICSS-44 11), 2011, pp. 1-9.
8. M. Lisovich, D. Mulligan, and S.B. Wicker, "Inferring Personal Information from Demand-Response Systems," *IEEE Security & Privacy*, vol. 8, no. 1, 2010, pp. 11-20.
9. K. O'Hara and N. Shadbolt, *The Spy in the Coffee Machine: The End of Privacy As We Know It*, Oneworld, 2008.
10. "Proofpoint Uncovers Internet of Things (IoT) Cyberattack," press release, 16 Jan. 2014; www.proofpoint.com/uk/about-us/01162014.
11. J. Brill, "The Internet of Things: Building Trust and Maximizing Benefits through Consumer Control," *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*, K. O'Hara, C. Nguyen, and P. Hayes, eds., IOS Press, 2014.
12. E. Luger and Tom Rodden, "An Informed View on Consent for UbiComp," *Proc. 2013 ACM Int'l Joint Conf. Pervasive and Ubiquitous Computing*, 2013, pp. 529-538.
13. I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Brooks/Cole Publishing, 1975.
14. L. Palen and P. Dourish, "Unpacking 'Privacy' for a Networked World," *Proc. SIGCHI Conf. Human Factors in Computing Systems*, 2003, pp. 129-136.
15. H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Univ. Press, 2010.

Kieron O'Hara is a senior research fellow in the Web and Internet Science Group in the Electronics and Computer Science Department at the University of Southampton. His research interests include trust, privacy, open data, and Web science. O'Hara has a DPhil in philosophy from the University of Oxford. Contact him at kmo@ecs.soton.ac.uk.

 Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.