"*Home, Tweet Home*": Implications of the Connected Home, Human and Habitat on Australian Consumers

by
Alexander Vulkanovski
ACCAN Intern (of Things)
February 2016

“Home, Tweet Home”: Implications of the Connected Home, Human and Habitat on Australian Consumers

Authored by: Alexander Vulkanovski
Edited by: Narelle Clark

Published in 2016

Supported by the Australian Communications Consumer Action Network (ACCAN).
The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

The internship was sponsored by Google Australia Pty Ltd.

Australian Communications Consumer Action Network
Website: www.accan.org.au
E-mail: research@accan.org.au
Telephone: +61 2 9288 4000
TTY: +61 2 9281 5322

ISBN: 978-1-921974-37-3

This work is copyright, licensed under the Creative Commons Attribution 3.0 Australia Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the author(s). To view a copy of this licence, visit http://creativecommons.org/licenses/by/3.0/au/

This work can be cited as: Vulkanovski, A.,2016, *“Home, Tweet Home”: Implications of the Connected Home, Human and Habitat on Australian Consumers*, Australian Communications Consumer Action Network, Sydney.

DISCLAIMER: The views and opinions expressed in this report are the author’s own.

Table of Contents

Executive Summary

The 'Internet of Things' ("IoT") has no 'official' definition. On face value, it is a buzz phrase coined by Kevin Ashton in 1999 to describe connecting everyday objects to the Internet. Since IoT is not an 'official' term, many definitions exist. This report favours the following definition by the EU Research Cluster on the Internet of Things:

> *"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."*

Forecasts of 'size' and 'value' of IoT vary greatly, change frequently and the measurements used are inconsistent amongst different entities. For instance, some entities interpret 'value' as economic output, while others also consider cost savings. Based on the research conducted, this report concludes that no one entity can predict, with any reasonable accuracy, how big or valuable IoT will be. The IoT 'value' forecasts for 2020-25 are in the tens of trillions of dollars, and the 'size' forecasts are in the hundreds of billions of connected devices. Analysis on the Australian market is very limited – there are no major analytics reports that focus on Australia exclusively, and of the few Australian IoT studies available, global estimates are used to calculate the value of IoT in Australia. For this reason, this report warns against relying on any existing IoT forecasts to foresee the future of IoT in Australia, and recommends the establishment of a public IoT body to conduct research on IoT in the Australian market, for the benefit of the public and policymakers.

The consumer IoT issues identified in this report are derived from three broad consumer-focused use-cases. These use-cases are 'smart' homes and appliances (Connected Homes), wearables (activity trackers, smartwatches, implantable devices etc.) and health care (Connected Humans), and smart cities and smart cars (Connected Habitats). From these three IoT use-cases, this report identifies the following broad IoT consumer issues: privacy, security, interoperability, serviceability, consumer protection, wearables and healthcare, affordability, changing consumerism, issues of choice and control, environmental implications, and the implications of IoT on specific consumer groups like children, the elderly and persons with disabilities.

The two biggest *conceptual* consumer issues are privacy and security. This report concludes that IoT does not bring anything entirely new to existing digital privacy and security concerns. However, it does *add* the following:

1. *Scale* – It creates more data collection points, since more 'things' collect data;
2. *Method* – It creates novel ways of collecting data, such as via sensors and smart things;
3. *Reach* – It penetrates more intimate areas of our lives, such as data on our bodies and inside our homes;
4. *Nature* – An advanced IoT ecosystem is designed to collect data covertly and 'in the background' via sensors and other digital tools, meaning that consumers may not be *aware* of the collection of personal information; and

5. *Depth* – The collective result of the above four concepts will be greater than the sum of the parts. As a result of greater scale, new methods, reach and nature of data collection and processing, IoT will have a 'synergetic' effect on existing privacy and security concerns.

This report, via several consumer surveys and academia, draws a direct link between privacy and security, and consumer confidence. Consumer confidence is essential for a healthy uptake of IoT products and services, especially in these relatively early days. This report also predicts a growing consumer demand for private and secure digital services, and in turn, a market opportunity for businesses that empower consumers in respect of their own personal data. Recommendations for IoT product and service providers include adopting privacy and security 'by design', giving consumers the tools to control their personal information, adopting data minimisation policies and considering the recommendations of the Office of the Australian Information Commissioner (OAIC).

Supplementary to consumer privacy and security recommendations, this report recommends that IoT developers and service-providers give consumers the choice to 'opt out' of certain features or services. This may mean activating desired features and disabling unwanted features, simplifying the process of unsubscribing from a service, or using a system of 'incremental consent' for IoT services. For example, if a consumer purchases a 'smart' fridge, they ought to be able to disable unwanted features (such as barcode scanners) and enable wanted features. In addition, consumers ought to be given the option to make a 'smart' thing 'dumb' again, essentially 'opting out' of connectedness. For example, future consumers may no longer be able to purchase a 'dumb' fridge, so should be given the option of limiting the features of their connected fridge to just refrigeration of food.

Privacy, security, 'opt out' and also accessibility are best implemented 'by design'. This report strongly recommends that IoT designers and developers adopt a policy of privacy, security, opt-out and accessibility *by design*, ensuring that products are built for these purposes. This recommendation echoes that of many sources included in this report.

The most significant *practical* consumer IoT issue is interoperability. The IoT industry does not have any official, widely accepted or universally applied communication or network standards that are fit for the requirements of most IoT devices (constant connectivity, low power usage, and in most cases, short-distance communication). This report recommends that consumers take up IoT products and services with a caveat – 'make sure that each new IoT product or service will 'talk' to existing devices, and operate harmoniously with any existing IoT ecosystem'.

The most important recommendation for consumers is to develop a base-level understanding of IoT. This includes how IoT devices and services operate, what data is collected, the inferences that can be drawn from that data, and the tools at their disposal to minimise the risk of privacy or security intrusion. By staying informed and choosing their IoT products and services wisely, consumers can avoid communication breakdown (from conflicting standards), pick a durable and trusted product, maximise their privacy and security, and build a safe, user-friendly Connected Home. An informed consumer is an empowered consumer, and an informed and empowered consumer base can shape an ideal IoT consumer market.

On the topic of policy and regulation of IoT, this report concludes that any attempts to regulate IoT at this relatively early stage may become a hunt for a 'solution without a problem'. Regulators, policymakers and government are advised to *'innovate, wait, then regulate'.* The IoT market is still in early days and any attempts to regulate its growth at this crucial stage may be inhibitory. This report recommends that regulators and legislators remain constantly informed, but refrain from any regulatory action unless a major market failure is identified.

One opportunity for the public sector is to become an early adopter and market leader of IoT. This ensures early experience and exposure to IoT, an IoT-trained labour force, economic benefits, a better delivery of public sector services, and the opportunity to *create* an ideal domestic IoT market by investing in secure, trustworthy and innovative IoT providers.

The 'Connected Human' areas of IoT carry the biggest opportunities for public healthcare, but also the biggest challenges for privacy and security. Wearables, activity trackers, smart watches, implantable, and digestible connected 'things' all collect an unprecedented amount of intimate data about our bodies, our physical activities and our whereabouts. This report identified some of the data collected by these devices, how it is handled and inferences that can be drawn from this data (APPENDIX 2). Also identified is a gap in privacy law regarding the identification and categorisation of Connected Human data (like heart rate data, collected by many activity trackers and smartwatches). This report recommends that policymakers address this gap and regulate the handling of this potentially sensitive data.

IoT has a number of financial implications for consumers. The greatest financial impact is the sharing of IoT-collected data with insurance companies. The conclusion was unsurprising – good behaviour (eating well, exercising) may be rewarded with discounts, while risky behaviour (driving recklessly) may be 'punished' with price premiums. The other financial implications of IoT include personalised price discrimination, personalised real-time marketing, and the costs associated with maintaining, powering and connecting IoT ecosystems. Fortunately, these costs are minimal and unlikely to affect consumer attitudes or IoT take-up.

This report concludes that IoT does not raise any novel concerns for Australian privacy or consumer protection law. However, IoT will likely complicate *existing* technology-related legal issues. One particular area of concern is the relationship between faulty software and consumer guarantees in Australian Consumer Law. Notwithstanding, existing consumer laws are likely to be flexible enough to address emerging IoT issues as they arise.

In summary, IoT *can* be 'utopian' or 'dystopian', but in reality, it will fall somewhere in between. The market will likely dictate the direction of IoT's future, and the government should only intervene as an 'early adopter' or to address any market failures and inhibitors. IoT is unlikely to create *new* consumer issues – but it may complicate and supplement existing ones. New technology brings uncertainty and distrust, but these should be seen as opportunities to innovate and develop new standards of consumer empowerment and protection. The good news is that IoT is relatively new and still forming. This means that Australian consumers, businesses and government are in an excellent position to determine what IoT in Australia ends up looking like.

"I like to think (it has to be!)
of a cybernetic ecology
where we are free of our labors
and joined back to nature,
returned to our mammal
brothers and sisters,
and all watched over
by machines of loving grace"

- All Watched Over By Machines Of Loving Grace
by **Richard Brautigan** (1967)

Introduction

In 1950, **Ray Bradbury** wrote a sci-fi short story titled *The Veldt* (originally *"The World the Children Made"*) about the fictional Hadley family, who lived in "The HappyLife Home". It was a connected, autonomous home that had relieved them of their domestic burdens. The HappyLife Home did everything for them without them even needing to ask, it *"clothed and fed and rocked them to sleep and played and sang and was good to them".*

The concept of an immersive, machine-assisted world is even older than the Hadley family. In a 1930 essay titled *Economic Possibilities for our Grandchildren*[1], economist **John Maynard Keynes** envisioned a machine-assisted living bringing high standards of living and leisure. As a result, he predicted that by 2030 everyone would only need to work fifteen hours a week and could devote the rest of their time to arts, pleasure and leisurely pursuits. Keynes' reality may be upon us, although it may not seem apparent today.

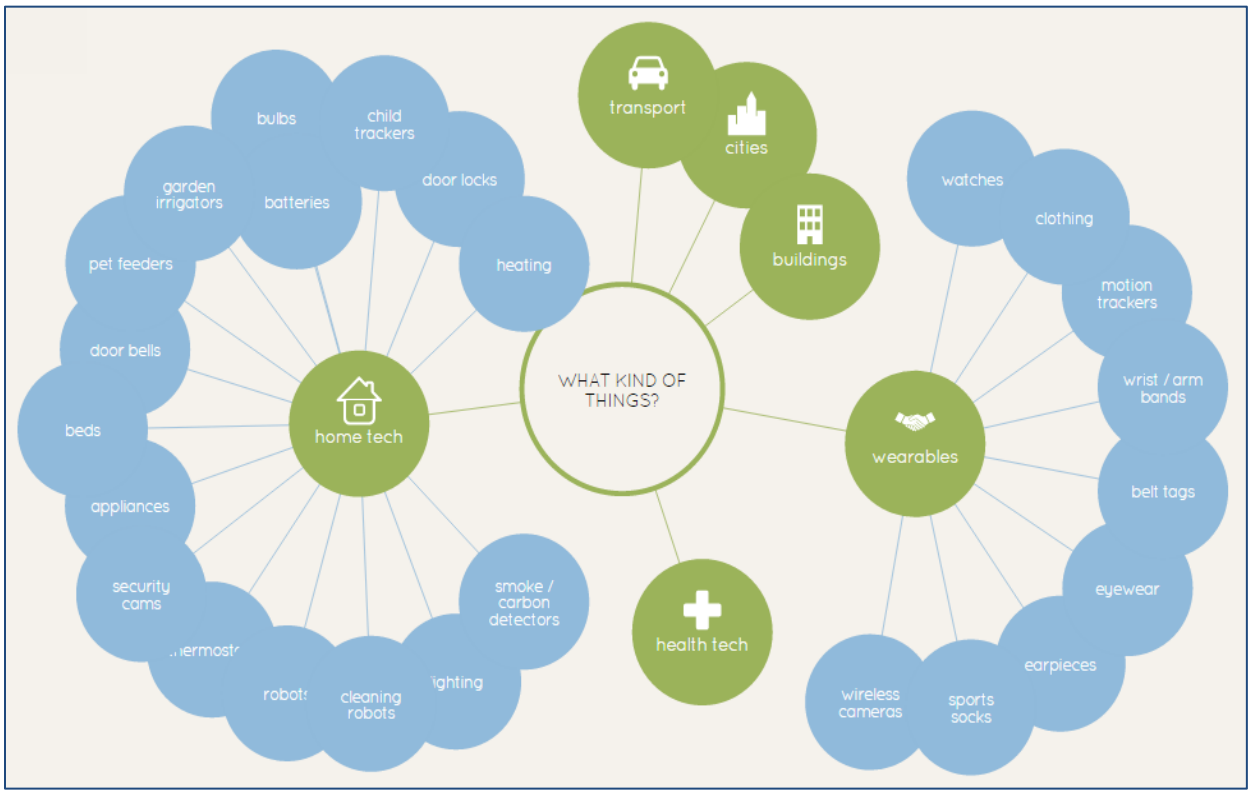


Figure 1 – 'IoT Ecosystem'. Source: Information is Beautiful

Existing kitchen and home appliances can compile shopping lists and provide real-time updates on milk supply using sensors and scales. Smart air-conditioning and heating can be controlled with a smartphone and turn on when the user is near. Connected security, fire detection and home monitoring systems mean home security and surveillance from anywhere, anytime. Smart watches

[1] John Maynard Keynes, 'Economic Possibilities for our Grandchildren' in John Maynard Keynes, *Essays in Persuasion* (Norten, 1963) pp 358-373.

and activity trackers now monitor fitness levels, blood pressure, caloric expenditure and sleep. Traffic sensors and real-time traffic analytics, smart parking space management and improved emergency response will streamline infrastructure services. Roadside sensors can communicate with connected and autonomous cars, exchanging data on speed, locality, accidents and breakdowns for everyone's benefit. **Figure 1** above breaks down some areas of consumer goods and services that will be revolutionised by the Internet of Things, including home technology and connected wearables.

The Internet of Things (hereafter **"IoT"**) has been described as a *"new age of embedded, intuitive computing in which our homes, cars, stores, farms, and factories have the ability to think, sense, understand, and respond to our needs"*[2]. Connecting our 'things' will give them senses, intuitive analytics and more data collection capability than ever. The future of our Connected Home, Humans and Habitat is not in its marvel, but in its familiarity – operating seamlessly in the background. IoT is here, and pretty soon, we won't even know so.

About this Report

This report is a research and literature review on Australian consumer issues in the context of IoT. The purpose of this research report is to identify IoT in its current and future state, and the implications of IoT for Australian consumers.

The report will begin by introducing readers to the Connected Home, Human and Habitat and IoT as a concept, including its past, present and future globally. It will then discuss IoT consumers - who are they? What do they expect? What is their perception of IoT?

The proceeding body of the report will follow the **Babel family** in the Sydney, Australia of 2020. Johannes, Olivia and their daughter Evey Babel live in an IoT world where the Connected Home, Human and Habitat are all part of their daily routine. The journey through their reality will be in **four scenes - each with fresh consumer IoT issues.** Finally, the report will make a number of recommendations for consumers, IoT business and the public sector.

Defining the 'Internet of Things'

IoT, as yet, has no 'official' definition. Individuals and organisations have formed their own definitions[3] with subtle differences. Corporate stakeholders have been quick to give IoT their own 'buzzword' branding. **IBM** has 'Smart Cities', **General Electric** has 'Industrial Internet', **Cisco** calls it the 'Internet of Everything' and **Microsoft** calls it 'The Internet of Your Things'.

On face value, it refers to an ecosystem of 'smart' and connected everyday objects communicating with each other. However, IoT goes much deeper. 'Internet of Things' was admitted into the Oxford

[2] Theodore Forbath, 'The third wave of computing' *Forbes* (online) 3 October 2013 <*http://fortune.com/2013/10/03/the-third-wave-of-computing/*>
[3] Postscapes Labs, *Internet of Things: Definitions* <*http://postscapes.com/internet-of-things-definition*>

English Dictionary in 2013 as *"the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data"*[4].

That too is an oversimplification. The best definitions are comprehensive and elemental. In 2013-14, the **International Organisation for Standardization / International Electrotechnical Commission Joint Working Group 1 ("ISO/IEC JTC 1")** reviewed over 30 definitions and consolidated them in their IoT Preliminary Report 2014:

> *"An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."*[5]

This report prefers the following definition by the **IoT European Research Cluster**[6] for its elemental nature, broad wording and technological focus (**Figure 2**):

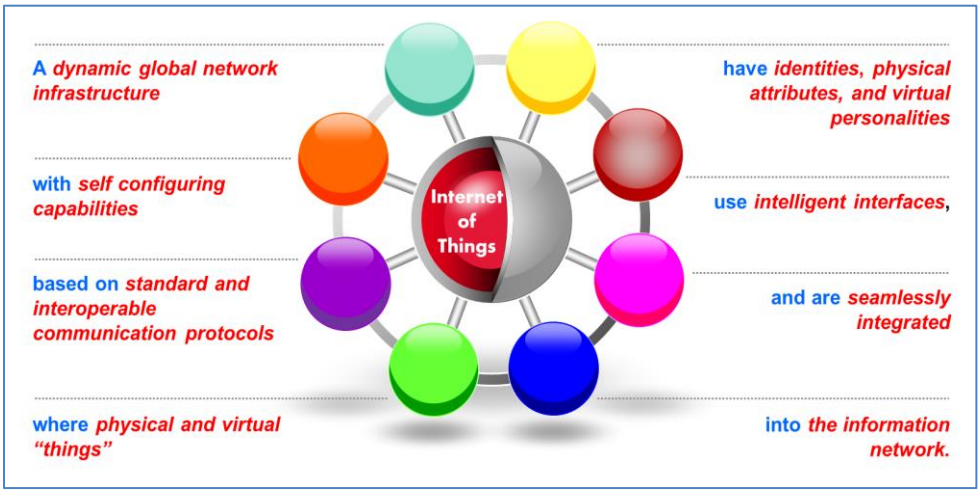


Figure 2 - EU IoT Cluster definition of 'Internet of Things'. Source: IERC

Internet of Things in the Digital Menagerie

IoT overlaps with a number of peripheral concepts. **Machine-to-Machine ("M2M")** communication, simply, refers to communication between *devices*. M2M is an enabler of IoT, because it allows 'things' to interconnect and communicate. **Cloud computing** refers to a system of *online storage* in other locations but connected across the Internet, where data can be uploaded and stored online, and then accessed from other devices. Some common products include Dropbox, iCloud and Google Drive.

'Big Data' refers generally to the concept of enormous datasets that are used to analyse trends, patterns and human behaviour. 'Big Data' is also interpreted by the *inability* to sufficiently process

[4] Definition of 'Internet of Things', *Oxford English Dictionary (UK)* <https://www.oxforddictionaries.com/definition/english/Internet-of-things>
[5] International Organisation for Standardization/International Electrotechnical Commission Joint Technical Committee 1 ("**ISO/IEC JTC 1**"), *Internet of Things (IoT) Preliminary Report 2014*, 2015 <http://www.iso.org/iso/internet_of_things_report-jtc1.pdf> p.4
[6] European Research Cluster on the Internet of Things, *Internet of Things* <http://www.internet-of-things-research.eu/about_iot.htm>

these enormous datasets, often defined by using the 5 'Vs' – a set of data that is *"too big (volume), arrives too fast (velocity), changes too fast (variability), contains too much noise (veracity) or is too diverse (variety) to be processed...using traditional approaches and techniques"*[7]. IoT is an *enabler* of Big Data – more 'things' collecting data means Big Data gets 'bigger'.

In order for connected 'things' to become intuitive and autonomous, the data from IoT would require **Ubiquitous Computing** (also known as 'pervasive computing' or 'everyware'). This is where computing can be anywhere and everywhere, and machines perform actions cognitively[8] and without human intervention. **Stefan Poslad** in 2009 identified the characteristics of an ideal ubiquitous (and thus ideal IoT) network:

1. A networked, transparent physically distributed system;
2. Implicit interaction between humans and computing devices/systems;
3. Context-aware;
4. Autonomous operation; and
5. 'Intelligent' decision-making and interaction[9].

The Connected Home, Human and Habitat

This report invites the reader to examine the environment that they are sitting in. This may be in public, sitting at a desk, or reading this on a smartphone or tablet. In the near future, IoT will transform all of these surroundings. Many 'things' are already 'connected', and chances are that someone, somewhere, is developing ways of connecting the 'things' that aren't.

Earlier in 2015, **Fjord and Accenture Digital** released a 103-page report entitled *The Era of Living Services*[10]. They envisioned a utopian Connected Home, Human and Habitat:

> *"At home, personalized Living Services could adjust the heating, lighting or music volume to fit with the preferences of the person walking into the room, and take into consideration the time, temperature and daily behavioural pattern of that individual or family group... Living Services have the capability to help us get the most out of our leisure and downtime... Living Services will come to know what we enjoy doing, and will understand the context of our lives including our time and financial restrictions, how happy, healthy and fit we are, and with whom we are spending our leisure time. Designed to learn through real time analytics, they will be able to curate choices and deliver personalized recommendations tailored to the weather, our location, mood, health and even our bank balance*[11]".

