The Massive Internet of Things
Dr Victoria Baines, IT Livery Company Professor of IT
5 December 2023

In Walt Disney's *Fantasia*, inanimate objects come to life. The sorcerer's apprentice, Mickey Mouse, works out that if he puts on his master's hat, he can activate a broomstick to fill his master's cauldron with buckets of water. The plan is sound in theory. In the animation, sequenced to Paul Dukas' orchestral composition, Mickey's automation of his task is the ultimate labour-saving device and productivity measure. Until, that is, our hero falls asleep without having cast a spell to stop the broomstick filling the cauldron. When he awakes, he finds the room flooded. A desperate and – to modern audiences – rather disturbing attempt to extinguish the broomstick's life with an axe result in its multiplication. An army of anthropomorphic broomsticks fills the room with even more water. The animate(d) objects are out of control. Only the return of the sorcerer restores order.

Just eighty years later, we no longer need to rely on magic for objects to communicate with each other, nor is a world of functional automata something that we need to imagine. Some months ago, I found myself in a very similar situation to Mickey. One Saturday morning I was having a lie in, enjoying a cup of coffee in bed before fully facing the day. I heard a noise that I didn't immediately recognise, so I went into the living room to find out what it was. My 'robot' vacuum cleaner was busy cleaning the floor. That was all well and good, but I had no recollection of asking it to. It took a moment for me to realise that this was entirely my fault. The device's operations are controlled by an app on my phone, and when I took delivery, I had set some test tasks, about which I had evidently forgotten. Programmer error had disrupted my domestic bliss.

My vacuum cleaner is part of the Internet of Things (IoT), billions of connected 'smart' devices. In fact, an estimated 15.14 billion of them in 2023, expected to almost double to 29.42 billion by 2030, according to market insights company Statista;[1] That's an average right now of two connected things to every human on earth, and in seven years' time projected to be four for each of us. Another projection, in a 2019 report for *Business Insider*, estimates that there will be a whopping 64 billion connected things by 2025.[2] What kinds of things are we talking about? Let's consider this at the personal, domestic, urban, national, and planetary levels.

Networks of connected objects, from people to outer space

On and in our bodies, devices already use Bluetooth. Bluetooth is a short-range wireless technology in which devices pair with each other. In the previous lecture, 'Brain Computer Interfaces', we saw how neural implants use it to communicate brain signals. It's also how your fitness tracker and your headphones communicate with your smartphone, and it's the standard communication channel for remotely controlled sex tech, which we will explore in more detail in the next lecture, 'Sex and the Internet'.

Increasingly, our homes also contain devices that communicate with each other using Wi-Fi. In a 2020 survey of 20,784 people in the UK conducted by University College London and Neighbourhood Watch, the majority of respondents reported having a Smart TV. Half of 18- to 30-year-olds had a smart speaker. When we add

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[2] https://www.businessinsider.in/tech/news/iot-report-how-internet-of-things-technology-growth-is-reaching-mainstream-companies-and-consumers/articleshow/73133090.cms

thermostats, doorbells, security systems, games consoles, and baby monitors to the mix, it's clear that many of us already have domestic Internets of Things.