[7] ISO/IEC JTC 1, *Big Data Preliminary Report 2014* (2015) <http://www.iso.org/iso/big_data_report-jtc1.pdf> p.5
[8] Mark Weiser, 'The Computer for the 21st Century' (1991) 265(3) *Scientific American* 78.
[9] Stefan Poslad, *Ubiquitous computing: smart devices, environment and interaction* (John Wiley & Sons Ltd 2009).
[10] Fjord and Accenture Digital, *The Era of Living Services* (2015) <https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Digital_1/Accenture-Living-Services.pdf>
[11] Ibid p.10

IoT can be split into eight areas: homes, health care, cities, vehicles, manufacturing, transportation, energy and agriculture[12]. This report will focus on the *consumer* areas – **homes** (Connected Home), **health care** and wearables (Connected Human), and **cities** and **cars** (Connected Habitat).

McKinsey & Company and **Global Semiconductor Alliance (GSA)** have compiled a table summarising some IoT applications consumers can expect to see in the near future **(Figure 3)**[13].

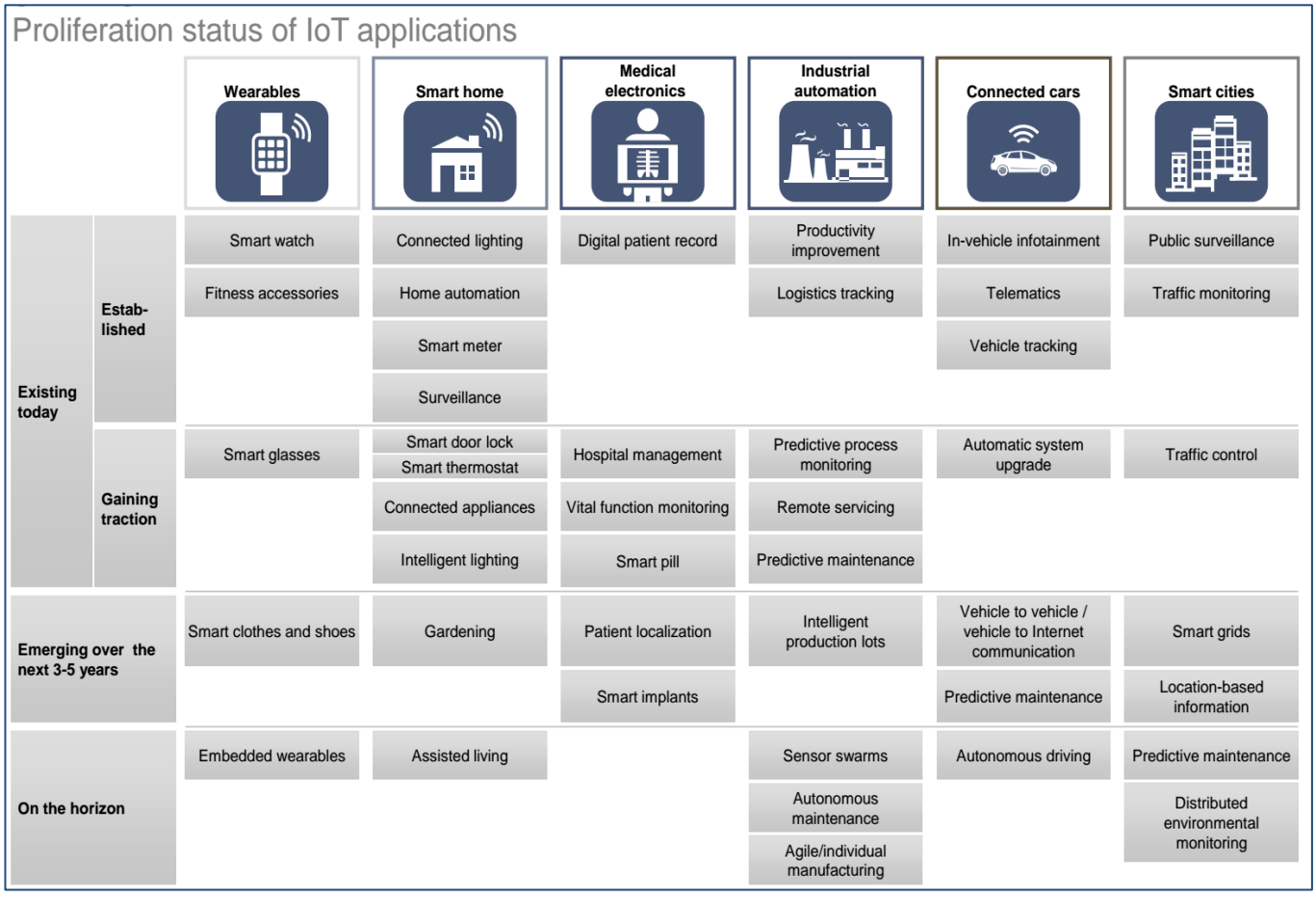


Figure 3 – Existing IoT case studies. Source: McKinsey

The Connected Home

Much like Bradbury's 1950's vision of the future home, the Connected Home will seamlessly wrap itself around our domestic lives. The smart kitchen will hold the biggest opportunities. Smart fridges will allow consumers to track and manage inventory from anywhere around the world using their PC, smartphone or tablet. Barcode scanners will tell consumers their favourite brand and where to buy it.

[12] Alec Scott, '8 ways the Internet of things will change the way we live and work' *The Globe and Mail: Report on Business* (online) <*http://www.theglobeandmail.com/report-on-business/rob-magazine/the-future-is-smart/article24586994/#health*>

[13] McKinsey&Company and Global Semiconductor Alliance (**GSA**), *Internet of Things: Opportunities and challenges for semiconductor companies* (May 2015) <*http://www.gsaglobal.org/wp-content/uploads/2015/05/1.-GSA-McK_Report-IoT_Text_Executive-Summary.pdf*> Exhibit 1 p.2.

Weight sensors and smart jars will let consumers know when they're running low, and RFID tags on the bottle will notify them when the product is about to expire.

Figure 4 – IoT innovation? Source: Humoar

The Connected Home will learn its occupants' habits – their smart watch (with heart-rate monitor), alarm clock, smart shower and smart kitchen will all work in unison to ensure that the occupants wake up at the optimal part of their sleep cycle and that their toast pops out as soon as the relevant individual passes the kitchen door's sensor. Entertainment will be seamless – every speaker, smart TV and media device will run on the home network and be controlled centrally. Sensors will allow media to follow occupants around the house, streaming their music as they leave and enter each room. TV programs can even follow them into the kitchen[14]. All consumers have to do is give their Amazon Echo a shout. Their Google Nest products will take care of temperature, home surveillance and fire safety, ensuring that their absence does not go unnoticed. When they return home, sensors and smartphone geo-location will let the home know to unlock the doors, turn the alarm system off, turn the air conditioner off and ready the lights when they are near.

The Connected Human

These days, a mobile phone seems like the only organ outside of our bodies. **Forrester Research** in 2013 envisioned a very connected human (a 'Wearables Man' – **Figure 5**), as our smartphones get smaller, become wearable, embeddable and even implantable[15]. Current activity trackers and smartwatches can log heart rate, caloric expenditure, location, distance travelled and sleeping patterns in real-time.

Connected wearables extend to smart rings, smart clothing and even mobile 'mood monitoring' services that can predict signs of depression. Like smartphones, many wearables are GPS-enabled and can help keep tabs on objects, children, infants, pets and elderly relatives that need round-the-clock care. The Connected Human's 'life-logging' devices won't just be wearable – they will be ingestible, invisible and implantable. **Google** and **Novartis** are working on contact lenses for diabetics that monitor blood glucose levels[16]. **Proteus Digital Health** offers smart pills, patches and mobile apps to help monitor health.

[14] Sam McNerney, 'Smart Fridge Manages Your Grocery List And Monitors Food Freshness' *PSFK* (online) (29 January 2012) <*http://www.psfk.com/2012/01/samsumg-smart-fridge.html*>
[15] Tom Kaneshige,'How the 'Modern Man' Will Wear Technology' *CIO* (online) (11 December 2013) <*http://www.cio.com/article/2380278/consumer-technology/how-the--modern-man--will-wear-technology.html*>
[16] Andrew Morse, 'Novartis and Google to Work on Smart Contact Lenses' *The Wall Street Journal* (online) (15 July 2014) <*http://www.wsj.com/articles/novatis-google-to-work-on-smart-contact-lenses-1405417127*>

What does this mean for you?

Being able to 'quantify' oneself and one's movements will give consumers an unprecedented insight into their own personal health. It may also revolutionise patient care, as smart implants allow for remote diagnostics and patient monitoring. As more and more data is collected on unhealthy *and* healthy individuals, more accurate medical decisions can be made[17]. Medical practitioners can use non-consumer devices like **Google's** health-tracking wristband and tools such as Apple HealthKit and ResearchKit to collect accurate, real-time clinical data on patients and population.

Pairing activity trackers with other devices may prove to be a convenient, but risky affair. Take, for example, real-time heart-rate data. This data can tell how fit someone is and how they sleep, but timely fluctuations can also suggest other *inferences* be made about them. This may include caffeine consumption, arousal to certain stimuli, when and which recreational drugs they take[18], and when, how often and intensity of their sex life[19]. Some wearables on the market even offer 'sexual performance tracking' as a feature. Interestingly, the technology used in this application is virtually identical to similar products on the market, indicating that most wearables have this capability but these particular capabilities are not part of the 'features' offered as part of the product.

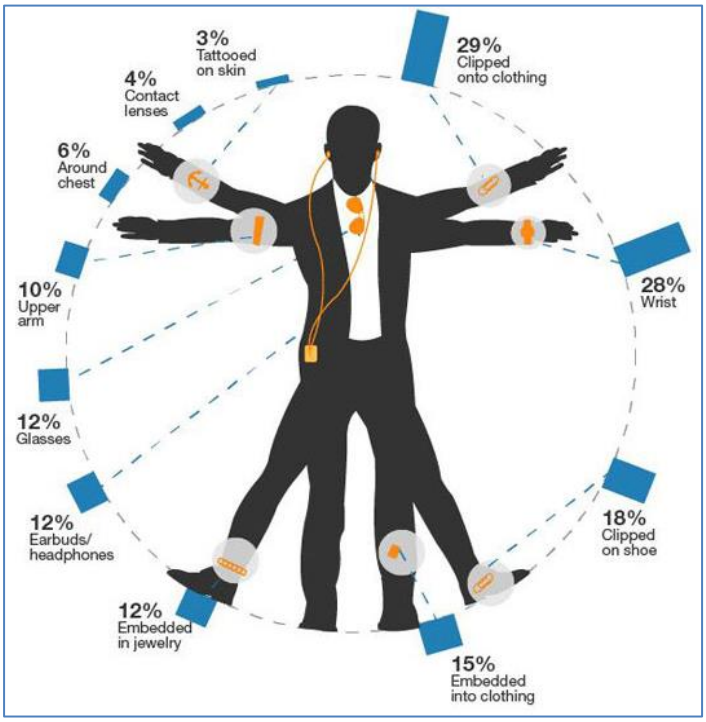


Figure 5 – Forrester's Vitruvian "Wearables" Man. Source: CIO

The Connected Habitat

In the short-to-medium term, IoT will have a greater impact on the public sector and industry than on individual consumers. Most current IoT case studies offer consumers either novelty or convenience - neither of which are revolutionary. **Marcus Weldon**, CTO of Alcatel-Lucent, described current IoT devices as "cute" and "curiosities" but not "transformative"[20]. The consumer safety, cost savings and time saving implications are yet to be fully realised. In the *short to medium term*, IoT offers far more significant benefits to *industry and public sector*. They stand to benefit from IoT innovation, supply chain optimisation, real-time environmental analytics and boosts in productivity. However, once IoT

[17] Derrick Harris, 'Why data is the key to better medicine — and maybe a cure for cancer' *Gigaom Research* (online) (27 November 2012) <https://gigaom.com/2012/11/27/why-data-is-the-key-to-better-medicine-and-maybe-a-cure-for-cancer/>

[18] Azad Ghuran and Jim Nolan, 'The cardiac complications of recreational drug use' (2000) 173(6) *Western Journal of Medicine* 412.

[19] RA Stein, 'Cardiovascular response to sexual activity' *American Journal of Cardiology* (2000) Jul 20;86(2A):27F-29F.

[20] Robin Wauters, Interview with Marcus Weldon for *Tech EU* (online) (via video interview, June 2015) <http://tech.eu/features/5230/alcatel-lucent-cto-marcus-weldon-video-interview/>

'synergy' is fully realised, *consumers* will be the *long-term* beneficiaries of IoT by way of cheaper and improved delivery of products and services.

Smart cities are the most ambitious of IoT projects. Millions of sensors and mass upstream data collection will allow government to better manage public infrastructure. Parking space sensors will guide commuters to the nearest free spot. Road sensors and in-car GPS data will allow better monitoring of traffic and toll management as traffic is managed and diverted in real-time. In-car data can synchronise with traffic lights to ensure better traffic flow.

Connected/autonomous vehicles and smart traffic are two more exciting areas of IoT. Modern cars already contain an ever-growing plethora of 'smart' and 'connected' features, such as the new BMW flagship sedan and the highly anticipated Tesla range of connected electric cars. **Google** is currently leading the way in testing their driverless cars[21], with other manufacturers following suit[22]. A number of reputable studies indicate that over 90-99% of accidents are due to human error[23]. Autonomously driving cars have the potential to remove some of the risks of human drivers, including fatigue, response time, distraction and drink-driving. Additionally, sensors can notify drivers of road conditions, and real-time smart city analytics will ensure safer routes.

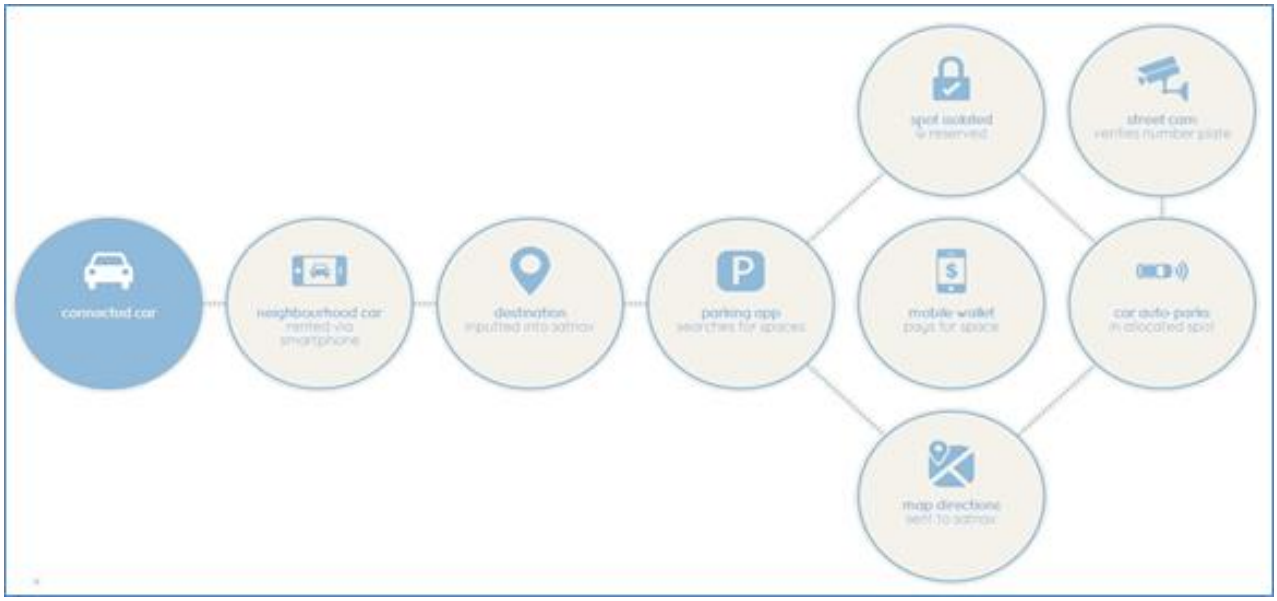


Figure 6 – Visualising the connected car. Source: Information is Beautiful

[21] Darrell Etherington, 'Google's Latest Self-Driving Car Prototypes Are Now On Mountain View Streets' *Techcrunch* (online) (25 June 2015) <*http://techcrunch.com/2015/06/25/googles-latest-self-driving-car-prototypes-are-now-on-mountain-view-streets/*>

[22] Richard Willingham, 'Driverless cars: closer and safer than you think' *Sydney Morning Herald* (online) (29 May 2015) <*http://www.smh.com.au/victoria/driverless-cars-closer-and-safer-than-you-think-20150528-ghc3wl*>

[23] Bryant Walker Smith, 'Human Error as a Cause of Vehicle Crashes' *The Center for Internet and Society* (online) (18 December 2013) <*https://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes*>

Internet of Things: Past, Present and Future

History of the Internet of Things

The term 'Internet of Things' was first used by **Kevin Ashton** in a presentation for US consumer goods company Procter & Gamble in 1999[24], in which he explained how he was able to track lipstick inventory using an RFID tag.

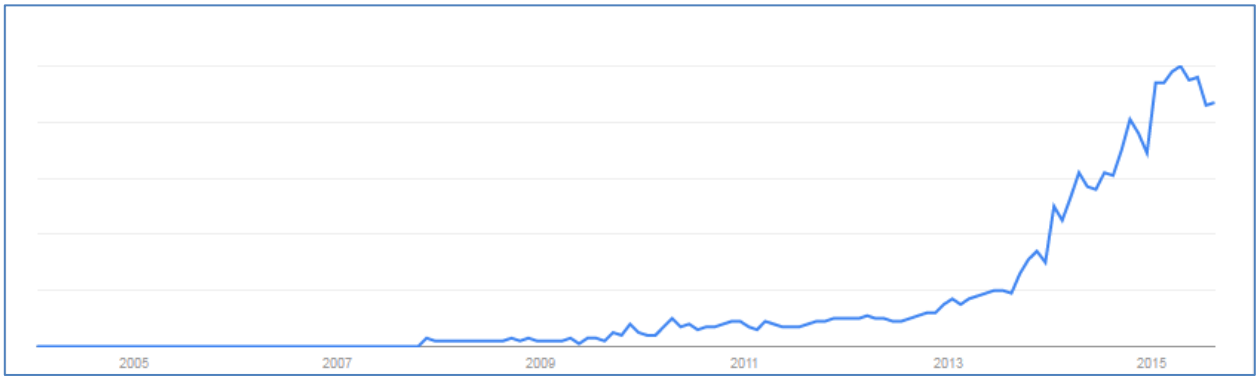


Figure 7 – Google search: "Internet of Things". Source: Google Trends

The first 'connected device' is often attributed to the 'Xerox PARC networked coke machine' in the late 1980's, a vending machine at Carnegie Mellon University that was connected to the Internet so that the inventory and temperature could be monitored[25]. In 1990, **John Romkey** and Australian **Simon Hackett** connected a toaster to the Internet for the Interop Internet IT show[26]. In 2008-09, the number of 'things' exchanging data on the Internet exceeded the number of people, with Cisco describing this event as the 'birth of the Internet of Things'[27].

The Current State of Internet of Things in Australia

Australian IoT statistics are difficult to come by, default proof of IoT's conceptual immaturity domestically. Even Australia's former Minister for Communications, Malcolm Turnbull MP, had to use non-Australian statistics when opening a recent AIIA IoT Conference[28]. It is perceived by some that Australian consumers are "hardly awake even to the existence of IoT"[29].

It is not until recently that Australian organisations have conducted research and produced public reports on IoT. Two notable examples, both released over the past two months, are the Communications Alliance report titled "Enabling the Internet of Things in Australia", and the ACMA's occasional paper titled "Internet of Things and the ACMA's areas of focus—Emerging issues in media

[24] Kevin Ashton, 'That 'Internet of Things' Thing' *RFID Journal* (online) (22 June 2009) <http://www.rfidjournal.com/articles/view?4986>
[25] Frank Palermo, 'Internet of Things Done Wrong Stifles Innovation' *Information Week* (online) (7 July 2014) <http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/a/d-id/1279157>
[26] William Stewart, 'The Internet Toaster' *Living Internet blog* <http://www.livinginternet.com/i/ia_myths_toast.htm>
[27] Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything* (Cisco White Paper, April 2011) <http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> p.3.
[28] Malcolm Turnbull, opening address for the AIIA Summit: *Navigating the Internet of Things* (26 March 2015) <https://www.youtube.com/watch?v=t8lZl7hGCFI&index=3&list=PLpK9LWXfxsoo4ZUN3fgVt2CYswyEzv21f>
[29] Interview with Malcolm Crompton, former federal Privacy Commissioner (via email, 3 July 2015)

and communications". The former is a comprehensive, high level overview of IoT and industry issues, and the latter takes a focus on spectrum and numbering implications for Australia.

In discussing the economic value of IoT in Australia, both aforementioned reports cite a McKinsey Global Institute June 2015 report titled "Unlocking the potential of the Internet of Things", which predicted IoT's value at $11.1 trillion globally by 2025. Australia's contribution is around 1.15% of global GDP, translating to a ~116 billion annual impact on the Australian economy[30] (**Figure 8**).