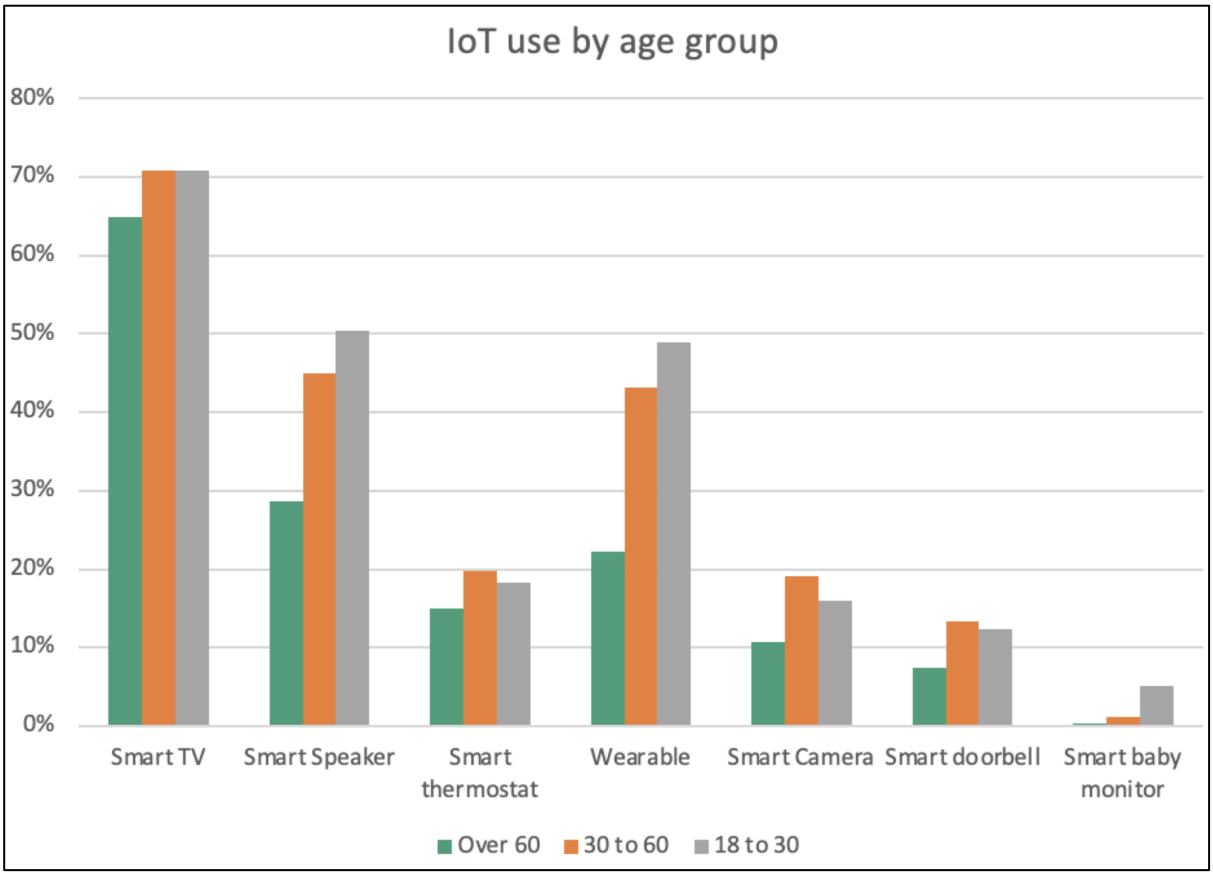

Figure 1. Use of IoT by age group in the U.K, from Nikolovska & Johnson. (2021). COVID-19 and Crime Survey Part I: Survey Overview and Online Security Behaviour [see further reading].

Mention of baby monitors brings to mind smart toys, which use Bluetooth to connect to another device or Wi-Fi to connect to a home network. In recent years, security experts and consumer organisations expressed concern over the ease with which strangers could communicate with and listen to children simply by downloading the relevant apps and pairing with toys such as My Friend Cayla, Furby Connect, and the I-Que Intelligent Robot.[3] In 2017, the telecoms watchdog in Germany banned My Friend Cayla for failing to protect children's data.[4]

Apps on our mobile devices now enable us to control lighting, sound, heating, security, and other domestic operations. The vision of some developers is that our phones and tablets can be processing hubs for our home networks, enabling Machine to Machine (M2M) communication between our connected appliances.

An example of this is the Wi-Fi embedded refrigerator, which allows you to see what's inside from your phone wherever you may be, tags food expiration dates to reduce waste, learns from your tastes and preferences to provide a weekly meal planner of suggested recipes, and sends cooking instructions to your smart oven. A screen on the door means you can watch TV while you cook, answer the front door if the smart doorbell rings, check what is going on in other rooms using smart cameras and motion detection, all while standing by the fridge.[5] For people who benefit from using assistive technology, one can see how these features could be helpful. For others, the labour-saving gains may be less obvious. It's perhaps for this reason that fewer than half of smart home appliances remain connected to the Internet.[6]

[3] https://www.which.co.uk/news/article/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys-a5BL72j4HeAS

[4] https://www.bbc.co.uk/news/world-europe-39002142

[5] See, for example, https://www.samsung.com/uk/refrigerators/all-refrigerators/smart/.

[6] https://arstechnica.com/gadgets/2023/01/half-of-smart-appliances-remain-disconnected-from-internet-makers-lament/

Smart(er) cities

Outside our homes, there are even more ways for things to communicate. If you make contactless payments with Apple Pay, Google Pay, or another mobile wallet, you're using Near Field Communication (NFC). We also have RFID – Radio-frequency identification – which uses radio waves to read chips over longer distances. Debit and credit cards use EMV, named after Europay, Mastercard, and Visa. Circuits are integrated into objects – they're the chips of chip and PIN. If you use a plastic travelcard for public transport, you're using RFID. And if your pet is microchipped, they are, too. You may also have seen RFID tags on trackable packages and deliveries. Smart tags like Apple AirTag and Samsung Galaxy SmartTag+ use Ultra-wideband (UWB) radio technology.

A plethora of devices contain SIM cards or software-based eSIMs – not just phones and tablets. Increasingly, cars contain SIMs for live traffic updates and directions, entertainment streaming, provision of Wi-Fi hotspots, and connected control over smart home systems. But what about streetlights and traffic lights? Lighting units that transmit signals and respond to stimuli are key components of emerging smart cities.

Traffic lights containing SIM cards have been around for a while. As far back as 2011, authorities found that this had unintended consequences. Criminals in Johannesburg, South Africa found that these SIMs could be used to make phone calls, so they stole 400 of them.[7] One of the things I love about my job is the reminders I receive from time to time that people's mischief can be ingenious.

Now, 15 billion things engaged in Machine to Machine (M2M) communication puts considerable pressure on our current Internet infrastructure. Faced with the prospect in the coming years of even more billions of connected things, it's entirely unsustainable. So, telecoms companies have been developing new ways of supporting a massive number of devices. Fifth generation cellular technology (5G) offers lower latency and capacity to connect many more devices than 4G – 10 times more by some estimates.[8] Sixth generation cellular (6G) is projected to be able to support ten times that – 10 million devices per square kilometre – with 'one microsecond latency', data transfer at one millionth of a second. 6G will also be able to send data at ultra-high frequencies, in the hundreds of gigahertz (GHz), or terahertz (THz), as opposed to 5G's frequencies of up to 100 gigahertz (GHz). The International Telecommunications Union (ITU) expects to have the initial standardisation of 6G complete by 2030 at the latest, with some countries such as South Korea planning to deploy it before then.[9]

Smart = connected + intelligent

Integrating data from different sources can improve outcomes. In a transport network, being able to identify how many people have checked in with their RFID cards to a particular metro station, or where there has been a road traffic accident, can tell public transport operators whether additional capacity is required. In smart transport networks, it's envisaged that AI could take the place of human operators in making routine decisions and alterations, such as re-routing driverless cars.

So, too, in farming and food production, where drones, tags, and sensors are already used to monitor crops and livestock. 'Precision farming' is a vision of agriculture that can identify exactly what is needed to improve yield and quality, and also potentially reduce environmental impacts. It combines expanded deployment of IoT components with data analytics, Machine Learning, and robotics. In logistics and manufacturing, a similar combination of technologies is currently referred to as 'Industry 4.0.' It's envisaged that continuous tracking and monitoring will enable predictive maintenance and increase productivity.

Power consumption by an ever-growing Internet of Things is an inevitable concern. Low-power Wide Area Network (LPWAN) is a networking protocol designed to allow communication between connected things at a much lower bit rate – between 0.3 and 50 Kilobits per second, compared to 5G's peak data rate of 20 Gigabits per second. But even at lower rates, a power source is required for communication and processing. Until now, many IoT devices have relied on lithium batteries, which need to be changed or recharged. While it is possible to recycle these, the prospect of many more connected things inevitably threatens further depletion of the world's minerals. So, several manufacturers are working on battery-free processors, such as Wiliot's

[7] https://www.bbc.co.uk/news/world-africa-12135841
[8] https://www.statista.com/statistics/1183690/mobile-broadband-connection-density/
[9] https://www.6gworld.com/exclusives/itu-6g-standardisation-ready-no-later-than-2030/

postage stamp-sized Pixel2, which harvests energy from radio waves;[10] and Atmosic Technologies' and Matrix Industries' collaborative development of devices that harvest thermoelectrical energy from their environments.[11]

Sensing things, from the Cloud to the Edge

What might the sensors in connected things sense? Types of sensors already in use include those that can variously detect proximity, noise, motion, pressure, moisture, temperature, gases, pH, and water levels. Objects can also be fitted with gyroscopes, accelerometers, and optical sensors. An electric vehicle prototype announced by Sony and Honda earlier this year and set to go on sale in North America in 2026 boasts over 40 sensors embedded in its exterior.[12]