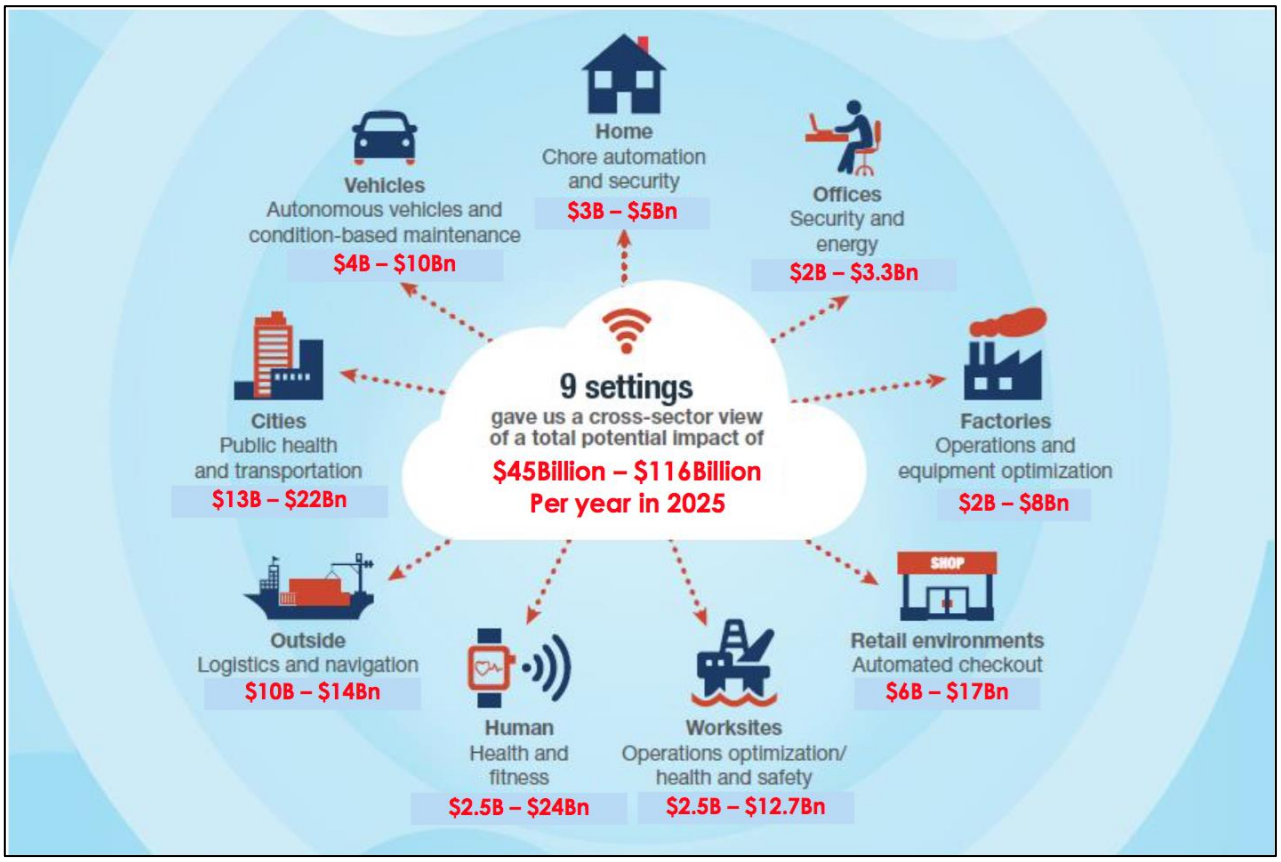


Figure 8 – High-level estimate of Australian economic impact of IoT. Source: Comms Alliance

A 2013 study by **Cisco** calculated the size of the Australian IoT market at $36 billion[31]. Research from **Frost & Sullivan** calculates the APAC M2M market at around $4.6 billion in 2013, predicted to grow to $58 billion by 2020. Of that, China contributes to 45.0% of total IoT spending, with Australia at around 3.8%[32]. Recent research from **Vodafone** and **Ovum** forecasted Australia's M2M market to be

[30] Communications Alliance, *Enabling the Internet of Things in Australia* (online) (2015) <*http://www.commsalliance.com.au/__data/assets/pdf_file/0009/50967/Enabling-the-Internet-of-Things-for-Australia.pdf*> p 67.
[31] Cisco, *Internet of Everything Value Index* (online) (2013) <*http://ioeassessment.cisco.com/explore/full#/country/aus*>
[32] Frost & Sullivan, *Asia Pacific IoT Market Overview* (2014) <*https://www.telstra.com.au/content/dam/tcom/business-enterprise/machine-to-machine/pdf/business-m2m-2014-asia-pacific-ict-awards.pdf*>

worth A$530 million by 2019 with an annual growth rate of around 20%[33]. **Microsoft** estimated that Australia has 1.9 million M2M devices operating today, and over 3 million by 2017[34].

The Future of Internet of Things

From its humble inception in 1999, IoT has emerged as one of the most hyped terms in the digital space. In fact, the **2015 Gartner Hype Cycle**[35] placed IoT and related concepts at the highest point of the 'Peak of Inflated Expectations' (**Figure 9**):

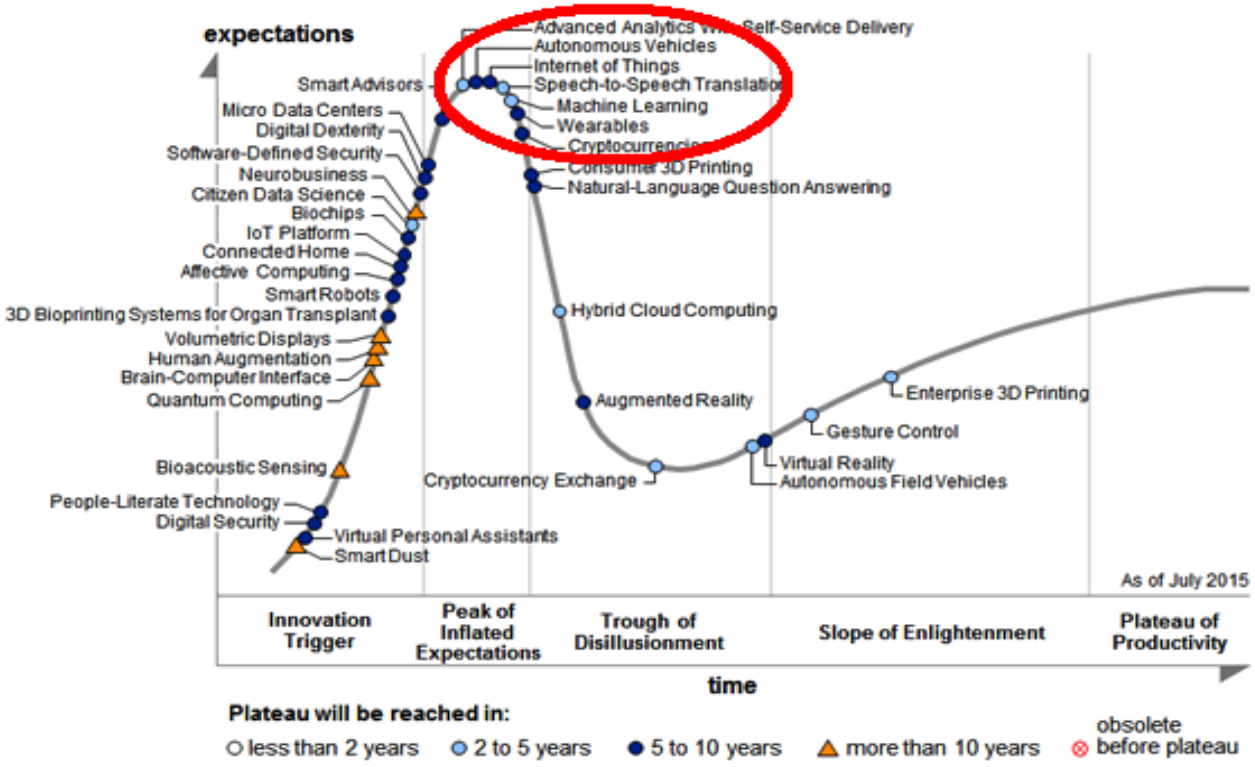


Figure 9 – Gartner's Hype Cycle 2015. Source: Gartner

In the opinion of UNSW academic **Kate Carruthers**, the development of IoT will follow **Amara's Law**: *"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run"*[36]. It is hard to disagree with this prediction in the context of IoT.

Potential 'Size' of Internet of Things

Projections of IoT's size are staggering. One of the most cited statistics is **Cisco's** predicted 50 billion connected devices by 2020[37]. **IoT Analytics** has compiled a number of IoT projection summaries[38], including one on global IoT device forecasts, below (**Figure 10**).

---

[33] Vodafone, *Connected Nation: M2M in Australia 2014-2019* (September 2014) <http://www.vodafone.com.au/doc/Vodafone_Connected_Nation_M2M_in_Australia.pdf> p.3

[34] Microsoft and Telsyte, *Cut through: How the Internet of Things is sharpening Australia's competitive edge* (February 2015) <https://mscorpnews.blob.core.windows.net/ncmedia/2015/02/Microsoft_IoT_Whitepaper.pdf> p.4

[35] Gartner, *Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor* (18 August 2015) <https://www.gartner.com/newsroom/id/3114217>

[36] Wikipedia, *Roy Amara: Amara's Law* (accessed 8 August 2015) <https://en.wikipedia.org/wiki/Roy_Amara#Amara.27s_Law>

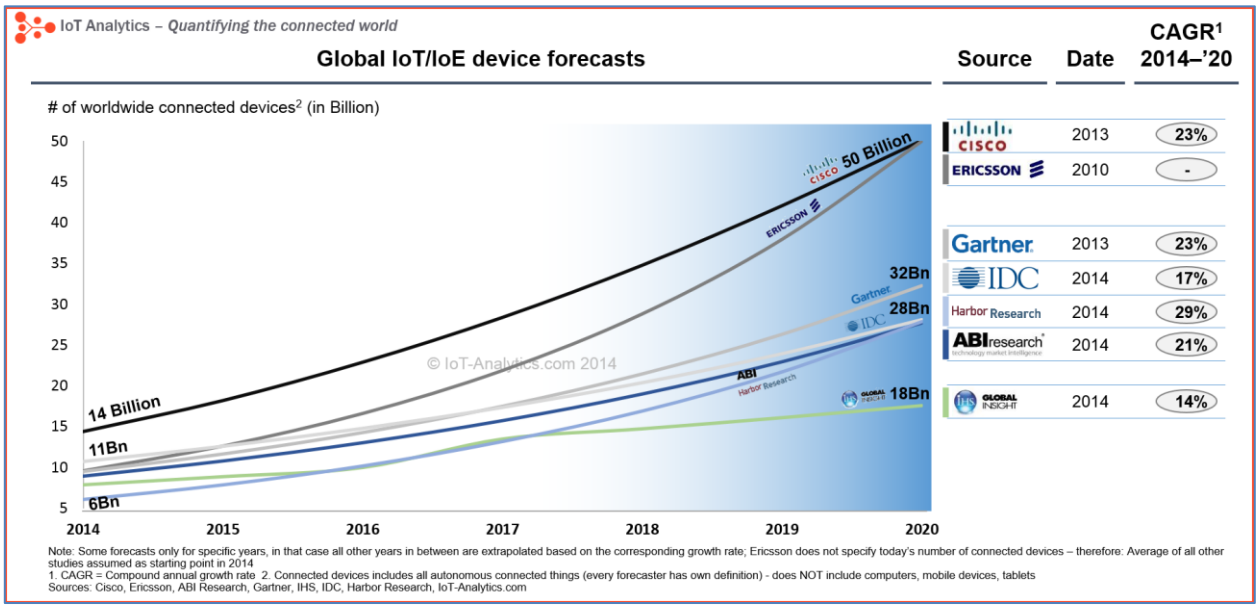


Figure 10 – Graphic summary of global IoT forecasts. Source: IoT Analytics

Potential 'Value' of Internet of Things

IoT Analytics has also compiled two IoT 'value' summary graphs[39]. **Figure 11** graphically summarises IoT's 'total economic value' and **Figure 12** shows IoT's 'annual generated revenue'.

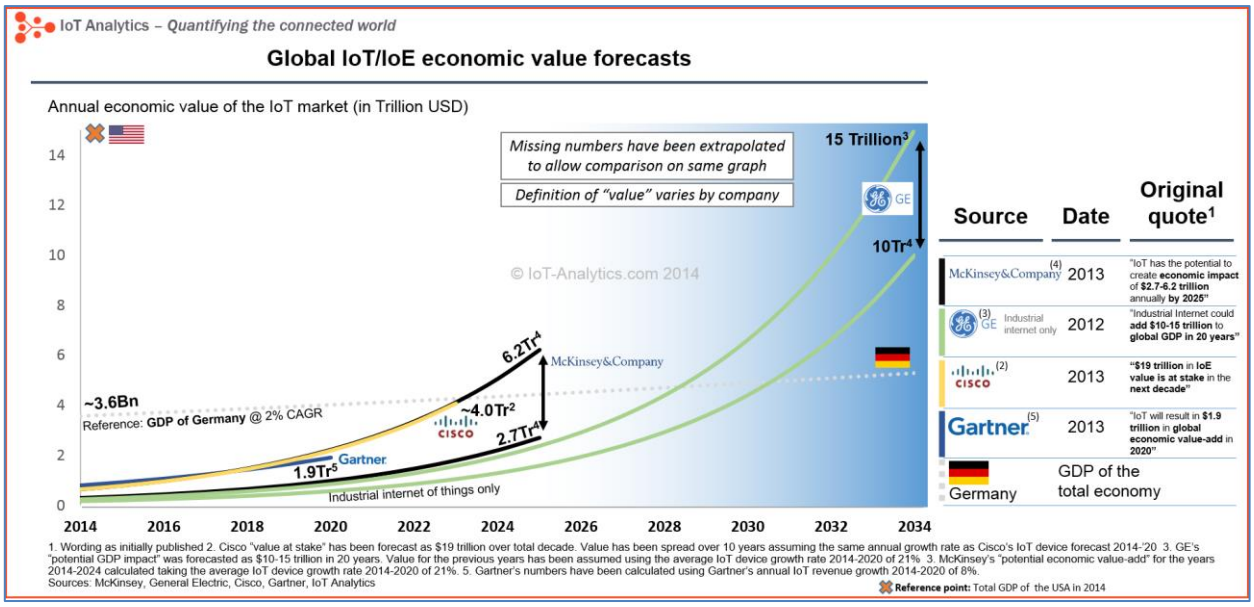


Figure 11 – Graphic summary of IoT total economic value forecasts. Source: IoT Analytics

---

[37] Cisco, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything* (White Paper, April 2011) <*https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf*> p 3.

[38] Knud Lasse Lueth, *IoT market analysis: Sizing the opportunity* (IoT Analytics report, March 2015) <*http://iot-analytics.com/product/whitepaper-iot-market-analysis-sizing-the-opportunity/*> p.1

[39] Knud Lasse Lueth, *IoT market analysis: Sizing the opportunity* (IoT Analytics report, March 2015) <*http://iot-analytics.com/product/whitepaper-iot-market-analysis-sizing-the-opportunity/*> pp 4-5.

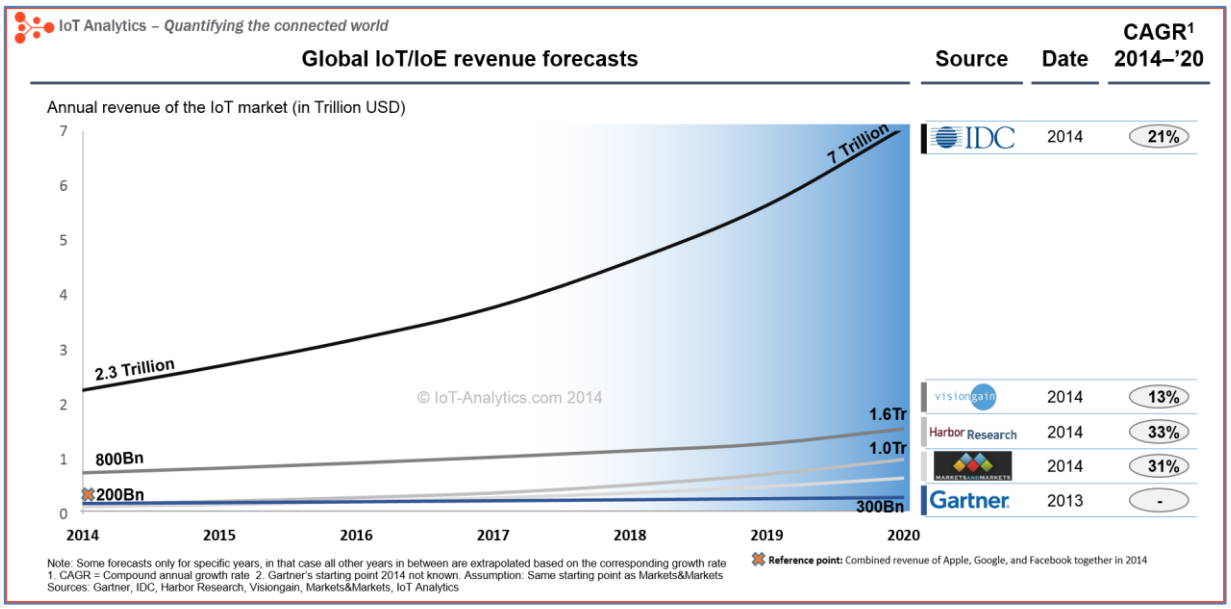


Figure 12 – Graphic summary of IoT annual generated income forecasts. Source: IoT Analytics

Cisco's 2013 IoT White Paper predicted that IoT would be worth USD$14.4 trillion in value by 2022[40], including *savings* created by IoT: reduced operating costs ($2.5 trillion); employee productivity ($2.5 trillion); and eliminating supply-chain waste ($2.7 trillion). This value figure was revised to $19 trillion in 2014[41]. **GE** calculated IoT *opportunity* to be worth $21 trillion, or 30% of the $70 trillion dollar world economy, as of 2011[42]. **McKinsey** predicted *annual* IoT value at $11.1 trillion by 2025 (including consumer surplus)[43], **Gartner** predicted a value of $1.9 trillion by 2020[44] and **IDC** predicted $8.9 trillion by 2020[45] (up from $7.1 trillion earlier that year![46]). Research by **Telsyte** predicts that *Australian* spending on Connected Home products will be $3.2 billion by 2019[47].

The **Comms Alliance IoT Report** provides some useful value calculations, in an Australian context[48].

[40] Joseph Bradley, Joel Barbier and Doug Handler, *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion* (Cisco White Paper, 2013) <http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf> p.1
[41] Cisco, *The Internet of Everything—A $19 Trillion Opportunity* (2014) <http://www.cisco.com/web/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf> p.1
[42] Peter C. Evans and Marco Annunziata, *Industrial Internet: Pushing the Boundaries of Minds and Machines* (GE report, 26 November 2012) <http://www.ge.com/docs/chapters/Industrial_Internet.pdf> p.13
[43] McKinsey&Company *The Internet of Things: Sizing up the opportunity* Executive Summary (June 2015) <http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity> p.4
[44] Gitta Rohling, 'Facts and Forecasts: Billions of Things, Trillions of Dollars' *Siemens* (online) (1 October 2014) <https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/internet-of-things-facts-and-forecasts.html>
[45] Larry Dignan, 'Internet of things: $8.9 trillion market in 2020, 212 billion connected things', *ZDNet* (online) (3 October 2013) <http://www.zdnet.com/article/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things/>
[46] Leon Spencer, 'Internet of Things market to hit $7.1 trillion by 2020: IDC' *ZDNet* (online) (5 June 2014) <http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/>
[47] Telsyte, 'Australian IoT @ Home market to reach $3.2 billion by 2019 embedding smart technology into everyday life' (10 August 2015) <http://www.telsyte.com.au/announcements/2015/8/10/australian-iot-home-market-to-reach-32-billion-by-2019-embedding-smart-technology-into-everyday-life-1>
[48] Communications Alliance, *Enabling the Internet of Things in Australia* (online) (2015) <http://www.commsalliance.com.au/__data/assets/pdf_file/0009/50967/Enabling-the-Internet-of-Things-for-Australia.pdf> pp 103-6.

Internet of Things and Consumers

Who is the 'Consumer' of Internet of Things?

In general, a 'consumer' is an entity that purchases goods and services for personal use. According to the Australian Telecommunications Consumer Protections Code, an *individual* Australian consumer is one that acquires a service for personal or domestic use[49]. This paper will approach the definition of 'consumer' broadly. For instance, *customers* are 'consumers' of a retail experience or marketing; *citizens* are 'consumers' of government services; *patients* are 'consumers' of health care; and *passengers* are 'consumers' of transportation services. Since IoT will affect all of these services, 'consumers' of IoT is a broad category indeed.

The Consumer Drivers of Internet of Things

In a 2014 preliminary report, the **ISO/IEC JTC 1** identified a number of IoT market drivers[50]. Of these, the relevant *consumer* drivers are listed and explained in **APPENDIX 1**. In summary, *"the market for IoT will be driven by the availability of: low cost; low/sustainable power; interconnected objects, people, systems and information resources; and of the desire to use the functionality provided by a collection of interconnected devices that can be configured into systems and modified as needed"*[51].

Building Consumer Confidence

While some surveys suggest that consumers are growing optimistic about IoT[52], others suggest a declining interest in domestic IoT products[53]. Australian technology consultant **Rachel Dixon** doesn't think that anyone has made a compelling enough argument for *consumer* IoT adoption yet, and that IoT is a *"solution in search of a problem"*[54].

Consumer Privacy and Trust

IoT privacy and security (in devices, networks and providers) are drivers of consumer trust, which in turn drives take-up rates. **Robert Gregory**, partner of Australian law firm Maddocks, says that *"the public must have confidence not only in the devices and supporting communications infrastructure, but the legal and policy frameworks which underpin them...[including] confidence that personal, financial and other confidential information will be protected and not inappropriately used by any of business, government or crime"*[55].

---

[49] Communications Alliance, *Telecommunications Consumer Protection Code* (TCP C628:2012, 2012) <http://www.commsalliance.com.au/Documents/all/codes/c628>

[50] International Organisation for Standardization/International Electrotechnical Commission Joint Technical Committee 1 ("**ISO/IEC JTC 1"**), *Internet of Things (IoT) Preliminary Report 2014*, 2015 <http://www.iso.org/iso/internet_of_things_report-jtc1.pdf> p.4

[51] International Organisation for Standardization/International Electrotechnical Commission Joint Technical Committee 1 ("**ISO/IEC JTC 1"**), *Internet of Things (IoT) Preliminary Report 2014*, 2015 <http://www.iso.org/iso/internet_of_things_report-jtc1.pdf> p.9

[52] Colin Neagle, 'How to sell the Internet of Things to consumers' *Network World* (online) (11 June 2015) <http://www.networkworld.com/article/2933318/opensource-subnet/how-to-sell-the-internet-of-things-to-consumers.html>

[53] Argus Insights, *Connected Home Demand Report* (Consumer survey report, 2015) <http://www.argusinsights.com/connected-home-2015/>

[54] Interview with Rachel Dixon, technology adviser (via telephone, 15 June 2015).

[55] Interview with Robert Gregory, Maddocks law firm (via online correspondence, 9 June 2015)

According to the **OAIC**, 60% of Australians would cease doing business with a company because of privacy concerns, and around the same figure are uncomfortable with websites or smartphone apps collecting personal information[56]. A global **Fortinet** study (including Australia) revealed that over half of respondents believe that privacy is important and that they do not trust the way that their data is handled[57]. Two thirds wanted greater control over handling of their personal data. Far more surveys on consumers and privacy perception have come out of the US. A recent **University of Pennsylvania report** revealed growing resentment and helplessness, with most US consumers believing it is futile to try and manage what companies learn about them[58]. A **Microsoft** report found that almost 100% of respondents are willing to give away personal information for cash rewards, 90% for discounts and two-thirds for loyalty programs[59]. A more recent, global survey by **Accenture** found that for 47% of respondents find privacy and security concerns a barrier to IoT take-up[60]. These consumer studies show that privacy and trust are not just ethical concepts - they make good business sense.

The underlying message is clear – *"what we need to remember is that this is not about the government, it's not about the telcos, it's about the customer...or citizen...what is the customer's need?...Then you make sure you can satisfy those needs in the most seamless, simple, compelling, attractive way possible and be as imaginative about it as you can"* – Malcolm Turnbull, Minister for Communications[61].

[56] OAIC, *Community Attitudes to Privacy Survey* (Research report, 2013) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf> p.4

[57] Fortinet, *Fortinet Reveals "Internet of Things: Connected Home" Survey Results* (23 June 2014) <http://www.fortinet.com/press_releases/2014/internet-of-things.html>

[58] Joseph Turow, Michael Hennessy and Nora Draper, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation* (Report, Annenberg School for Communication, University of Pennsylvania, June 2015) <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>

[59] Greg Sterling, 'Survey: 99 Percent Of Consumers Will Share Personal Info For Rewards, But Want Brands To Ask Permission', *MarketingLand* (online) (2 June 2015) <http://marketingland.com/survey-99-percent-of-consumers-will-share-personal-info-for-rewards-also-want-brands-to-ask-permission-130786>

[60] Accenture, *Igniting growth in consumer technology* (Global survey, 2015) <https://www.accenture.com/us-en/insight-ignite-growth-consumer-technology>.

[61] Malcolm Turnbull, opening address for the AIIA Summit: *Navigating the Internet of Things* (26 March 2015) <https://www.youtube.com/watch?v=t8lZl7hGCFI&index=3&list=PLpK9LWXfxsoo4ZUN3fgVt2CYswyEzv21f>

The Internet of Things and Consumer Issues

The main body of this report will follow the fictional Babel family of Sydney, Australia. The year is 2020 and they enjoy the benefits (and perils) of Connected Homes, Humans and Habitats. Their story is split into four scenes, and after each scene specific consumer issues are identified and discussed.

Scene One: Home, Connected Home

6:46am 6 July 2020 *- The Babel family begins to awaken, but their Connected Home did not sleep.* ***Olivia Babel*** *has to start her day as a 'data scientist' at 09:00. The Babel home knows her calendar, and has analysed traffic conditions. It talks to her activity tracker and, in unison, they decide that 06:46 is the best time to wake up - she is at the ideal point in her sleeping cycle and it gives her enough preparation time. They also measure her temperature, perspiration and movement, logging it with her sleep-tracking app. Her smart pyjamas send a mild sensory pulse throughout her body, slowly waking her up without a sound. This does not disturb her husband,* ***Johannes Babel****, who is sleeping next to her. He is a medical practitioner who monitors his patients remotely, allowing him to work from home. Once the room senses that Olivia is up and out, the smart lighting slowly intensifies, until Johannes gently wakes up at 07:34 in time for his teleconference at 08:00.*

The ***'ME-ternity'*** *smart home platform pre-sets the shower temperatures. Once notified that Johannes and Olivia are up, the kitchen gets to work. The smart fridge notes that there is not enough almond milk for everyone, so its screen tells the Babels that they can either accept a smaller serving and/or select from alternative recommendations based on what they have in their pantry and popular chefs' recommendations. They don't want a smaller serving. The fridge places an urgent order with their closest supermarket, and for a small premium in price, the almond milk is delivered by drone in under ten minutes. More groceries will be delivered by driverless truck by mid-afternoon.*

Olivia kisses her young daughter ***Evey Babel*** *good morning. Evey is busy playing games on her tablet. Olivia pauses the game from her own smartphone using a parental control app, and tells Evey that she can resume once she finishes her breakfast. Evey places her used cutlery in the dishwasher. It schedules a wash for midday, when water prices are usually lowest. Another sensor picks up on a fault, so makes an appointment with a technician when the Babel calendar is free. Johannes will confirm this calendar appointment when he gets the chance.*

Johannes is upstairs on the phone, moving between the bathroom, bedroom and hallway. The lights follow him throughout the house, and the Bluetooth speakers in each room allow him to continue his teleconference as he enters each room. His schedule displays on the bathroom mirror as he brushes his teeth, ending the call with a button on the wall (his mouth is too busy to end the call verbally). The toothbrush makes note of some biometric data, and lets his diet app know that his teeth are a bit stained. The diet app realises that he has been drinking a lot of coffee, confirms this with the usage data on the espresso machine, and sends his activity tracker a reminder to zap him when his 4th espresso causes his heart rate to spike one too many times. It's for his own good.
On their way out, the Babel home gives Olivia and Evey a summary of their journey to work and school.

It also congratulates Olivia on being in caloric deficit this weekend, based on her diet app and smart cutlery. Burger for lunch, she thinks. It's the little things.

Internet of Things: Devices, Standards and Interoperability

The Babels' Connected Home could do all of those things because every 'thing' talked to every other 'thing' seamlessly. For perfect M2M communication, each 'thing' must use the same communication protocol. For instance, when a TV's remote control 'talks' to the TV, it does so because they can send, receive and understand infrared signals (the 'standard' used). The TV and remote control are ***interconnected***, and because they both recognise the same 'standard' communication and work in unison, they are ***interoperable***. Another example is electricity ports - each port, socket and adapter in Australia is the same size and shape because they all adhere to a strict set of manufacturing standards. Standards ensure that manufacturers build each device with matching capabilities.

What are IoT 'Standards'?

A '**standard'** is a widely-accepted, often 'official' model, norm, measurement, protocol or process used in an industry to ensure that all products across the industry can communicate and operate with each other. **Table 1** below looks at some existing 'standards' that IoT may use:

Table 1 – Relevant standards for IoT

***Network* standards**	***Communication* standards**	**Sensors**
These standards ensure that devices can connect to one or many networks or the Internet. The device might have multiple 'standards' built in so that it is able to connect to one of a few networks.	These standards ensure that devices can communicate to each other and 'speak the same language'. This is the most relevant to IoT, because IoT requires many 'things' communicating seamlessly.	These may or may not be 'standardised', but are essential components of IoT devices. Each sensor collects specific data, and standardisation ensures that data is accurate across the board.
Examples: Cellular voice and data networks (2G/GSM, 3G/HSPA, 4G/LTE, GPRS, EDGE) and each mobile network frequency.	**Examples:** Wi-Fi (WLAN 802.11) standards, Bluetooth, GPS, Near Field Communication (NFC), USB and infrared.	**Examples:** Accelerometer, altimeter, gyroscope, proximity sensor, compass, barometer, heart rate monitor and hydrometer.
Applications: Using cellular data on your smartphone, connecting to different telephone operator networks to make calls.	**Applications:** Home Wi-Fi, in-car Bluetooth, Wireless headphones, GPS navigation, 'checking in' to places via location, Mastercard 'Paypass' and 'Visa Paywave', Wireless Sensory Networks (**WSNs**).	**Applications:** GPS Navigation, activity tracking, tracking 'steps taken', gesture control, determining atmospheric pressure or humidity, and vehicle detection systems.

Current IoT standardisation has been described as a "jumbled mess"[62] as there are no universal definitions, frameworks or consistency across the functional layers of the services they comprise. Most traditional devices are relatively power-hungry, and the network standards (above) may not be ideal for tiny 'things' containing simple sensors and without the physical space for larger capacity batteries. There are currently dozens of wireless communication standards used in IoT devices, none of which are universally accepted.

One important international standards body is the **Institute of Electrical and Electronics Engineers** Standards Association **(IEEE-SA)** responsible for some of the most widely-used and widely-recognised standards IEEE 802.11 (Wi-Fi), and IEEE 802.15.4 (Zigbee). In the IEEE, there are more than 350 IEEE standards that are applicable to IoT, 40 of which are being revised to better support IoT. Furthermore, there are more than 110 new IoT related IEEE standards in various stages of development. The IEEE is also sponsoring 10 or more different IoT advocacy and support groups. While theirs is possibly the strongest, the IEEE is certainly not alone as the **International Telecommunications Union** (ITU) also has standards groups such as the IoT Global Standards Initiative (IoT-GSI) and the IoT Joint Coordination Activity (JCA-IoT) as does the **Internet Engineering Task Force** (IETF).

What is the 'Ideal' IoT Standard?

Picking the ideal network or communication standard for IoT will depend on the requirements of the connected 'things' – do they need to communicate across large distances? Will they emit tiny bursts of data frequently? Is battery-life important? Is their usage data heavy? Do they need a constant, reliable connection or can they cache data and send it later?

IoT devices have unique requirements, and *generally* require three properties:

1. Constant data connection;
2. Low power usage; and
3. The ability to communicate short distances[63].

In May 2015, **McKinsey** compiled a similar list of IoT device requirements and related them to some IoT case studies: smart meters, smart watches and industrial automation (**Figure 13**)[64].

[62] Kieren McCarthy, 'The Internet of Things: a jumbled mess or a jumbled mess?', *The Register* (online) (14 May 2015) <http://www.theregister.co.uk/2015/05/14/the_internet_of_things_a_jumbled_mess_or_a_jumbled_mess/>
[63] Ibid.
[64] McKinsey&Company *The Internet of Things: Sizing up the opportunity* (Summary Report, June 2015) <http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity> p.14

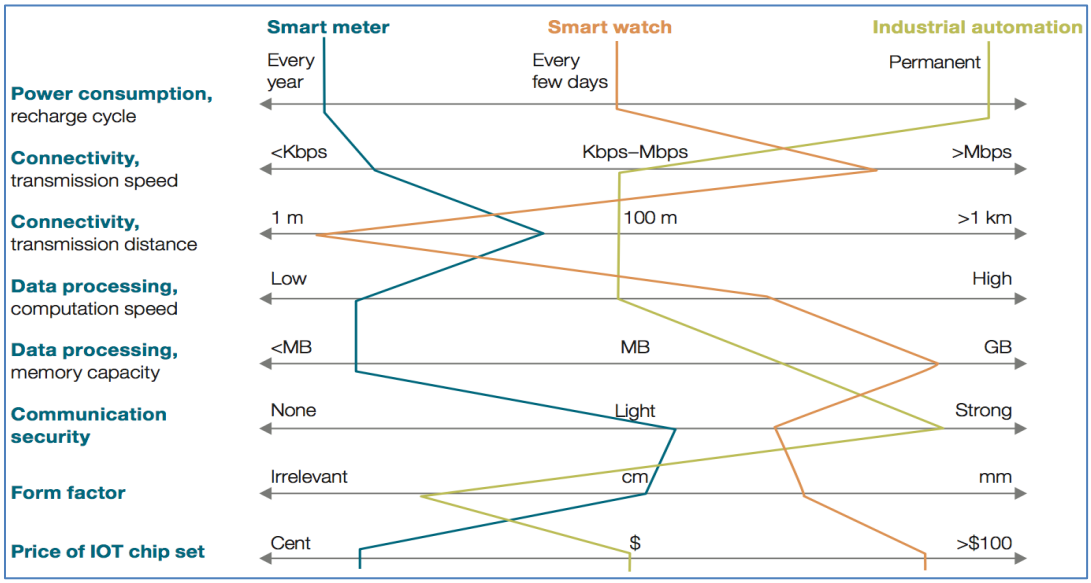


Figure 13 – IoT devices and common requirements. Source: McKinsey

In addition to the network and device characteristics, picking the 'ideal' standard for a specific IoT ecosystem will also depend on the nature of the network – is it dispersed across great distances? Are the IoT devices fixed to a power source? **Table 2** is a matrix describing some of the geo-spatial characteristics and the ideal corresponding network[65].

Table 2 – M2M applications by dispersion and mobility. Source: OECD

	Geographically Fixed	Geographically Mobile
Geographically dispersed	**Application:** Smart grid, smart meter, smart city and remote monitoring **Technology required:** PSTN, broadband, 2G/3G/4G, power line communication	**Application**: Car automation, eHealth, logistics, personal devices **Technology required:** 2G/3G/4G, satellite
Geographically concentrated	**Application:** Smart home, factory automation, eHealth **Technology required:** Wireless personal area networks (WPAN), wired networks, indoor electrical wiring, Wi-Fi, RFID, Near Field Communication	**Application:** On-site logistics **Technology required:** Wi-Fi, WPAN

Most connection standards are not new – NFC, cellular and fixed broadband standards have been around for decades. Some new IoT-specific communication technologies are emerging, mostly in the form of Wireless Sensory Networks ("**WSNs"**), specifically designed for IoT 'things'. Industry players and organisations have formed 'alliances' to create their own IoT device ecosystems and technology frameworks, including: **Zigbee** (Comcast, Kroger, Philips, ARM, AT&T and more), **Z-Wave** (ADT, SmartThings, LG and more), **NikeFuel** (Nike), **Open Interconnect Consortium** (Cisco, Intel, GE,

[65] Communications Alliance, *Enabling the Internet of Things in Australia* (online) (2015) <*http://www.commsalliance.com.au/__data/assets/pdf_file/0009/50967/Enabling-the-Internet-of-Things-for-Australia.pdf*> p 30, reproduced from Chapter 6: 'Emerging Issues: The Internet of Things' in OECD, *OECD Digital Economy Outlook 2015* (15 July 2015) <*https://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm*> p 266.

Samsung, Dell, HP, Siemens and more), **Industry Internet Consortium** (Intel, IBM, ATT, Cisco, GE and more), **AllJoyn** (Qualcomm, LG, Sharp, Haier, Panasonic, Sony, Cisco, Canon, HTC, Microsoft and more), **Thread** (Google, Samsung, ARM, Nest and more), whilst more proprietary platforms include **Weave** (Google) and **Apple HomeKit/HealthKit.** Doubtless many more are will emerge and disappear as the markets mature.

After discussing some of the main communication and network standards relevant to IoT, the **Comms Alliance IoT Report** made several observations on IoT standards:

1. Interoperability is a key enabler of IoT systems;
2. Australia should not endeavour to create *new* IoT standards – there is a sufficient amount available; and
3. Choosing the right 'standard' will depend on the industry, application or service performed by the IoT device(s) and IoT network/ecosystem[66].

This report makes similar observations and agrees that there is no 'one-size-fits-all' standards solution. While industry working groups and regulatory intervention may be useful, it is the opinion of the author that market forces will determine the dominant IoT standards for specific needs much faster than policy-makers will. Policy-makers should 'innovate, wait *then* regulate' in the event of a market failure.

Communication Breakdown in the Connected Home

Without clear IoT standards, there can be no reliable interoperability or interconnectivity. This makes building a seamless Connected Home difficult. Let's assume that Johannes' smart toothbrush was not Internet-enabled. If it wanted to talk to his espresso machine (also 'unconnected'), it would probably do so with a short or mid-range connection like Bluetooth or NFC. But what if his espresso machine did not support the same communications protocol?

Australian homes currently have an average of 9 connected devices, and this figure is expected to increase to an average of 29 by 2020[67]. The **OECD** predicts that by 2022, there will be an average of 50 connected devices per household in OECD countries[68] (**Table 3**). Unless all of these devices could communicate and interoperate, the potential of the future Connected Home is greatly reduced, and will look nothing like the Babel's 2020 Connected Home.

[66] Communications Alliance, *Enabling the Internet of Things in Australia* (online) (2015) <*http://www.commsalliance.com.au/__data/assets/pdf_file/0009/50967/Enabling-the-Internet-of-Things-for-Australia.pdf*> p 87-88.
[67] Harry Tucker, 'NBN report says we will need faster internet to handle modern lives, but will our broadband be fast enough?' *News.com.au* (online) (23 November 2015) <*http://www.news.com.au/technology/online/nbn/nbn-report-says-we-will-need-faster-internet-to-handle-modern-lives-but-will-our-broadband-be-fast-enough/news-story/79d7d16d9afa406c195e06a242b182fc*>
[68] Chapter 6: 'Emerging Issues: The Internet of Things' in OECD, *OECD Digital Economy Outlook 2015* (15 July 2015) <*https://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm*> p.256

Table 3 – OECD's Connected Home of 2022. Source: OECD

2012	2017	2022
2 smartphones	4 smartphones	4 smartphones
2 laptops/computers	2 laptops	2 laptops
1 tablet	2 tablets	2 tablets
1 DSL/Cable/Fibre/Wi-Fi Modem	1 connected television	3 connected televisions
1 printer/scanner	2 connected set-top boxes	3 connected set-top boxes
1 game console	1 network attached storage	2 e-readers
	2 e-readers	1 printer/scanner
	1 printer/scanner	1 smart meter
	1 game console	3 connected stereo systems
	1 smart meter	1 digital camera
	2 connected stereo systems	1 energy consumption display
	1 energy consumption display	2 connected cars
	1 internet connected car	7 smart light bulbs
	1 pair of connected sport shoes	3 connected sport devices
	1 pay-as-you-drive devices	5 internet connected power sockets
		1 weight scale
		1 e-health device
		2 pay-as-you-drive devices
		1 intelligent thermostat
		1 network attached storage
		4 home automation sensors
Devices that are likely but not in general use		
E-readers	Weight scale	Alarm systems
Sportsgear	Smart light bulb	In-house cameras
Network attached storage	E-health monitor	Connected locks
Connected navigation device	Digital camera	
Set-top box		
Smart meter		

In the words of **Andy Caddy**, CIO of Virgin Active, *"We want standards because it's very hard to do anything when Nike want to talk about 'Fuel' and Fitbit want to talk about 'Steps' and Apple want to talk about 'Activity', and none of these things equal the same things"*[69]. **Chris Taylor** from Mashable describes this domestic communication breakdown as *"A mess of threads tangled around different objects in separate rooms, each one guarded by different companies that beckon developers and users while growling at each other"*[70].

[69] Interview with Any Caddy in Jonathan Brandon, 'Exclusive: How Virgin Active is getting fit with the Internet of Things', *Business Cloud News* (online) (10 July 2015) <http://www.businesscloudnews.com/2015/07/10/exclusive-how-virgin-active-is-getting-fit-with-the-internet-of-things/>

[70] Chris Taylor, 'Nest Cam is here, but the 'Internet of Things' still isn't', *Mashable* (online) (18 June 2015) <http://mashable.com/2015/06/17/nest-cam-internet-of-things/>

Serviceability of the Connected Home, Human and Habitat

Another consumer issue that arises in the above scenario is that of device serviceability. Effectively managing up to '50 connected things per household' may be a challenge for some consumers.

Maintenance of 'Things'

Maintenance has a hardware and software element. In terms of **hardware maintenance**, all physical parts wear with use and time. As we adopt more and more 'smart' light bulbs and sensors, it will mean more physical 'things' that need to be replaced if they malfunction or become worn out. What if one sensor, of many, stops functioning? Do manufacturers need to build in 'sensors for sensors', so that the malfunction is identified, or will the 'thing' simply carry on, collecting and transmitting *inaccurate* data?

Software maintenance requires appropriate updates and monitoring. Software should be constantly updated for security and performance. When dozens or hundreds of 'things' need software updates, what is the best way to manage this? *Automatic updates* are one option, but may leave users vulnerable to unwanted features. Another solution is for IoT service providers to notify users of *'significant' updates* only. *Manual updates* give users greater control, but leave them vulnerable to security risks until the software is updated manually.