[10] https://www.forbes.com/sites/johnkoetsier/2022/04/12/this-cheap-stamp-sized-3-core-no-battery-computer-could-drive-iot-to-trillions-of-smart-devices/

[11] https://www.electronicproducts.com/partnership-promises-battery-free-iot-devices/

[12] https://www.theverge.com/2023/1/4/23539863/sony-honda-electric-vehicle-afeela-ces-reveal-photos

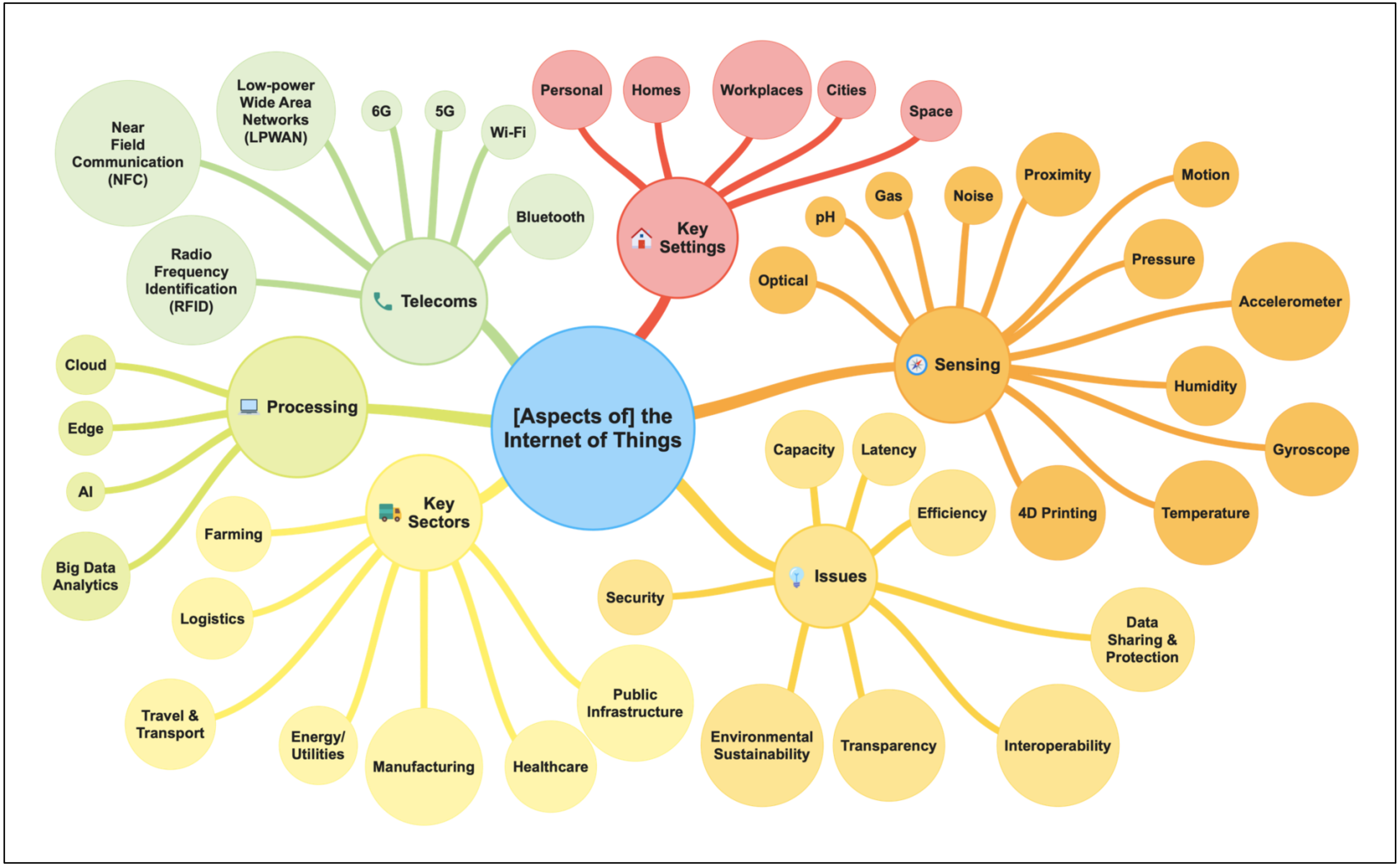

Figure 2. Aspects of the Internet of Things (selection)

Sensors might also cause objects to respond to external stimuli, as in the case of 4D printing, otherwise known as additive manufacturing. What distinguishes 4D objects from 3D objects is their ability to change their geometric properties, transforming over time. By printing objects with programmable materials such as hydrogels or Shape Memory Polymers (SMPs), they can be transported in one state or shape and transformed into another when stimulated – for example, by moisture, light, time, heat, or pH. At the micro level, stents could be inserted into human bodies that adjust their shape when required. There's also a good deal of interest in 4D printing for space missions, where remote activation of objects could dispense with the need for deployment machinery such as booms and antennae to be transported, thereby reducing the overall weight of materials. Weight is an important consideration for space tech leaders like Elon Musk, who earlier this year announced his ambition to get a million people to Mars by 2050.[13] Regardless of whether you think that is likely, it's certainly the case that Low Earth Orbit (LEO) satellites, of which Musk's Space X has the largest single market share, and constellations of tiny picosatellites are expected to provide critical infrastructure for the Massive Internet of Things.

IoT devices, contacts, and communication generate data, which needs to be processed. Rather than sending massive and ever-increasing amounts of data back to proprietary company or government servers, the Internet of Things already makes extensive use of cloud computing. Practically speaking, this means that much of the world's IoT processing depends on the largest cloud providers, based in the US and (to a much lesser extent) China. According to Statista, Amazon, Microsoft, and Google currently dominate the cloud computing market, with 32%, 22%, and 11% market share respectively. That doesn't mean that the data physically resides in the US. But it does mean that two thirds of the cloud processing infrastructure for the Internet of Things will likely rely on the operations of just three US companies.

Whereas cloud computing hosts applications in data centres, edge computing hosts applications closer to end users. So, current iterations of fitness trackers and smart home technology use smartphones as processing hubs. In industrial edge computing, Raspberry Pi single-board computers are widely used. In 2020, the Raspberry Pi Foundation announced that the industrial market accounted for 44% of its total annual sales.[14]

Can we have interoperability *and* privacy/safety/security?

The sheer number of connected objects is already massive by anyone's standards. In that respect, what we have been exploring until now is just the Internet of Things in general. Information technologists tend to distinguish the Massive Internet of Things (MIoT) described above from Critical IoT applications in which security, timely responses, and reliability are paramount. These would include anything related to public infrastructure, such as power and water supply, traffic safety, emergency response, and medical procedures.

The distinction is not always so clear-cut when we start to look at practical use cases. Smart electricity supply certainly concerns critical infrastructure and makes use of dedicated communications networks. But to be effective it relies on smart meters installed in our homes reporting usage and demand. That domestic electricity supply may power a car that will make its way through a smart urban traffic system. That car will interact with and respond to personal, local, municipal, and critical networks and stimuli. At the same time, the biggest perceived gains in some current smart city case studies come from integrating – or at least triangulating – personal, public, and private sector datasets, bridging traditional divides between private and public life.

[13] https://www.scientificamerican.com/article/musk-and-bezos-offer-humanity-a-grim-future-in-space-colonies/

[14] https://www.theregister.com/2020/12/17/raspberry_pi_to_anoint_design/

A truly 'smart' city is envisaged as one in which data is gathered from a wide range of sensors and connected objects and monitored and managed in real time. It requires a 'platform of platforms' to make sense of data collected from different sources, like the CityVerve smart city demonstrator trialled in Manchester, UK.[15] The project grouped data analytics around four themes: culture and public realm; health and social care; energy and the environment; and travel and transport.

In Singapore, where the world's first self-driving taxis launched in 2016 and robot police officers have been interacting with members of the public since 2021, the 'ConnectedLife' home monitoring solution uses a city-wide, decentralised data exchange to share information on elderly citizens' health and wellbeing with family members, healthcare providers, insurance providers and the government. In Fukuoka, Japan, a systematic care model for elderly people with dementia combines data from door-to-door visits by public workers and service providers with 'care-tech' apps and IoT-based monitoring using personal tracking devices.[16]