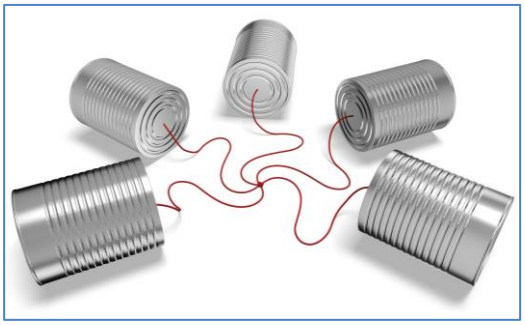


Figure 15 – Communication breakdown. Source: Shutterstock

Obsolescence and Device Life

Software updates can only go so far – IoT software will eventually outstrip hardware capacities. What happens if the Babels' smart fridge becomes obsolete and the manufacturer stops supporting its software? What if third-party software developers no longer build or update applications for it?

Sciencewise describes 'planned obsolescence' as *"a policy of producing consumer goods that rapidly become out of date, achieved by frequent changes in design, termination of the supply of spare parts, and the use of non-durable materials"*[71]. Some experts express concern about this: *"My car is 16 years old. I'm not sure I'd appreciate replacing a vehicle every few years due to software or security glitches that can't be patched because the wheel size is wrong"*[72]. How long will it be until the Babel family's cheap smart toothbrushes, or their expensive smart car, is obsolete?

Powering your 'Things'

Hundreds of 'things' means hundreds of 'things' that require power. Battery longevity is essential for connected 'things'. This is usually not a problem since most sensors use very little power. Also, connected 'things' may be embedded and can be constantly connected to a power source, or even

[71] Footnote 13 in Sonia Bussu, *The Internet of Things: the case of public voice* (ScienceWise Expert Resource Centre research report, July 2014) <http://www.sciencewise-erc.org.uk/cms/assets/Uploads/2014-11-14IOTEdited-for-publicationFinal.pdf> p.3

[72] Michael Kassner, 'Why experts are nervous about the Internet of Things' *TechRepublic* (online) (26 February 2014) <http://www.techrepublic.com/article/why-experts-are-nervous-about-the-internet-of-things/>

solar powered. Consumers need to consider energy consumption when connecting their home – cost, installation, maintenance and logistics.

Device Migration and Data Portability

Let's assume the Babel family wanted to move, renovate or simply change network providers. Moving or renovating their Connected Home will now involve reconnecting their home, re-synchronising their devices, reconnecting their 'things' and with any luck, retaining their digital status quo. Computerworld contributing editor **Preston Gralla** shared his own ghastly vision of re-connecting an IoT home:

> *"You replace an old router with a new one. Your refrigerator, oven, microwave, light bulbs, heating system, air conditioner, door locks, security system, and even your toothbrushes (yes, there are already network-connected toothbrushes) were all connected to your old network. Now you need to connect them to your new one... There will be no common operating system for them, no standard way to connect and disconnect... how easy do you think it will be to connect your stove?"*[73]

Migrating data between IoT 'ecosystems' is a bigger problem. **Steve Dalby**, former Chief Regulatory Officer of iiNet, noted some "costs of disengagement" when switching IoT ecosystems: psychological pressure, re-synchronising each device, re-configuring for different standards and software, severing brand loyalty and the general hassle of data transfer[74]. Let's say that the Babel family are an **Apple** family – they have built their home based on an Apple HomeKit ecosystem and their activity trackers use Apple HealthKit. The devices synchronise and communicate fluently. What if they start using a few **Google** or **Amazon** products and realise that they prefer them? What if Apple's IoT platform is not compatible with others – the data backed up and stored in ways that only allow for Apple-to-Apple interoperability? The Babel family are forced to either find third-party applications to do this, reluctantly stick to Apple products or 'migrate' their entire Connected Home because their original IoT ecosystem doesn't 'play nicely' with others.

Another conundrum arises if the Babels ever want to move, or sell their Connected Home. It is essential that the Babel family do not leave behind any personal information. Any connected fixtures may be difficult to remove, and their data must be securely wiped, thus the Babels need to remove all personal information stored by their Connected Home and connected 'things'. If the Babels do not wipe or change the connected security system codes, security cameras or appliances, and therefore still have remote access to these, the new occupants are vulnerable to privacy or security intrusion. Recently, the **Online Trust Alliance** and **US National Association of Realtors** compiled a useful checklist for vendors and purchasers of Connected Homes.

[73] Preston Gralla, 'The Internet of Things: Your worst nightmare' *Computerworld* (online) (7 July 2015) <http://www.computerworld.com/article/2944680/internet-of-things/the-internet-of-things-your-worst-nightmare.html>
[74] Interview with Steve Dalby, former iiNet Chief Regulatory Officer (via telephone, 4 June 2015).

'Cognitive Bandwidth'

A more conceptual consumer issue is 'cognitive bandwidth'. This refers to our capacity to mentally manage daily information input. In the context of IoT, this is the ability to 'keep on top of' all of our 'things'. If each 'thing' needs maintenance and attention, how long before we become overwhelmed by so many connected devices?

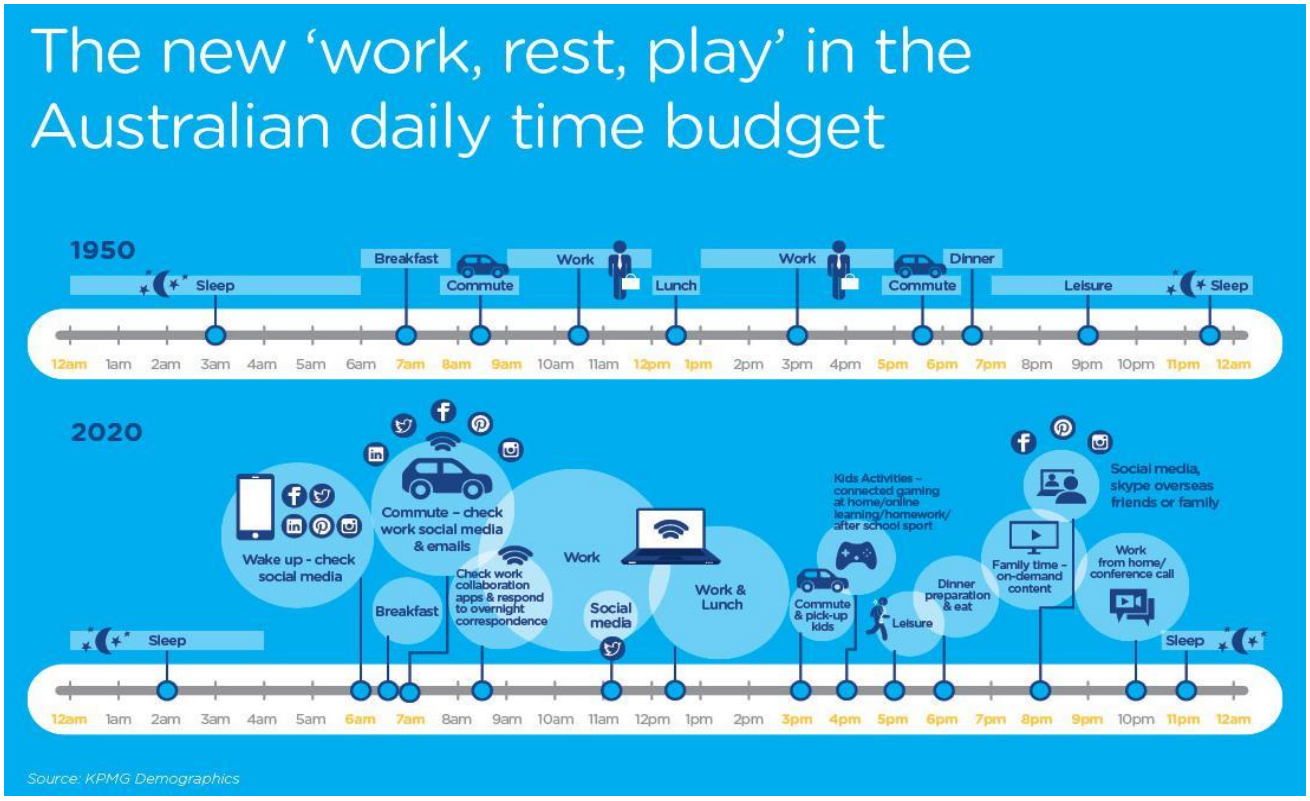


Figure 16 - Digital Australians. Source: nbn via KPMG Demographics.

Cognitive bandwidth may be the IoT version of the 'Dunbar Effect'. British anthropologist **Robin Dunbar** found that humans have a 'maximum' number of meaningful social relationships we can effectively manage – 150. **Accenture** recently combined this with **Nielsen** research that found that despite an increased use of mobile phones, the average number of apps used remained static at around 25[75]. If we apply these findings to the Babel family, we can quickly see how keeping up with so many devices can become mentally draining. **Jenny Judge** of The Guardian is more optimistic, envisioning an automated life that brings solitude, leisure and time for reflection[76].

[75] Nielsen, 'Smartphones: So many apps, so much time' (1 July 2014) <http://www.nielsen.com/us/en/insights/news/2014/smartphones-so-many-apps--so-much-time.html>

[76] Jenny Judge, 'The search for solitude in an internet of things', *The Guardian* (online) (20 July 2015) <http://www.theguardian.com/technology/2015/jul/20/the-search-for-solitude-in-an-internet-of-things>

Scene Two: Guardian Angels

11:46am, 6 July 2020 *– It's a slow day for Johannes. His patients are not doing much, and the data from their activity trackers confirms this. He walks out of his office and into the kitchen to make his second double-espresso for the day. His smartwatch vibrates – his diet app is being worrisome again. The Babel kitchen sensed his arrival and his medical monitoring program is now displayed on the smart fridge's screen. He finishes his espresso and walks into the lounge room. Again, his work program follows him to the screen of the main TV set. He sits on the couch. "ME-ternity, listen!" he exclaims. The Babel home's ME-ternity home hub springs to life – within half a second, it captures the sound bite, sends it to the ME-ternity server in Estonia, authenticates his voice, and confirms the command. "TV, split screen, channels one and six", he commands. ME-ternity splits the TV screen between his work program and a shopping channel. He sees George Clooney holding up a cup of his favourite brand of espresso. This is followed by an advertisement for longer lasting sex. "ME-ternity - TV, mute!" He turns his attention to his tablet.*

The 'Me-Money; Me-Problems' personal finance app displays the Babel expenses summary. The power usage is unusually high – probably the solar panels on Evey's window shades playing up. Something catches his eye – his insurance premiums seem to fluctuate monthly, although still payable annually. He zooms into the bar graph and notices that each hour showed a different rate, and seems to change frequently. His health insurance has gone up, but Olivia's has gone down. Home insurance dropped by 10% last month and has stayed down. These fluctuations seem to begin around Christmas (when the family received activity tracking smartwatches) and when Johannes installed the 'Safe-me First' home security system.

"ME-ternity, Jon to RisQi Insurance, teleph-" – he is cut off by another notification, this time via his medical monitoring program on the TV screen. One of his patients has triggered the distress button on his wearable device. He rushes back to his desk. His program follows him onto his laptop screen. He accesses the patient's health records via the NSW Health E-Health database – ***Wayne NACCA****, 80% vision impairment...* ***Assistance*** *'Field Medic' GPS bracelet, guide-dog ("****Harrison"****).*

Johannes tracks Wayne's heart rate in real-time – it is high, but not indicative of a disorder. No other biometric signs of emergency. The 'Field Medic' GPS shows that Harrison's GPS dog collar is around the corner. Harrison must have run off. "ME-ternity, Jon to Sutherland Shire Council, Medical Assistance, Non-Emergency, telephone…", he yells, eyes glued to the screen. ME-ternity connects him to an operator. Johannes briefs the operator, who dispatches a mobile medical unit to Wayne's location. He is reunited with Harrison. Heart rate stabilises. Johannes makes a note on Wayne's E-Health record. He steps away from his office. Another espresso. Another vibration. Another health insurance fluctuation.

The Connected Human: Healthcare and Wearables

In the above scenario, we see a few different sides to IoT, healthcare and wearables. Wearables in the medical industry allowed Johannes to monitor his patient remotely, in real-time and with very accurate physiological data. He was able to remedy Wayne's (non) emergency remotely. On the flip side, Wayne was tracked, raising privacy and consent issues. Astute readers will also recall Johannes' caffeine consumption and Olivia's recent health kick – are their wearables sharing this information with their health insurance provider?

As part of this 'healthcare revolution', users may be required to share some of their most intimate personal information with strangers. This sharing is dictated by the privacy policy of the IoT service provider, which users need to click 'agree' to. This can include data that devices collect, as well as any *inferences* that can be drawn from that data. Some of these inferences are very personal (and the quality of inference highly variable), including drug consumption, whereabouts in real-time, biological disorders, stress levels, fitness levels and even sexual performance. This section touches on all of these implications.

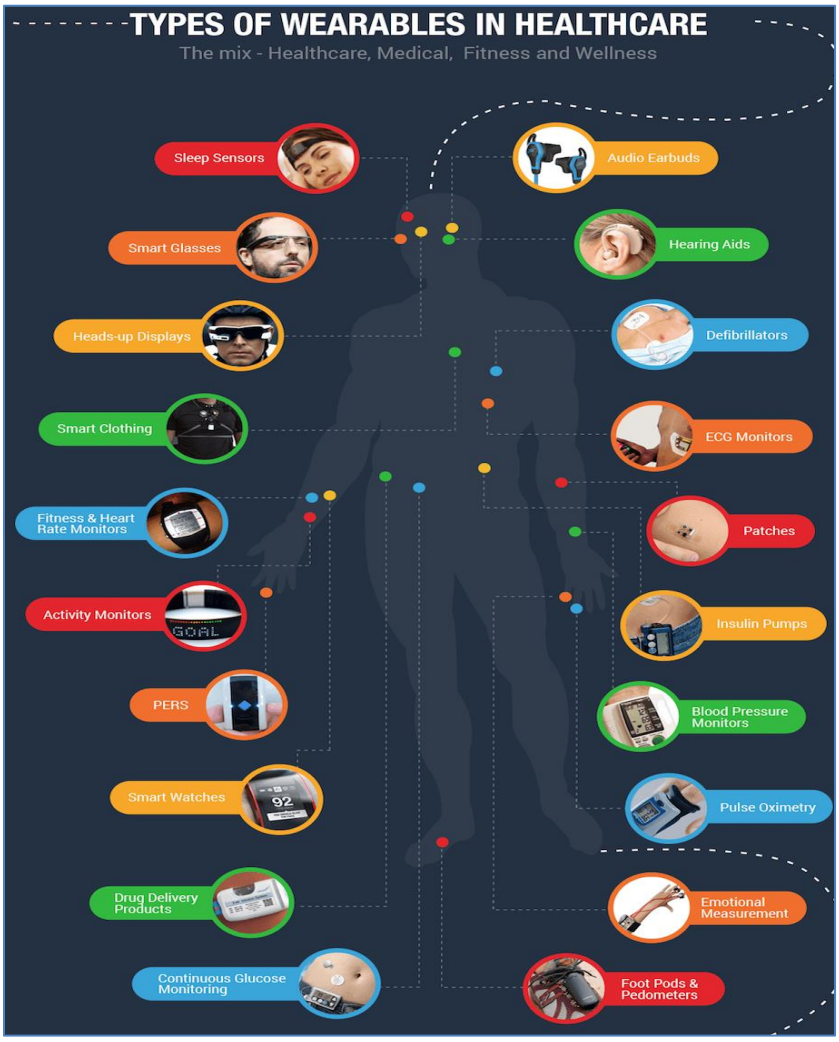


Figure 17 – Wearables in healthcare.
Source: Boston Technology

What Kinds of Devices are on the Australian Market?

The consumer market is already awash with wearable devices. **Figure 17** is an extract from a graphic depiction compiled by US firm **Boston Technology**[77]. Australian consumer group **CHOICE** is a good starting point for those wanting to seek out what's available locally[78]. The current Australian wearable market can be split into two main categories – activity trackers and smartwatches. The latter are more expensive, but frequently offer the features of activity trackers anyway. Examples of the former include Fitbit, Jawbone, Nike+, TomTom and Garmin products. Examples of the latter include the Pebble smartwatch, Apple Watch, Samsung wearables and Android Wear smartwatches.

Beecham Research created an interactive infographic depicting some wearables on the market, categorised by sector, application, functions and products[79] (**Figure 18**).

[77] HIT Consultant, *Infographic: Wearables in Healthcare* (13 February 2015) <*http://hitconsultant.net/2015/02/13/infographic-wearables-in-healthcare/*>
[78] Denis Gallagher, 'Smart watch review: Smartwatches - are we there yet?' *CHOICE* (online) (25 June 2015) <*https://www.choice.com.au/electronics-and-technology/gadgets/smartphone-gadgets/articles/smartwatch-reviews*>
[79] Beecham Research, *Wearable Technology Application Chart* <*http://www.beechamresearch.com/article.aspx?id=20*>

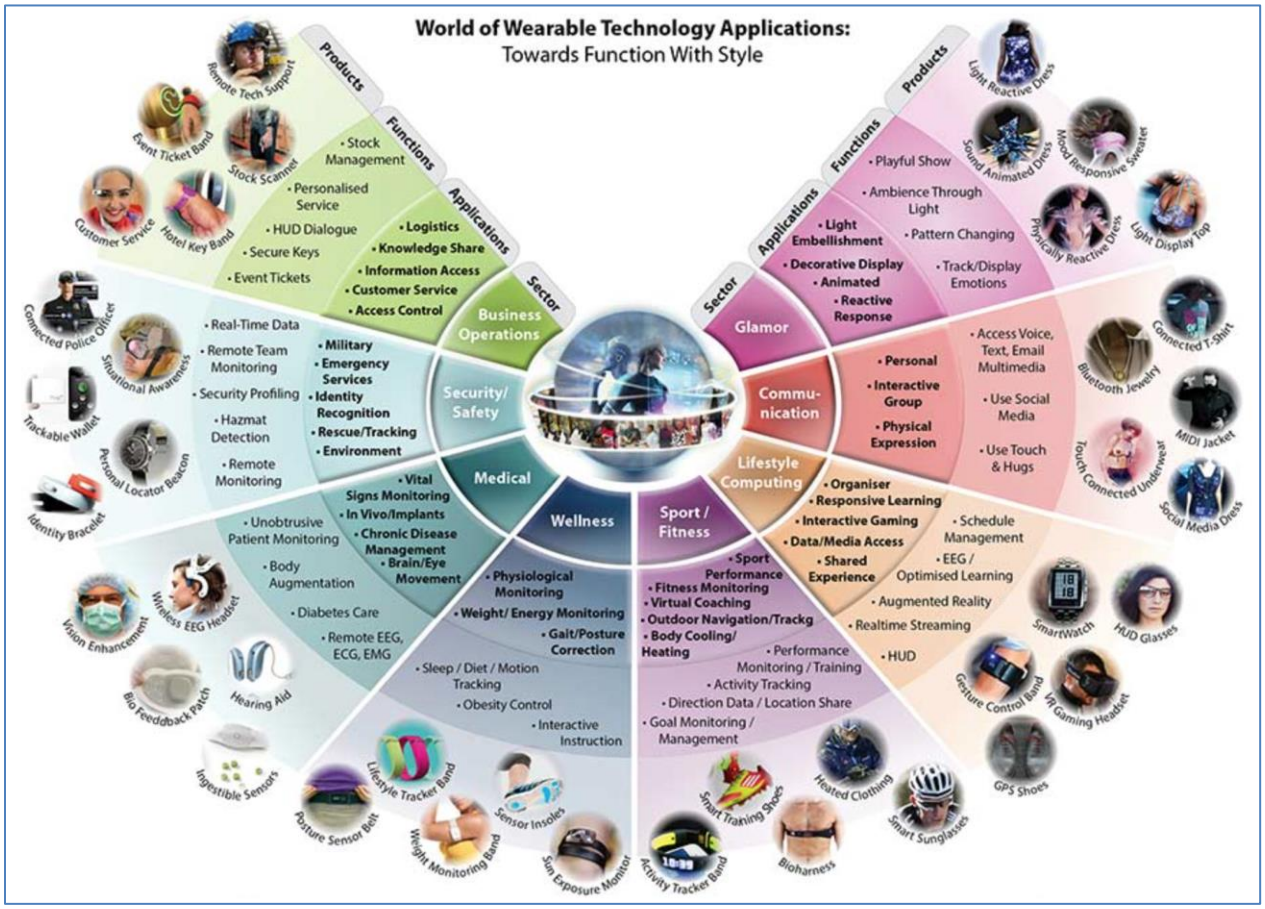


Figure 18 - Wearable technology application chart. Source: [Beecham Research]

What Kind of Data is being Captured?

Wearable devices contain an assortment of hardware components (like sensors or GPS), able to capture many types of physiological data. For example, altimeters can detect ascension (stairs taken) and accelerometers detect movement (activity). Combine GPS location and accelerometer data and 'steps taken' can also be reasonably ascertained. When cross-referenced with physical characteristics and data from the heart-rate monitor, an IoT service can estimate kilojoules expended.

Table 4 and **Figure 19** below list some example of datasets captured by wearables.

Table 4 – The Connected Human: Examples of Datasets Collected.