The Manchester CityVerve trial quite rightly placed controls on how data was accessed and used. Whenever there is potential for aggregation of large sets of data on individual citizens' movements and behaviour, it's important that the right to a private life is not unduly compromised in the name of efficiency. In 2021, the UK government conducted a five-month 'proof of concept' trial on a motorway junction near Birmingham, in which CCTV and wireless technology were embedded in streetlights. The proposal is that processors in streetlights could be used to communicate with autonomous vehicles, pushing out traffic updates and information on speed limits along the National Highways network. The government press release on the trial noted that "Drivers would have been oblivious to the CCTV and communications technology hidden away in the streetlamp as it was installed when the lights were switched to the improved, greener LED lighting."[17]

This raises some important considerations. Data protection legislation, of which the EU's General Data Protection Regulation (GDPR) is perhaps the best-known example, promotes the principle that data processing should be transparent. While the use of CCTV in streetlights described above may be for the purpose merely of identifying that a vehicle – any vehicle – is approaching, the stress on drivers' lack of awareness is something of a misstep. Ensuring that people in smart cities are aware of when they are being tracked will be crucial to fostering and maintaining public trust in the overall effectiveness of data gathering and management initiatives. GDPR also states that data should only be processed for the purposes intended. It should not be repurposed without the consent of the data subject.

In a fully integrated and interoperable smart city, it would, for example, be technically possible to penalise someone who refuses to recycle their domestic rubbish by charging them higher fares on public transport. This could, of course, be sold differently, as giving discounted fares to those who do recycle. Current signals of this kind of data aggregation can be found in China, where a Social Credit System has been spearheaded by local governments.[18] In the City of Rongcheng, each adult resident is given a score of 1,000 points. Credit may be lost for traffic violations, earned for voluntary service. High scorers are rewarded with perks such as free bicycle rental and heating discounts.[19] Citizen conduct has been gamified through data and digital technology.

It has become fashionable to refer to the Internet of Things as the world's 'digital nervous system." Capturing and analysing data from billions of physical objects in real time highlights

[15] https://reports.raeng.org.uk/datasharing/case-study-2-cityverve-manchester

[16] https://www3.weforum.org/docs/WEF_Smart_at_Scale_Cities_to_Watch_25_Case_Studies_2020.pdf

[17] https://www.gov.uk/government/news/intelligent-street-lighting-illuminates-the-way-to-digital-roads-for-national-highways

[18] https://www.wired.co.uk/article/china-social-credit-system-explained

[19] https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/

yet another respect in which digital and physical realms are converging. The prospect of large numbers of things with the capacity to respond to stimuli, without direct human intervention, raises key questions that are currently being asked of Artificial Intelligence. How will we ensure that the future Internet of Things operates safely, securely, and transparently? Who will be responsible for that, and who will have oversight? How can we ensure that the benefits outweigh the risks? Lastly, who benefits? In a vision for the future in which efficiency and productivity equate with a reduction in human labour, expansion of a truly Massive Internet of Things may serve some members of society at the expense of others. In a society that prioritises data analytics above all else, in which humans are just a fraction of many billions of data generators, we may need to work extra hard to assert ourselves as individuals, to distinguish ourselves from other data assets. To return to our Disney analogy, the risk is not so much that the broomsticks will take over. It's that we will neglect to ensure that the broomsticks serve *all* of us.

Epilogue – going back to the future

In early 2012 I found myself standing in my father's kitchen on the South Coast of England. I was living in The Netherlands at the time, working for EUROPOL, the European police agency. The all too rare occasions when I returned to the UK gave me an opportunity to check on my dad's health. At the age of just 35, he had suffered a massive heart attack and had received one of the world's first triple heart bypass operations. Thanks to this procedure and superb follow-up care, his life was prolonged by an incredible 28 years, during which he benefitted from further medical advances.

On the occasion of my visit, he proudly showed off a pacemaker-defibrillator that had recently been implanted under his skin, near his collar bone. He explained that the device communicated wirelessly with a base station on his bedside table, which then used his home Internet connection to report his heart function to the local hospital. This allowed my dad's cardiologist to monitor him continuously and remotely. The defibrillator component was designed to deliver a shock to 're-boot' his heart if it began to struggle. Once I had duly marvelled at the wonders of modern medicine, we went to sit down in the living room, from where we could see his rather old, rather clunky desktop computer. This reminded him to ask me for help with something that had been irritating him.