Heart rate	Steps taken	Physical movement	Altitude
Body Mass Index (BMI)	Sleep data (duration, REM quality, time, hours)	Respiratory rate	Blood glucose
GPS location	Blood pressure	Caloric intake/expenditure	Body temperature
Body fat	Environmental exposure (UV, humidity etc)	Atmospheric exposure (pollution etc.)	Compass data

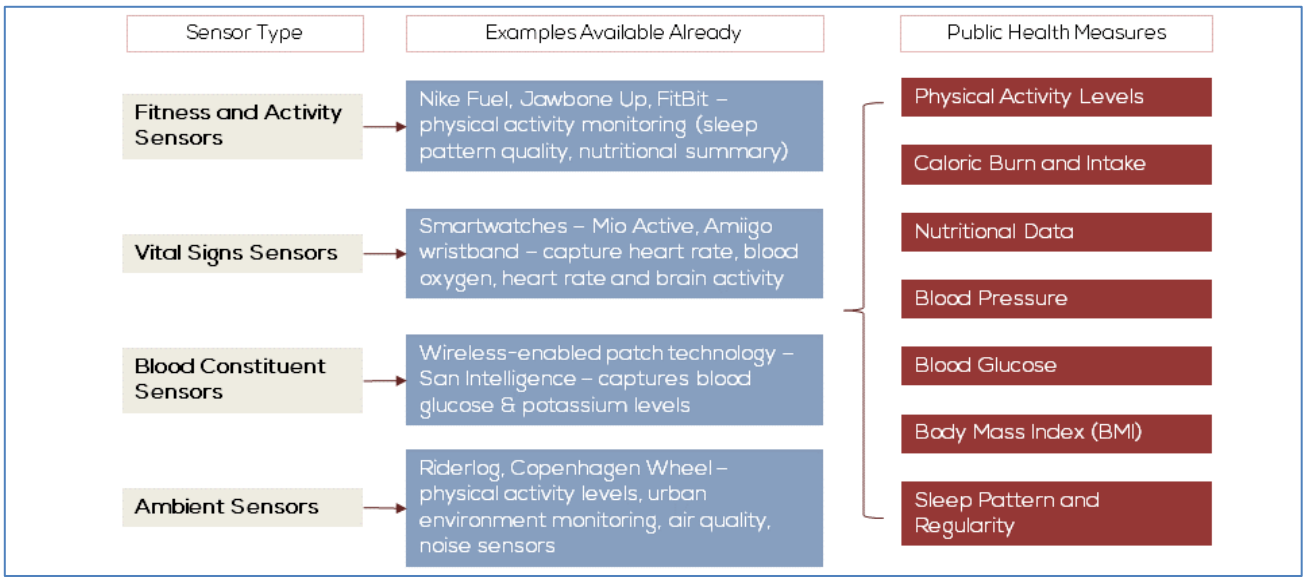


Figure 19 – Wearables sensors and inferences.
Source: Seeking Alpha compiled from academic research by Robert Steele and Andrew Clarke, USyd

What Inferences can be drawn from Connected Human Data?

Multiple data sets, when coupled with *contextual information* can form the basis of very uncomfortable and intrusive inferences. In the above scenario, Johannes formed some semi-accurate inferences from Wayne's wearable data. Wayne's real-time heart rate data was not indicative of an emergency, despite being in distress. When cross-referenced with the GPS data on Wayne and his guide dog Harrison, he could draw a more accurate inference.

However, Johannes himself was the subject of more sinister inferences. A combination of his heart rate, toothbrush data and smart espresso machine output (see **Scene One**) revealed his high caffeine consumption. This (de-identified) data was sold to marketers, who personalised coffee advertisements for him. This was followed by another advertisement for 'longer lasting sex' (see **Scene Two**). Coincidence? Perhaps his physical activity data was sold to opportunistic pharmaceutical companies for 'selective marketing'? It is not hard to join the dots in this scenario.

APPENDIX 2 is a table compiled by the author demonstrating three things: inferences that can be drawn from wearable data, how those inferences are drawn and possible value[80]. These inferences can be made by anyone with access to the data, especially if *multiple datasets* are available and combined with *contextual information* like time, location and personal details. For example, a rapid, significant spike in heart rate may be innocent. When combined with context (Saturday night, young male, located at a music festival etc.), it may *suggest* drug consumption.

[80] This list is non-exhaustive, and is the product of the author's reasonable deductions and limited biological knowledge.

How is Connected Human Data Handled?

Further to the above discussion on what data is captured, and how inferences can be drawn from that data, this section focuses on how data is handled. Is this data sold to third parties? When? Do we have notice of, or give consent to, these transactions? **Short answer – it's in the Privacy Policy**.

Let's take a look at an example. **Fitbit** is a market leader of fitness trackers in Australia. Data collected by Fitbit devices is governed by Fitbit's Privacy Policy. All users must 'agree' to this before use. This Policy details *what* types of data Fitbit collects, *how* they use this data, *which* data is shared with third parties, and *other ways* that data is shared. Unfortunately, **OAIC** research suggests that only half of Australians read privacy policies, because they are too long (52%), complex (20%) or boring (9%)[81].

Let's focus on the following excerpt from Fitbit's Privacy Policy (emphasis added):

> *"How we Use Your Data*
>
> *...**De-identified data** that does not identify you may be used to **inform the health community about trends; for marketing and promotional use; or for sale to interested audiences**. See Sharing of De-identified Data That Does Not Identify You to learn more..."*
>
> *What Data May be Shared with Third Parties?*
>
> *First and foremost: **We don't sell any data that could identify you**. We only share data about you when it is necessary to provide our services, when the data is de-identified and aggregated, or when you direct us to share it...*
>
> *...Fitbit may **share or sell aggregated, de-identified data that does not identify you with partners and the public** in a variety of ways, such as by providing research or reports about health and fitness or in services provided under our Premium membership...."*[82]

As per above, data held by Fitbit is either *identifiable* or *de-identified*. Under Fitbit's Privacy Policy, the latter can be sold to third parties for a wide array of uses, including marketing and promotional material. The data is *anonymised* – which means that only a set of data is sold, but not the identity of the user. That third party then uses that anonymous data for research, marketing or other purposes. If it is used for marketing, like in the case of Johannes, the marketer simply links 'data A' with 'anonymous user A', not 'Johannes' data' with 'Johannes'.

Medical Benefits of Connecting Humans

Data from wearable devices will allow unprecedented levels of personal health and fitness monitoring. Activity levels, training statistics, health and personal goals are available in real-time and in the palm of your hand (or on your wrist). As **Kevin Petrie** at Techcrunch puts it, *"informed people make better lifestyle decisions... and informed doctors provide better care, creating the right incentive to share vital data"*[83]. Sleep monitoring can help insomniacs and those wanting to improve their

---

[81] OAIC, *Community Attitudes to Privacy Survey* (Research report, 2013) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf> p 4.
[82] Fitbit AU, *Fitbit Privacy Pledge* (last updated 10 August 2014) <http://www.fitbit.com/au/privacy>
[83] Kevin Petrie, 'The Latest Big Data Innovation Is Consumer Empowerment', *TechCrunch* (online) (29 June 2015) <http://techcrunch.com/2015/06/29/the-latest-big-data-innovation-is-consumer-empowerment/>

energy levels. Heart rate monitors will give consumers a more detailed snapshot of their fitness levels than ever before. People with specific conditions will be able to better monitor them, including diabetics and even expecting mothers. Fitness fanatics can track their personal bests and progress, even sharing it with their friends or competitors.

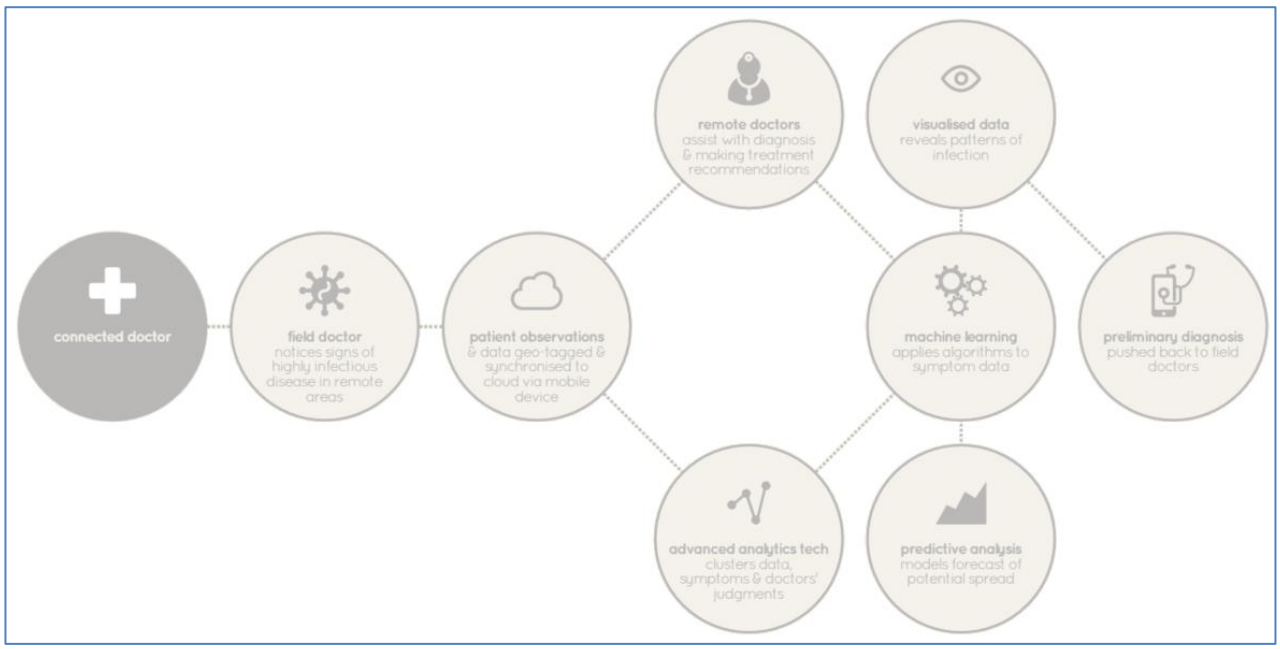


Figure 20 – Future patient/physician interactions. Source: Information is Beautiful

The benefits are arguably greater for the public if this data is stored centrally and accessed by medical practitioners. The UK Blackett IoT Review identified three areas of opportunity for public health: prevention and early identification, research, and tailored healthcare[84]. Another is remote monitoring of patients, such as Wayne in Scene Two. Academics in India recently consolidated the benefits of e-health into ten E's: efficiency, enhanced healthcare quality, based on evidence, empowerment of consumers and patients, encouragement of new relationships between patients and medical practitioners, education of physicians and patients, enabling exchange of information, extending scope of healthcare, ethics and equity[85].

Challenges of Connecting Humans

Greater collection of intimate personal information creates equally greater challenges. Journalist, writer and former legal practitioner **Kashmir Hill** raises several concerns about wearables[86], listed in **Table 5** below. The author has added commentary and an additional concern.

[84] UK Government Office for Science,*Internet of things: Blackett review* (Stakeholder input report and IoT literature review, 18 December 2014) <*https://www.gov.uk/government/publications/internet-of-things-blackett-review*> p. 29
[85] Yatin Jog, Apurva Sharma, Kalyani Mhatre and Anand Abhishek, 'Internet of Things As A Solution Enabler In Health Sector' (2015) 7(2) *International Journal of Bio-Science and Bio-Technology* 9, 10.
[86] Kashmir Hill, 'The privacy and security questions we must ask about the Apple Watch', *Fusion* (online) (9 March 2015) <*http://fusion.net/list/61049/apple-watch-privacy-security/*>

Table 5 – Wearables: Kashmir Hill's risks and concerns

Risk / Concern	Commentary
Is it easy to hack?	If a wearable device is connected, it can be compromised. The **US National Security Telecommunications Advisory Committee** made the distinction between the security of 'things' and the security of medical 'things': *"For an individual consumer, the risk is often minor; the failure of commercial IoT devices may be inconvenient, but generally do not threaten life or national security. Medical devices, however, including implantable ones, differ because an increasing number of them have built-in connectivity."*[87]
The device is always on and always on you	Just like our smartphones are 'the only organs outside of our body' – wearables never leave us. This attachment to our devices means that *every* action and fluctuation can be put into context.
What are your apps doing and sharing?	The **US Federal Trade Commission** ('FTC') had active discussions on IoT and wearables. The FTC studied 12 mobile fitness and health apps, revealing that they disseminated user information to 76 third parties. A similar study by **Evidon** found 20 apps disseminating data to 70 third parties[88], and one by **Privacy Rights Clearinghouse** stated that *"consumers should not assume any of their data are private in the mobile app environment – even health data that they consider sensitive"*[89].
Can your heart rate be subpoenaed?	Like any other stored data, it can be used as evidence in litigation or a criminal trial. In Canada, Fitbit data was used in a personal injury case[90] and in the US, Fitbit data was used to disprove sexual assault allegations[91].
Let's add another Connected Human consumer issue to Hill's list...	
Who will be monitoring this?	Wearable tracking is useful for personal fitness; medical diagnosis; treatment; and keeping tabs on loved ones. It can also be valuable to other specific groups of people: • **Athletes and coaches** benefit from this data. It allows them to quantify the fitness, training and progress of professional athletes. In the future, expect to see coaches mould their game plans around which athletes are quantified as the fittest. • By using wearables, **employers** can track employee location, health, sleep, alertness and productivity[92]. This may influence their daily decisions. For instance, if employee X didn't get much sleep last night, perhaps employee Y might

[87] US National Security Telecommunications Advisory Committee, *Report to the President on the Internet of Things* (19 November 2014) <*http://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20(updat%20%20%20.pdf*> p.5

[88] Eleanor Harding, 'Personal details in smartphone fitness apps 'sold to other firms': 20 most used products pass information to nearly 70 companies', *Daily Mail Australia* (online) (3 September 2013) <*http://www.dailymail.co.uk/news/article-2409486/Personal-details-smartphone-fitness-apps-sold-firms-20-used-products-pass-information-nearly-70-companies.html*>

[89] Emily Steel and April Dembosky, 'Health apps run into privacy snags', *Financial Times* (online) (1 September 2013) <*http://www.ft.com/intl/cms/s/0/b709cf4a-12dd-11e3-a05e-00144feabdc0.html*>

[90] Samuel Gibbs, 'Court sets legal precedent with evidence from Fitbit health tracker', *The Guardian* (online) (19 November 2014) <*http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker*>

[91] Marielle Moon, 'Fitbit tracking data comes up in another court case', *Engadget* (online) (28 June 2015) <*http://www.engadget.com/2015/06/28/fitbit-data-used-by-police/*>

[92] Peter Ker, 'Australian workers are starting to have their brains monitored in the workplace', *Sydney Morning Herald* (online) (3 July 2015) <*http://www.smh.com.au/business/mining-and-resources/australian-workers-are-starting-to-have-their-brains-monitored-in-the-workplace-20150701-gi292b.html*>

	be better to lead the big client pitch. • Wearable data is very valuable to health insurance companies, since they can track how active someone is, and the quality of their sleep. Some are offering free Fitbits and discounts to members as an incentive to sign up and stay fit[93].

Internet of Things and Affordability

In Scene Two, Johannes Babel was confronted with a number of confusing expense fluctuations. His health insurance varied hourly, and his health insurer seemed to give different family members different rates. It is likely that his insurance companies knew about Olivia's health kick and Johannes' fourth espresso, and adjusted their health premiums according to their revised 'riskiness'.

Jessica Rich, director of the Bureau for Consumer Protection at the FTC, explained that *"health data from [a person's] connected device, may be collected and then sold to data brokers and other companies [they do] not know exist... these companies could use [their] information to market other products and services to [them]; make decisions about [their] eligibility for credit, employment, or insurance; and share with yet other companies"*[94].

Internet of Things and Insurance

Insurance companies analyse large datasets to form accurate risk assessments. This is IoT's main benefit to the insurance sector. 'Usage-based Insurance' (**'UBI'**) refers to 'pay as you use' insurance pricing models where price is based on usage, behaviour and other relevant factors. Other factors may include fitness levels and diet, or the presence of home security systems.

A report by **BI Intelligence** lists some IoT use-cases in the insurance sector:

1. Car insurers using 'pay as/how you drive' pricing models;
2. Using IoT analytics to foresee and track severe weather conditions in real-time;
3. Encouraging consumers to adopt IoT devices that alleviate risk, like in-car drowsiness detectors or proximity sensors, or atmospheric sensors for impending storms; and
4. Home insurers using IoT devices like drones to survey damage after an event[95].

Case Study: Wearables, Smart Fridges and Insurance

APPENDIX 2 identifies some inferences from wearables and their sensors. The manufacturer and third parties could deduce how healthy someone is, how active someone is, whether they smoke, take recreational drugs or suffer from minor mental disorders. These inferences may influence

[93] Lucas Mearian, 'Insurance company now offers discounts -- if you let it track your Fitbit', *Computerworld* (online) (17 April 2015) <http://www.computerworld.com/article/2911594/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html>

[94] Dana Liebelson, 'Are Fitbit, Nike, and Garmin Planning to Sell Your Personal Fitness Data?', *Mother Jones* (online) (31 January 2014) <http://www.motherjones.com/politics/2014/01/are-fitbit-nike-and-garmin-selling-your-personal-fitness-data>

[95] John Greenough, 'From fitness trackers to drones, how the Internet of Things is transforming the insurance industry' *Business Insider Australia* (online) (7 July 2015) <http://www.businessinsider.com.au/how-the-internet-of-things-is-transforming-the-insurance-industry-2015-7?r=US>

the risk profile of a member. Even in Australia, AIA Insurance offers discounts to consumers who share their Fitbit data, and Medibank offers FlyBuy points for taking 10,000 steps every day[96]. The Connected Home has similar value to insurers.

Smart fridges of the future may record what consumers eat and how much of it. If someone suffers from cholesterol, but still insists on full-fat butter, their health insurance premium may fluctuate. Alternatively, if the grocery lists are full of greens, the member may see discounts on their insurance bill.

Case Study: Connected Cars and Car Insurance

Some of the features of a connected car, including driving statistics and eye movements, can be logged by the manufacturer and sold to third parties such as insurance companies and government bodies. These are some of the benefits for *insurers*:

1. **Reliable, real-time data on driving habits** such as braking, acceleration, speeding, time and distance driven, weather conditions and other driving habits. These allow insurers to set prices based on driving behaviour.
2. **Affirming or dismissing claims**. If a car's dashboard tracks eye movements at the time of an accident, and the driver was speeding, hands were off the wheel, or they were driving negligently, the insurer will know about it.
3. **Assessing damage**. Connected cars will be full of sensors. These sensors not only act as a way to track maintenance and faults, but can also assess damage. For instance, if 'sensors indicate 70% damage', the insurer may assess it as a write-off.

Some Australian insurers offer discounts for using their smartphone app[97]. These apps may track location (and so speed, distance and time travelled).

Internet of Things and Creditworthiness

By now the IoT formula is clear – more devices collecting more data means more of consumers' personal information being sold to third parties. IoT data can also determine credit scores and product consumption patterns. At a 2013 FTC IoT Conference, **Scott Peppet** of the University of Colorado law school said *"I can paint an incredibly detailed and rich picture of who you are based on your Fitbit data... That data is so high quality that I can do things like price insurance premiums or I could probably evaluate your credit score incredibly accurately"*[98].

[96] Kelsey Munro, 'Data collection: Wearable fitness device information tracking your life' *Sydney Morning Herald* (online) (18 April 2015) <http://www.smh.com.au/digital-life/digital-life-news/data-collection-wearable-fitness-device-information-tracking-your-life-20150416-1mmzbq.html>
[97] AAMI, *AAMI Safe Driver App* <https://www.aami.com.au/car-insurance/safe-driver-smartphone-app.html>
[98] Thorin Klosowski, 'Lots of Health Apps Are Selling Your Data. Here's Why' *Lifehacker* (9 May 2014) <http://lifehacker.com/lots-of-health-apps-are-selling-your-data-heres-why-1574001899>

Internet of Things and Price Discrimination

Price discrimination does exist innocently, and most users accept it. Take, for example, concession or pensioner discounts, early-bird prices on flights and loyalty or bulk-buy discounts. More 'sinister' forms of price discrimination are used to explore consumer demand, steer customers into different products, create targeted advertising and set prices based on a number of personal factors like behaviour, preferences and income bracket. Data-based price discrimination was identified as such a big problem that it formed the basis for a White House paper on big data and differential pricing in February 2015 and an FTC Workshop on Big Data as a tool for exclusion in September 2014.

Manufacturers and service providers can share IoT data with third parties, allowing them to 'price discriminate' in real-time. For example, if someone is identified as an Apple customer, retailers may charge them a premium on Apple accessories. If someone's online calendar shows that they have a commitment in Melbourne coming up, they may be willing to pay more for flights to Melbourne because they *need* to be there, regardless of price. **Patrick Fair**, partner at law firm Baker & McKenzie, has been a vocal player in Australian IoT discussions, and has expressed concern over this consumer issue. In a presentation to the Communications Alliance IoT Think Tank recently, Mr Fair described the "major imbalance in bargaining power in transactions" between consumers and IoT vendors and service providers.

The 'Freemium' Business Model

IoT will proliferate 'freemium' business models, as vendors (and our own former Communications Minister, **Malcolm Turnbull**) begin to realise that *"the value of the information produced by all of these connected things will soon start to outweigh the small cost of producing the sensors that gather that data, and possibly even the products that they're embedded inside"*[99]. UNSW academic **Kate Carruthers** noted that *"connected devices are transformed from a single-purchase product into a service that generates recurring income... value is not in the devices, but in new services related to the devices"*[100]. IoT will become an enabler of the 'freemium' business model – vendors will give out discounted or free goods and services, banking on all of the valuable data that will be collected afterwards. It is vital that consumers are aware of the implications of these emerging business models, so as to create a market for ethical or privacy-focused services.

Home Management

In the above scenario, we saw Johannes manage the Babel home from his tablet, assisted by the fictional Babel home hub platform, '*ME-ternity*'. The future Connected Home will have data points and sensors everywhere – every outlet, every solar panel, every 'smart thing'. Energy and water sensors will give a detailed breakdown of consumption. According to recent **iControl** study, heating and cooling account for 48% of energy consumption in the average US home[101]. **McKinsey** predicts that

[99] Malcolm Turnbull, opening address for the AIIA Summit: *Navigating the Internet of Things* (26 March 2015) <*https://www.youtube.com/watch?v=t8lZl7hGCFI&index=3&list=PLpK9LWXfxsoo4ZUN3fgVt2CYswyEzv21f*>

[100] Kate Carruthers, 'How the internet of things changes everything: The next stage of digital revolution' (2014) 2(4) *Australian Journal of Telecommunications and the Digital Economy* 69, 74.

[101] iControl, Networks, *2015 State of the Smart Home Report* (2015) <*http://www.icontrol.com/wp-content/uploads/2015/06/Smart_Home_Report_2015.pdf*> p.3

by 2025, 'chore automation' will cut 100 hours of labour per household and nearly $135 billion in savings, followed by an energy consumption saving of between $50 - $110 billion[102].

Smart thermometers, lights and air conditioners may ensure that energy is consumed efficiently. When no one is home, the Connected Home will use power conservatively. Smart thermostats use sensors, real-time weather forecasts, and daily domestic activity to reduce monthly energy usage and keep occupants comfortable without their input. This may save users money on their utility bills. Smart washing machines and dishwashers can delay wash cycles for off-peak periods. All of this can be managed with home/smartphone programs like SmartThings and CSIRO's Eddy smart home energy app, allowing consumers to control their home from anywhere.

Greater Cost of Connectivity?

Cost of data becomes another consumer issue for the connected consumer. If each device needs *internet* connectivity, does this mean a new SIM card and data plan for each device? Are they all able to connect to the Wi-Fi network? Do consumers need to worry about upgrading their broadband?

The short answer is no. The IoT market and existing connectivity standards make cost of data a minor issue for most consumers. There are a few reasons for this. Firstly, IoT devices generally use *very* small amounts of data. Even though they emit data constantly, each data packet is only a few kilobytes[103]. Secondly, most mobile IoT devices don't use *internet* connectivity. Most wearables synchronise using Bluetooth or NFC technology.

Elderly Consumers and Consumers with Disabilities

Internet of Things and the Elderly

The elderly will be one of the biggest beneficiaries of wearable 'things'. A recent **iControl** study found that 72% of consumers aged 25-34 and 74% of parents would 'sleep better at night' if their parents or grandparents had smart home technology[104]. Connected thermometers (in the home or on the person) can alert authorities if elderly residents are experiencing dangerous levels of heat or cold. It is no secret that Australia faces an ageing population challenge – one that can be mitigated with IoT solutions.

Internet of Things and Persons with Disabilities

Some accessibility challenges faced by elderly consumers are also faced by consumers with disabilities. Some disabilities that may hinder accessibility include mobility-related disabilities, chronic illnesses and sensory impairment. A 2012 **ABS** study found that 4.2 million or 18.5% of Australians had a disability[105].

---

[102] McKinsey&Company *The Internet of Things: Sizing up the opportunity* (Full Report, June 2015) <*http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity*> p.8

[103] One gigabyte of data equals one million kilobytes. Most Australian home broadband plans offer between 50GB per month to 'unlimited'.

[104] iControl, Networks, *2015 State of the Smart Home Report* (2015) <*http://www.icontrol.com/wp-content/uploads/2015/06/Smart_Home_Report_2015.pdf*>

[105] ABS, *Disability, Ageing and Carers, Australia: Summary of Findings, 2012* (online) (13 November 2013) <*http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/A813E50F4C45A338CA257C21000E4F36?opendocument*>

IoT can bring new opportunities for consumers with disabilities. Wearables can enhance day-to-day safety via remote monitoring and embedded alarm features. Fitness trackers collect essential physiological data and enhance illness detection and management. For example, buddi offers wearable, monitored emergency alarm systems with built in heart rate monitor, GPS, location alerts, and 'fall' sensors.

Table 6 – IoT and accessibility opportunities. Source: G3ict

Type of Disability	Examples of Useful Functionalities Enabled by IoT
Physical and Dexterity	Remote support and services at home Speech activated devices Automated accessibility functions in public spaces
Visual	Interpretation of user environment for way finding Near field automation Speech activated devices which communicate with speech output
Hearing	Captioning in glasses delivered by beacons Visual cues about status of home devices on mobile device
Cognitive	Localisation and orientation Automated reminders Programmable safety processes

IoT also has the innovative potential for user input, user interface and device interaction. These include gesture control, speech input, text-to-speech, eye tracking and innovative product designs, like cubes that act as 'remote controls' for the Connected Home or Braille smartwatches. These innovative methods of interacting with our devices could dramatically improve the lives of some users, who will be able to interact with technology like never before.

Scene Three: Into the Wild

1:09pm 6 July 2020 *– Olivia Babel decides that it's time for lunch. She steps away from her desk, the monitor automatically locking. The* ***'Ego-Centro'*** *shopping mall across the road is a good opportunity to do some shopping. She brings up her kitchen inventory on her smartphone, checking to see what they need. As she steps through the automatic doors, the Bluetooth beacons detect her smartphone and activity tracker. She also connects to the Ego-Centro free Wi-Fi, after accepting the terms and conditions she didn't read. As a regular customer, Ego-Centro adds this visit to her ongoing user profile.*

The Wi-Fi and Bluetooth sensors detect her proximity to the food court. Her Ego-Centro marketing profile is under the demographic 'fit mum' and they know of her regular healthy preferences. As she nears, the Ego-Centro app on her smartwatch sends her a notification telling her of the specials on healthy meals. She dismisses the notification and checks her diet app (synchronised with her fitness tracker) – she has been in caloric deficit all week, so decides to indulge. She turns to ***'Self-Patty Burgers & Grill'*** *and purchases a burger, using her NFC-enabled smartwatch to pay. Her diet app, Ego-Centro app and fitness app all try to figure this out – is she stressed? Has she taken in fewer calories this morning so is extra hungry? Later that week, a data broker will sell this data to 'Self-Patty Burgers & Grill' so that they can figure out when Olivia might indulge again.*

After lunch, she steps into her favourite department store, ***'Me-Tail Therapy'****. The Me-Tail Therapy*

*app talks to the Wi-Fi, Bluetooth beacons and sensors to update her user profile, including recent purchases and searches. It's her daughter Evey's birthday next week and Evey's social media use seems to indicate that she might like the **'Barb-bb-me'** Wi-Fi doll. As Olivia walks past an interactive screen, it beams an advertisement for this product. Olivia doesn't notice. The Me-Tail eye movement tracker on the panel noted this, and ensures that Barb-bb-me isn't charged for the advertisement in this instance.*

*A pair of shoes catches her eye. She stops, picks them up, checks the price tag, puts them back down. Disappointed, she moves on down the aisle. The RFID tag in the shoes, sensors and eye trackers sensed her interest. Me-Tail checks her creditworthiness with data from the Babel **'Me-Money-Me-Problems'** service and knows she's a suitable candidate. It sends her a 15% discount on her smartwatch seconds later. She succumbs, puts the shoes in a Me-Tail smart bag. As she leaves the store, the exit sensors read the RFID tag on the shoes, find her Me-Tail profile and charge her the discounted price as she walks out. No awkward checkout conversations.*

Back at home; Johannes gets another notification on his smart watch. Evey has left the school grounds. He gets up visibly agitated. "ME-ternity, Jon to Liv, SMS, Evey is skipping school again – please take care of it", he bellows. Olivia gets the notification on her smartwatch and reads the SMS on the smartphone. She is agitated and her heart rate spikes. She tells the office that there's an emergency and rushes to her Connected Car. She turns it on with her fingerprint and brings up Evey's smartwatch coordinates on the dashboard GPS. The location is unreliable – Evey must have her GPS turned off, relying instead on less accurate cell towers. Olivia drives to Evey's general vicinity – turning corners sharply, accelerating quickly and going well beyond the speed limit. Warnings trigger, she dismisses them. Her in-built digital radio plays an ad for longer lasting sex.

Eye trackers on the dashboard sense that her eyes aren't staying in front and that she just went through her third red light. Her car notifies the closest police patrol car, which quickly stops her. She explains that she has lost Evey, and gives the police a description. They inform their local Smart City control centre. An analyst scans the nearby CCTV cameras, sensors, public Wi-Fi hotspots and other people's smartphone sensors, trying to spot Evey or her smartwatch. Several sensors show that she just walked into a local cafe. Public CCTV footage and facial recognition software confirm that it's her. The analyst notifies a police officer, who is dispatched to collect her.

After this ordeal, Olivia finally returns to her desk. Her activity tracker has detected high levels of stress and adrenaline. It asks her if she's okay, she confirms. Some chamomile tea might help. Her local cafe sends a promotional code to her smartwatch.

Internet of Things and Consumerism

A lot has happened in the above scenario. On a simple lunchtime trip to the shopping mall, Olivia Babel interacted with a number of modern trends in consumerism – data analytics, real-time personalised marketing, interactive advertisements, customer tracking, customer profiling and automatic checkout. **The Alexandra Institute's** 2011 IoT comic book depicts some of these, extracted in **APPENDIX 3**.

Internet of Things and making Purchases

The Internet and mobility has revolutionised how consumers make purchases. Connected and smart 'things' will drive this revolution in several key ways:

1. **Personal inventory management** refers to the ability to check, in real-time, how much of something is in stock. In Scene One, this was the Babel's smart fridge and the limited almond milk supply, and in Scene Three this was Olivia remotely checking her fridge's contents. As appliances, clothing and other items become 'connected', personal inventory management will become much easier.
2. IoT will introduce **new, novel ways to make purchases**. One of the best examples recently released on the market is the Amazon Dash Button. The concept is simple – physical 'buy' buttons that can be attached to things. When pressed, they order more of that product from Amazon or other vendors.
3. **Autonomous and predictive purchasing** is an emerging area of consumerism. Once a device or service recognises a user's purchasing patterns, it can autonomously make purchases, or recommend certain products. When paired with personal inventory management, it can be pre-set to make purchases of items that are running low – such as almond milk. Amazon is also working on Amazon Dash Replenishment Service (DRS). This is a service that detects when a specific item is running low and orders more. This service can either be built in to an appliance (such as a sensor in an espresso machine) or existing services can be synchronised to Amazon's DRS.
4. **Embedding wireless tags in products or packaging** will become more commonplace. This offers benefits for both the retailer and consumer. Including sensors in clothing allows vendors and consumers to manage their wardrobe digitally and even be notified of wear and tear. **Estimote** is one of many companies harnessing the convenience of Bluetooth beacon and smartphone integration for this purpose.
5. Connected devices will be **harder to counterfeit and easier to authenticate**, ensuring consumers know that they are buying legitimate products. This also has protects the intellectual property of the owners of the trademark or design in a product.

Internet of Things, Data Analytics and Marketing

Personalised advertising and data brokerage is a multi-billion dollar industry. It is not a new concept, but IoT does set a new bar – more connected 'things' means more personal data is shared with more third parties – with one key purpose being marketing. According to the Harvard Business Review:

> *"Smart, connected products allow companies to form new kinds of relationships with customers... they gain new insights into how products create value for customers, allowing better positioning of offerings and more effective communication of product value to customers"*[106]

In Scene Three, when Olivia walked into the *Ego-Centro* shopping centre and favourite retailer *Me-Tail Therapy*, the vendors knew more about her than she knew about them. Before she walked in,

[106] Michael E Porter, 'How Smart, Connected Products Are Transforming Competition' *Harvard Business Review* (online) (November 2014) <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition>

they did their homework on her, her life, her purchases and the type of customer she is. They even did their homework on others, anticipating Evey's upcoming birthday, finding out what Evey liked and then sending Olivia useful suggestions or promotional advertising.

Internet of Things and how Consumers Shop

In Olivia's short shopping trip, she was exposed to a number of 'futuristic' technologies, many of which are used *today*.

Real-Time, Personalised Promotions

Once a retailer has profiled a consumer, they can use the tools at their disposal to deliver promotions, information and advertisements in real-time. Smartphones and smart watches can connect to various sensors or networks around the store. Customers can 'interact' with items and allow retailers to 'push' out notifications or promotions. For example, a consumer that has been Googling Singapore a lot may expect to receive a holiday promotion to Singapore on their smartwatch next time they walk past a travel agent.

Figure 21 – Eye-tracking meat.
Source: Business Insider

Similarly, technology allows new and innovative methods of advertising. When Olivia walked past an advertising panel, proximity sensors displayed personalised, digital signage when she was near. Eye-trackers detected her attention to the ad. Eye-trackers track where and how long someone's eyes look at certain areas of a product or advertisement. **Figures 21** and **22** are examples of where most consumers look at an item, and for how long[107].

Digital Assistance

IoT makes it easier to get product information. QR Codes already allow customers to bring up product information on their smartphone, but new IoT developments like Bluetooth beacons and Smart Glass allow consumers to simply *touch* an item or display and have information brought up on their smartphone, using their body as the 'conductor'.

Figure 22 – Eye-tracking advertising.
Source: Business Insider

Digital checkout is the natural progression from self-checkout. In Scene Three, Olivia enjoyed the ease of walking out of the store without a checkout

[107] Gus Lubin and Hayley Hudson, '26 Eye-Tracking Heatmaps Reveal Where People Really Look', *Business Insider Australia* (online) (23 July 2014) <http://www.businessinsider.com.au/eye-tracking-heatmaps-2014-7>

counter. RFID tags can scan products remotely, from metres away. Detected items can be paid for wirelessly with a smartwatch or an app that is linked to a customer account.

Customer Service

According to **Paul Weichselbaum** of the Harvard Business Review, the company-customer relationship is changing from the traditional 'fire and forget' model (where post-sale customer service is for warranty or product support only) to a more 'continuous, open-ended experience' with ongoing software updates, customer service and dynamic, real-time user profiles[108]. In other words, the 'transaction' is ongoing.

Figure 23 – IoT uses in retail. Source: McKinsey

In March 2015, **Altimeter** released a report examining how IoT can be used to build better customer relationships. It identified five 'use cases' of how IoT and sensors can be used to enhance customer experience: context-based awards, improved decision-making, facilitation of exchange, proactive, real-time service and opportunity for innovation[109].

Customer Tracking

Wireless sensors and CCTV footage can assist retailers determine which items or marketing are most popular and where customers remain the longest. According to the **Harvard Business Review**:

> *"You can know when customers enter your store, how long they are there, what products they look at, and for how long. When they buy something, you can know how long that item had been on the shelf and whether that shelf is in an area of things that usually sell fast or slowly. And*

[108] Paul Weichselbaum, 'The Internet of Things Changes the Company-Customer Relationship' *Harvard Business Review* (online) (29 June 2015) <https://hbr.org/2015/06/the-internet-of-things-changes-the-company-customer-relationship>

[109] Altimeter Group, *Customer Experience in the Internet of Things: Five Ways Brands Can Use Sensors to Build Better Customer Relationships* (March 2015) <http://boletines.prisadigital.com/Customer-Experience-in-the-Internet-of-Things-Altimeter-Group.pdf> p. 6

then you can view that data by shoppers' age, gender, average spend, brand loyalty, and so on"[110].

Internet of Things and Children

In Scene Three, Johannes and Olivia were able to track their missing daughter Evey by using her wearable device and with the aid of public sensory networks.

There are dozens of devices on the market that children can wear and use as smart watches. Many include a GPS, which allows remote monitoring and tracking. GPS-connected activity trackers can potentially reveal location, heart rate and other information in real time to concerned parents.

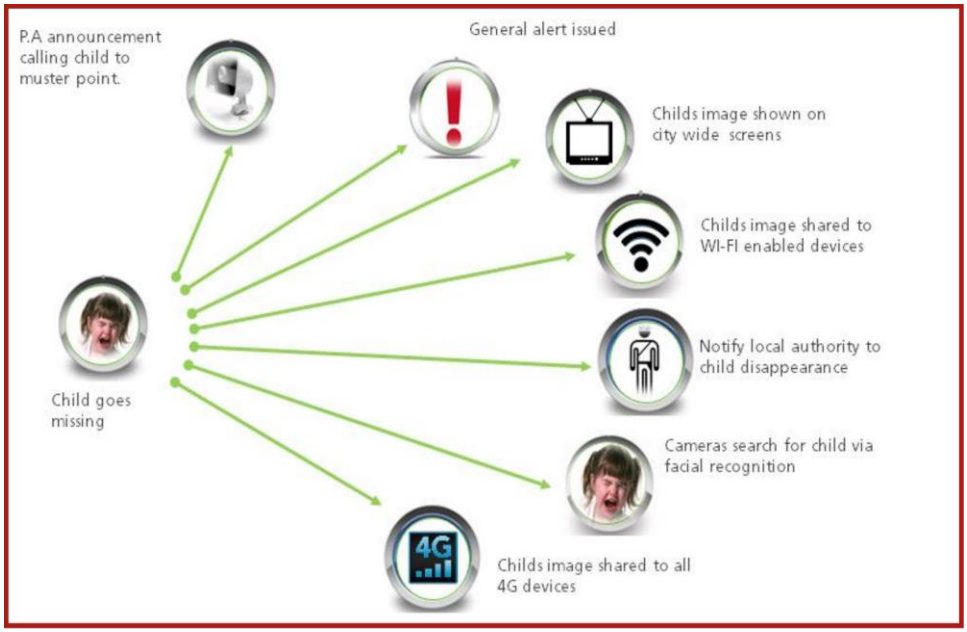


Figure 24 – IoT and lost children. Source: Oakton Applications

[110] Ric Merrifield, 'The Internet of Things Is Changing How We Manage Customer Relationships' *Harvard Business Review* (online) (5 June 2015) <*https://hbr.org/2015/06/the-internet-of-things-is-changing-how-we-manage-customer-relationships*>

Internet of Things and Privacy

"In the not-too-distant future, many, if not most, aspects of our everyday lives will be digitally observed and stored. That data trove will contain a wealth of revealing information that, when patched together, will present a deeply personal and startlingly complete picture of each of us."[111]

– **Edith Ramirez**, chair of the FTC

In 1970, **Newsweek** produced a cover with the tagline 'Is Privacy Dead?' (**Figure 25**) and an associated article entitled 'The Assault on Privacy'[112]. This 'slogan' is arguably more relevant in the digital age, but this image does serve as a reminder that *most* new technology is often met with fear, eventually accepted and then blended seamlessly into daily life. It is therefore likely that IoT will – ultimately – be met with the same reception.

IoT has been described as *"the greatest mass surveillance infrastructure ever"*[113] where information is *"bought, bartered traded and sold"*[114]. According to **US Senator Ed Markey**, *"Consumers' most sensitive information is collected and turned into dossiers that are pure gold in the hands of marketers and pitchmen"*[115]. **Vivek Wadhwa** thinks IoT has 'gone too far', writing that *"cameras are already recording our every move in city streets, in office buildings and in shopping malls. Our newly talkative devices will keep track of everything we do, and our cars will know everywhere we have been. Privacy will be dead, even within our homes"*[116]. **Jon Lawrence** of Electronic Frontiers Australia describes wearables "opt-in, ubiquitous, always-on surveillance"[117].

Figure 25 - Is privacy dead?
Source: The Daily Beast

[111] Easton, 'The Internet Of Things (IoT): Challenges And Benefits' *WT VOX* (online) (16 February 2015) <*https://wtvox.com/2015/02/the-internet-of-things-iot-challenges-and-benefits/*>
[112] Reproduced in The Daily Beast, *Is Privacy Dead?* (online) (11 June 2013) <*http://www.thedailybeast.com/articles/2013/06/11/is-privacy-dead.html*>
[113] Julia Powles, 'Internet of things: the greatest mass surveillance infrastructure ever?' *The Guardian* (online) (16 July 2015) <*http://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance*>
[114] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (White House report, May 2014) <*https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf*> p.50
[115] 'In the Privacy of Your Own Home' *Consumer Reports Magazine* (June 2015) 24-30, 26.
p.26
[116] Vivek Wadhwa, 'When your scale conspires with your fridge, the Internet of Things will have gone too far', *The Age* (online) (14 July 2015) <*http://www.theage.com.au/comment/when-your-scale-conspires-with-your-fridge-the-internet-of-things-will-have-gone-too-far-20150713-gibl3e*>
[117] Interview with Jon Lawrence, Electronic Frontiers Australia (via email, 7 August 2015)

Internet of Things and Consumer Privacy – In a Nutshell

This report will focus on the implications of IoT *specifically* on privacy *in general*. Privacy is made up of multiple elements, including ***personal privacy*** and ***information privacy***. IoT generally has its impact on *information privacy*, but specific 'things' like drones or embedded cameras may infringe on *personal privacy*. Conceptual discussions of privacy, such as 'what is privacy?' and 'what does privacy mean?', are omitted for lack of scope.

The Internet of Things raises five *unique* privacy concerns:

1. *Scale* – It creates more data collection points, since more 'things' collect data;
2. *Method* – It creates novel ways of collecting data, such as via sensors and smart things;
3. *Reach* – It penetrates more intimate areas of our lives, such as data on our bodies and inside our homes;
4. *Nature* – An advanced IoT ecosystem is designed to collect data covertly and 'in the background' via sensors and other digital tools, meaning that consumers may not be *aware* of the collection of personal information; and
5. *Depth* – The collective result of the above four concepts will be greater than the sum of the parts. As a result of greater scale, new methods, reach and nature of data collection and processing, IoT will have a synergistic effect on existing privacy concerns.