"You're good with computers, aren't you?" is a phrase that fills anyone who has ever worked in IT with dread. My dad said that his computer had been running really slowly, ever since one of his step-grandchildren had downloaded some games from the internet. As a cybercrime analyst, I knew that downloading games from dodgy websites was one-way computers could be infected with malicious software. When I asked my dad whether the computer's antivirus software was up to date, he confessed that he hadn't bothered to renew the subscription. Because he didn't really understand what it did, he had decided it was probably a waste of money.

An intelligent, capable man who ran his own business in the motor trade somehow didn't understand the implications of his home computer and a device that was monitoring his vital signs sharing an Internet connection, and that keeping that connection clean and secure would prevent criminals interrupting his healthcare. During the same cup of tea, which – as we all know – is a recognised measurement of time in the UK, I proceeded to explain this, to update the software on my dad's computer, and to impress on him the importance of keeping it updated. But it occurred to me that there were likely to be many others for whom the implications of being part of the Internet of Things were far from clear. In fact, already by the time of this conversation, there were millions of people walking around with connected pacemakers and defibrillators inside them, and millions more diabetics with connected continuous glucose monitors and insulin pumps, all of whom depended on their correct functioning.

My dad passed away a few months later. You'll be relieved to hear that he was not assassinated through his pacemaker. As far as we know, this is still the stuff of fiction, as in the TV series *Homeland*, reportedly based on former US Vice President Dick Cheney's concerns about the connectivity of his own pacemaker. But even after his passing, the bionic part of my dad was still a subject of confusion and debate. One family member couldn't understand why the pacemaker had not called an ambulance when my dad's heart finally failed, something that was never part of its design. As is often the case with Information Technology, we can find ourselves caught between a lack of awareness about what it does and hype-influenced expectations of what it ought to do. Those of us who grew up in the latter half of the twentieth century may feel legitimately aggrieved that we don't yet own a flying car. That doesn't mean it will never happen, just as the pacemaker of the future may well have the capability to dispatch and ambulance (or drone, or first responder robot). But it *is* incumbent on developers and distributors of IoT devices to explain clearly to us what they can do, what they can't, and what we need to do to keep them and us safe.

Resources

Several governments have published their smart city strategies. Singapore's 'Smart Nation' resource is perhaps the most accessible and consistent of these - https://www.smartnation.gov.sg/

The European Union's vison for the Internet of Things can be found here - https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-things

Several national and regional cybersecurity agencies have published policies and guidance concerning IoT and smart objects. Below is a selection.

- US Cybersecurity & Infrastructure Security Agency (CISA): "Securing the Internet of Things (IoT)" - https://www.cisa.gov/news-events/news/securing-internet-things-iot

UK National Cyber Security Centre (NCSC) guides:

- "Smart devices: using them safely in your home" - https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home
- "'Smart' security cameras: Using them safely in your home" - https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home
- For local authorities: "Connected Places: Cyber Security Principles" - https://www.ncsc.gov.uk/files/NCSC-Connected-Places-security-principles-May-2021.pdf
- "Organisational use of Enterprise Connected Devices" - https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices
- The European Network and Information Security Agency (ENISA) has created an interactive tool showing good practices for IoT and Smart Infrastructures - https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool
- The Norwegian Consumer Council produces informative guides in English on the safety of connected toys. Their 2016 video on My Friend Cayla and the i-Que robot can be found here - https://www.youtube.com/watch?v=IAOj0H5c6Yc

Further Reading

The Global System for Mobile Communications Association (GSMA) is a membership organisation of the world's leading telecommunications companies. You can read more about their collaborative development of Low Power Wide Area Networks (LPWAN) here - https://www.gsma.com/iot/massive-iot/

Greengard, S. (2021). *The Internet of Things*. MIT Press Essential Knowledge Series.

Nikolovska, M., & Johnson, S.D. (2021). *COVID-19 and Crime Survey Part I: Survey Overview and Online Security Behaviour.* Available at: https://covid19-crime.com/wp-content/uploads/sites/92/2022/03/Nikolovska-and-Johnson-2021-COVID-19-and-Crime-Survey-Part-I-FINAL.pdf

Nash, V., Davies, H. C., & Mishkin, A. (2019). *Digital Safety in the Era of Connected Cots and Talking Teddies*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407264

Schwab, K. (2017). *The Fourth Industrial Revolution*. Penguin: Random House.

World Economic Forum (2020). *Smart at Scale: Cities to Watch. 25 Case Studies*. https://www3.weforum.org/docs/WEF_Smart_at_Scale_Cities_to_Watch_25_Case_Studies_2020.pdf