In summary: IoT brings little new to the privacy table – it merely *enables* greater volumes, new types, methods and subtleties of data collection. In other words, it takes existing privacy issues and multiplies them.

Internet of Things in the 'Taxonomy of Privacy Violations'

In 2006, **Daniel J. Solove** of George Washington University compiled a 'taxonomy' of privacy violations. In **APPENDIX 4**, this report lists the four broad types of privacy violation and sub-categories, and explains each in the context of IoT[118].

EU WP29 – Privacy and Data Protection Challenges in the Internet of Things

The European Union Article 29 Working Party (**"EU WP29"**) is a collection of 28 EU national data protection authorities formed for the 'protection of individuals with regard to the processing of personal data'.

In late 2014, the **EU WP29** released the 'Opinion on the Recent Developments on the Internet of Things', where it outlined 10 privacy and data protection challenges of IoT[119], listed below.

[118] Table compiled by the author, content reproduced from Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 478-91.

[119] European Union Article 29 Data Protection Working Party ('WP 29'), *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (Report, 16 September 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>

1. Ensuring users have *sufficient control*, as they often cannot review the data before its 'publication'.
2. *Automatic or default communication* without the user being aware and the difficulty in controlling the flow of data.
3. A *lack of awareness by individuals*, other than the user, of a device's enhanced capabilities and the quality of their consent.
4. The *insufficiency of classical consent mechanisms* and the need for new methods of consent.
5. The risk of *stakeholders processing data beyond the original specified purposes*, particularly in light of the advances in algorithms and analytics engines.
6. IoT devices' *ability to determine the habits, behaviours and daily activities* of individuals.
7. The limits on the *ability to remain anonymous* while using IoT devices or services.
8. The *vulnerability of devices to "re-identification attacks"* where users can be identified by an unauthorised party.
9. The risk of turning an everyday object into a *privacy and information security target*.
10. The battle between device battery efficiency and the security of communications resulting in a *lack of encrypted data flows*.

In addition to the four IoT-specific privacy risks identified earlier in Solove's 'Taxonomy of Privacy Issues', the EU WP29 identified two more IoT-specific privacy risks that deserve particular attention – the risk of re-identification and the insufficiency of traditional consent models for the collection of personal information.

Identification, De-Identification... Re-Identification?

All IoT goods and services that collect personal information must do so under the provider's privacy policy. Most privacy policies handle personal information in a similar manner – personal information is 'de-identified' and can be shared with third parties for a number of reasons, including research, marketing and promotion.

Example: The Life Cycle of Olivia Babel's Fitness Wearable Data

Olivia's fitness wearable collects health information. Olivia has 'agreed' for that data to be shared with third parties. The terms are likely to be similar to those of Fitbit, discussed in earlier sections of this report.

In Scene Three, her fitness wearable provider 'de-identified' Olivia's datasets (such as heart rate, steps taken etc) and sold it to her diet app provider. The diet app received datasets for 'user X' (Olivia). The diet app then collated that data with more 'de-identified' datasets from other sources (like purchases or Internet browsing history) and made some inferences – 'User X is quite active, she eats well, she likes health pages on social media, she is a mother etc'. This data is then shared again with other parties, such as her favourite store, *Me-Tail Therapy*. Using those inferences, and knowing Olivia's unique smartphone details, *Me-Tail Therapy* was able to offer her personalised advertising, without ever knowing who she was. Technically, all they had was several de-identified and anonymous datasets. The algorithms did the rest.

One of the biggest issues in digital privacy is the risk of 're-identification'. This involves collecting so much de-identified/anonymised data on a set of users that, with enough algorithmic work and enough cross-referencing, someone can identify with accuracy who that person is. It can be argued that with enough 'anonymous' datasets, demographics and a bit of context, someone can be re-identified.

For example, 1,000 anonymous datasets of heart rate data, by themselves, are hard to re-identify. However, when the fluctuations in heart rate are cross-reference with other datasets (time, location, gym visit time, etc.) the relationship between the two data sets can be identified and linked. This issue was addressed in a 2015 FTC Staff Report on the Internet of Things, including recent studies on the topic. Most stakeholders conceded that re-identification is possible, but the risk is 'very small'[120] and re-identification is a "technologically rigorous and expensive endeavour, with very limited success rates"[121]. A 2009 research group tried to re-identify a set of 15,000 patient records that were de-identified under US health privacy standards, with a success rate of 0.013%[122]. Therefore, while difficult, re-identification of de-identified data is certainly possible.

Protecting the Privacy of Australian Consumers

The Australian Information Privacy Framework

Information Privacy focuses on the security of personal information, governed by 13 'Australian Privacy Principles' (**"APPs"**), found in Schedule 1 of *Privacy Act 1988 (Cth)* (**"the Act"**) (**APPENDIX 5**). Similar state legislation governs personal information held by statutory bodies[123]. These APPs set out the requirements for the collection, use, disclosure, retention, handling, destruction and de-identification of 'Personal Information', defined under s6(1) of the Act as *"information or an opinion about an identified individual, or an individual who is reasonably identifiable"*.

Protecting 'Health Information'

Health Information Privacy is concerned with health and genetic information. This information is *'Sensitive Information'* under the Act[124], and some APPs place a higher standard on its collection and handling. *'Health information'* falls under *'sensitive information'*, and is to be treated under the higher standard. The definition is broad[125], and almost all commentators interviewed for this report agree that it falls under this definition.

---

[120] US Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, January 2015) <*https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*> p.37

[121] Ann Cavoukian and Khaled El Emam, *De-identification Protocols: Essential for Protecting Privacy* (Office of the Information and Privacy Commissioner, Canada, 25 June 2014) <*https://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identifcation_essential.pdf*>

[122] US Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, January 2015) <*https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*> p 38.

[123] *Privacy and Personal Information Protection Act 1998 (NSW); Information Privacy Act 2009 (Qld); Premier and Cabinet Circular No 12 (SA); Personal Information Protection Act 2004 (Tas); Information Privacy Act 2000 (Vic).*

[124] Definition of 'sensitive information' in *Privacy Act 1988 (Cth)* s 6(1)

[125] Definition of 'health information' in *Privacy Act 1988 (Cth)* s 6(1)

Where this becomes particularly interesting in the IoT context is the handling of wearable data – is this considered '*health information'*, and therefore handled at a higher standard than regular '*personal information'*? No Australian privacy commissioner, state or federal, has yet addressed this question. On face value, Connected Human data provides a lot of information about a user's health, and new methods of steganography assert that individual can be identified based on their unique heart rate waveform[126]. According to UNSW academic **David Vaile,** *"Health data is the most sensitive of personal information... Anyone expecting protection in the contract or from the regulators is dreaming"*[127]. This distinction between 'Personal Information' and 'Sensitive Information' will have major implications for how businesses are able to handle Connected Human data.

This report will conclude discussion on IoT and privacy with an excerpt from a paper by US law firm **Goodwin Procter**:

> *"[IoT] data may reveal an individual's identity, location, medical issues, religious or political preferences, financial information, family and friends, sexual orientation, favorite coffee shop, driving habits, whether [their] home's doors and windows are locked, and when [they are] not home. Put bluntly, we have always made noise as we interacted with the world around us, but soon that world will be much better equipped to listen and make sense of what it hears"*[128].

Consumer privacy will be one of, if not the most, important consumer issues to emerge from IoT.

Scene Four: Old Man Yells at Cloud

7:13pm 6 July 2020 *- The Babel family has had a long day. Tensions are high and they are all exhausted. George Clooney's voice can be heard coming from the smart fridge, offering a discount on espresso for the next half hour. They decide to give the Connected Home a rest for the day and enjoy a night out. As they leave the house, the sensors count each member as they walk out of the door. Consulting embedded sensors and their smartphones' GPS, the Babel home waits patiently until it knows that they have left. Once they are 50 metres down the road, their Connected Home activates the security system, turns on the activity sensors and cameras and locks all of the doors. It also enters power-saving mode, and switches off all appliances except for the Wi-Fi and security systems. Johannes and Olivia get a notification on their smart watches that the Babel home is secure.*

An hour later, as they sit at a restaurant, they get another notification – the smoke alarm is going off. Johannes steps away from the table and accesses the home security cameras. He can log in to view them, but can't control them. Alarmed, he excuses himself and makes his way home. He approaches his house's front door and waits for the home security system to let him in. It doesn't seem to sense his presence. He tries to open the door – it's still locked. He can see smoke coming from

[126] Lily Hay Newman, 'Hiding Data in a Heartbeat' *IEEE Spectrum* (online) (10 October 2013) <http://spectrum.ieee.org/tech-talk/biomedical/diagnostics/hiding-data-in-a-heartbeat>
[127] Kelsey Munro, 'Data collection: Wearable fitness device information tracking your life' *Sydney Morning Herald* (online) (18 April 2015) <http://www.smh.com.au/digital-life/digital-life-news/data-collection-wearable-fitness-device-information-tracking-your-life-20150416-1mmzbq.html>
[128] Gerard M Stegmaier and Britanie Hall, *T*he Internet of Things: The Future of Listening' *JD Supra Business Advisor* (online) (24 September 2014) <http://www.jdsupra.com/legalnews/the-internet-of-things-the-future-of-li-46154/>

the kitchen window. His security system isn't responding to his smart phone app commands. He now curses himself for not upgrading to the model with the fingerprint scanner. There are now two fire alarms going off – the fire brigade is alerted. He makes his way to the back of the house, climbing through a window panel that wasn't 'connected'. The smart toaster is belching smoke and the smart fridge screen is flashing. He unplugs the toaster from the electricity socket and disconnects the Wi-Fi. The appliances go lifeless. The fire brigade arrives.

Johannes and Olivia are astounded. The smart toaster, fridge and espresso machine all took on a life of their own. The ME-ternity connection logs show that someone had gained unauthorised access to their home network. That explained why he was locked out of the home – almost everything connected to the Wi-Fi was compromised. It gave Olivia chills that a 'hacker' was able to peer into her home and view her security cameras.

*Upon further investigation, the first device comprised was the **'Unlock-me-Home'** garage door sensor, bought online from an overseas store that stocked counterfeit 'Unlock-me-Home' devices. A legitimate 'Unlock-me-Home' garage door sensor was triple the price. The counterfeit was identical, but with unofficial software, preventing counterfeit detection. The software had not been updated for months. Johannes called 'Unlock-me-Home' Asia-Pacific, who told him that he did not have a legitimate version of the product. He then complained to NSW Fair Trading, his internet service provider and the ACCC. Desperate, he turned to his neighbour **Alexander**, a law student and intern for ACCAN. Alexander told him that consumer redress would be difficult, and next time, to be more informed about his Connected Home, Human and Habitat.*

Securing the Internet of Things

While threats to consumer privacy present ethical, social and financial risks, connected device security could *literally* mean life or death. **Mark Pesce**, academic, author and technologist said about IoT, *"there will be billions of connected devices and that's great, but that also means billions of new attack platforms"*[129]. **Peter Greenwood** had the following to say:

> *"Somebody far away will be able to turn on your oven when you're on vacation. Your lawnmower will be part of a botnet sending spam. The fridge of the future will offer to reorder your preferred groceries, because it's been scanning the barcodes on everything you put inside. That's great, until bad guys figure out how to read the barcodes off bottles of antiretroviral drugs and learn who has HIV"*[130].

The Babel family learnt this the hard way – their Connected Home was 'hacked' at one of the weakest links – a cheap, disposable, illegitimate and under-secured garage door sensor. The software was not updated regularly, and vulnerable to new exploits. Since this was connected to the rest of their network, the hacker was able to gain access to the remaining appliances, wreaking havoc.

[129] Interview with Mark Pesce, academic and technology adviser (in person, 26 May 2015)
[130] Keith Winstein, 'Introducing the 'right to eavesdrop on your things' *Politico* (online) (June 2015) <http://www.politico.com/agenda/story/2015/06/internet-of-things-privacy-concerns-000107>

A New Frontier for Security Challenges

As with privacy, IoT does not present any *new* issues, but instead adds scale and complexity to existing ones. As **Symantec** put it in their 2015 Internet Security Threat Report, *"[IoT] is not a new problem but an ongoing one"*[131]. That same report found that 52% of health apps did not even have a privacy policy in place and 20% sent out unencrypted data. **OpenDNS** lists three new security challenges: IoT presents new avenues for remote exploitation, the IoT infrastructure is beyond user or IT department's control, and there is a casual approach to IoT device management, meaning largely unmonitored or unpatched connected 'things'[132]. The **FTC** foresees the following security challenges: companies inexperienced with IoT software and standards, and millions of cheap, disposable 'things' that would cost far more to secure (especially continuously) than to manufacture[133]. They also foresee IoT creating more platforms for facilitating attacks on other systems and unprecedented safety risks (like hacking bio-mechanical devices)[134]. **Michael O'Brien** raises the issue of expectations – users cannot be expected to keep *every* device patched and up-to-date, and businesses cannot be expected to invest the resources to keep every 'disposable, lightweight' device secure[135]. Interconnectivity is another unique IoT security issue. More devices connected to a single network equals greater risk – if a single connected light bulb is compromised, the rest of the network could be accessed. In fact, Target US suffered one of the biggest data hacks in consumer history via their air conditioning unit[136].

IoT opens up new frontiers for security at the *thing* level. A **2014 HP analysis** of 10 popular Connected Home devices[137] found that 80% had poor password management, 70% lacked encryption and 60% were vulnerable to a range of exploits. Making matters worse, 90% of devices collected at least one piece of personal information. Ransomware will be more intrusive, as hackers could take Connected Home or appliances 'hostage' unless a 'ransom' is paid. **The Australian** recently described how a fridge could one day hold personal information to ransom[138] and **Symantec** warns of the

---

[131] Symantec, *Internet Security Threat Report* (White paper, Volume 20, April 2015) <*https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf*> p.8

[132] OpenDNS, *The 2015 Internet of Things in the Enterprise Report: Executive Summary* (2015) <*http://info.opendns.com/rs/033-OMP-861/images/OpenDNS-2015-IoT-Executive-Summary.pdf*> p.4

[133] US Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, January 2015) <*https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*> p 13

[134] Ibid p.10

[135] Michael O Brien, 'The Internet of Things and the Inevitable Collision with Products Liability PART 2: One Step Closer', *Product Liability Advocate* (online) (15 July 2015) <*http://www.productliabilityadvocate.com/2015/07/the-internet-of-things-and-the-inevitable-collision-with-products-liability-part-2-one-step-closer/*>

[136] 'Target Hackers May Have Gotten In Through the Air Conditioner' *Infosecurity Magazine* (online) (6 February 2014) <*http://www.infosecurity-magazine.com/news/target-hackers-may-have-gotten-in-through-the-air/*>

[137] HP, *Internet of Things Research Study* (Research report, 2014) <*http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf*>

[138] Tony Allen-Mills, 'First they hacked your car, next they'll come for your fridge' *The Australian* (online) (26 July 2015) <*http://www.theaustralian.com.au/news/world/first-they-hacked-your-car-next-theyll-come-for-your-fridge/story-fnb64oi6-1227457423110*>

growing ransomware threat to smartwatches, particularly Android Wear devices[139]. On the other hand, technology journalist **Stilgherrian** does not see a 'Refrigergeddon' happening any time soon[140].

Securing the IoT also raises non-technical issues. **Herman Yau** says that businesses will need to offer *"security in a way that does not affect the overall user experience and also in a cost-effective manner"*[141]. **Stephen Wilson** of Constellation Research raised concerns about the challenges of managing the security of so many domestic devices, stating on social media *"I really don't want to be [system administrator] for my effing stove!"*[142]. This is one of the challenges of IoT developers.

Unlike most existing computing, IoT 'hacks' could prove fatal or catastrophic[143]. For instance, hacking someone's connected car or pacemaker could kill them, and hacking an oil rig, smart grid or major infrastructure via a tiny, connected 'thing' could prove disastrous.

Case Study: Hacking the Connected Car

Hacking the Connected Car has been one of the most publicised IoT safety issues. Recently, two security researchers were able to gain remote access to a Jeep via the mobile phone connection while a person was driving it[144], prompting a mass recall[145]. Other researchers examined several car manufacturers and documented their results in a table, finding different vulnerabilities in different manufacturers[146]. A Tesla Model S was also hacked, but a patch was quickly released[147] – a good example of efficient reactive security. Security researcher **Anyck Turgeon** cites a number of studies that reveal that nearly 100% of modern cars are hackable, and that hackers can gain access to almost every part of the car's operative mechanics and all the data being collected by the car, including personal information and registration, geospatial data (like location and speed) and private conversations (like telephone calls via the Bluetooth input or GPS commands)[148].

It is important to remember that these scenarios were planned, and the researchers set about targeting a specific car and were prepared for the attack. According to **Techguide** editor **Stephen**

---

[139] Symantec, 'The dawn of ransomwear: How ransomware could move to wearable devices' *Symantec Official Blog* (6 August 2015) <http://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices>

[140] Stilgherrian, 'All aboard the internet of things infosec hype train' *ZDNet* (online) (11 December 2014) <http://www.zdnet.com/article/all-aboard-the-internet-of-things-infosec-hype-train/>

[141] Charlie Osborne, 'The challenges of securing your smart home' *ZDNet Australia* (online) (21 July 2015) <http://www.zdnet.com/article/the-challenges-of-securing-your-smart-home/>

[142] Twitter, Steve Wilson (@Steve_Lockstep) <https://twitter.com/Steve_Lockstep/status/615945978231816192>

[143] Alexander Howard, 'Digitizing The World Through The Internet of Things Could Be Worth $11 Trillion By 2025', *Huffington Post* (online) (26 June 2015) <http://www.huffingtonpost.com/2015/06/26/internet-of-things_n_7664930.html>

[144] Danny Yadron and Mike Spector, 'Hackers show they can take control of moving Jeep Cherokee' *The Australian* (online) (22 July 2015) <http://www.theaustralian.com.au/business/technology/hackers-show-they-can-take-control-of-moving-jeep-cherokee/story-e6frgakx-1227452097431>

[145] Kate Knibbs, 'Chrysler Recalls 1.4 Million Cars For Being Easily Hackable', *Gizmodo Australia* (25 July 2015) <http://www.gizmodo.com.au/2015/07/chrysler-recalls-14-million-cars-for-being-easily-hackable/>

[146] Andy Greenberg, 'How Hackable Is Your Car? Consult This Handy Chart' *Wired* (online) (6 August 2014) <http://www.wired.com/2014/08/car-hacking-chart/>

[147] Kim Zetter, 'Researchers Hacked a Model S, But Tesla's Already Released a Patch', *Wired* (online) (6 August 2015) <http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/>

[148] Anyck Turgeon, '100% Cars Now Hackable, 50%+ Transmit Data & 65,000 Land Rover Bugged' *Linkedin Pulse* (15 July 2015) <https://www.linkedin.com/pulse/100-cars-hackable-50-transmit-data-65000-land-rover-anyck>

Fenech, consumers shouldn't be too worried about this: *"While the danger of a car being hacked is serious – you certainly shouldn't be losing sleep over it... a car being hijacked remotely and then controlled by a hacker is not impossible but highly improbable"*[149].

Figure 26 – Connected Car threats. Source: Fairfax

Case Study: Hacking the Connected Human

Hacking the Connected Human is arguably the most concerning of IoT security issues. Security researchers have already been able to compromise connected infusion pumps[150], pacemakers and defibrillators[151]. Tinkering with these devices could allow a malicious hacker to deliver lethal doses of drugs to a patient or disable life-supporting technology. Former US Vice President **Dick Cheney** famously disabled the wireless capabilities of his heart implant for fear of malicious hackers[152]. US security firm **IDD** predicted the first murder by 'hacked internet-connected device' would be by end of 2014[153]. In Symantec's 2015 security trend report, **Axel Wirth** listed some reasons why wearables are more vulnerable to attack than other IoT devices: they have a long-useful battery life, the high regulation means that availability of upgrades or security patches is delayed, they are used 24x7 and the logistical difficulty of removing malware from many devices at once[154].

---

[149] Stephen Fenech, 'Should you be worried about your car getting hacked?' *Tech Guide* (online) (24 July 2015) <http://www.techguide.com.au/blog/should-you-be-worried-about-your-car-getting-hacked/>

[150] Jeremy Hsu, 'Feds Probe Cybersecurity Dangers in Medical Devices', *IEEE Spectrum* (online) (27 October 2014) <http://spectrum.ieee.org/tech-talk/biomedical/devices/feds-probe-cybersecurity-dangers-in-medical-devices>

[151] Barnaby J Feder, 'A Heart Device Is Found Vulnerable to Hacker Attacks' *The New York Times* (online) (12 March 2008) <http://www.nytimes.com/2008/03/12/business/12heart-web.html>

[152] Andrea Peterson, 'Yes, terrorists could have hacked Dick Cheney's heart' *The Washington Post* (online) (21 October 2013) <https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/>

[153] Paul Peachey, 'Cyber crime: First online murder will happen by end of year, warns US firm' *The Independent UK* (online) (5 October 2014) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774955.html>

[154] Symantec, *Internet Security Threat Report* (White paper, Volume 20, April 2015) <https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf> p 29.

Securing the IoT creates new challenges, enhances existing ones and creates many, *many* new opportunities for innovation. Without effective security precautions, consumers will be placed into an IoT 'Sword of Damocles' situation. Consumer awareness, security by design and ongoing, effective patching will protect the integrity of consumer IoT ecosystems and likely determine who succeeds and fails in an environment where trust is key.

Internet of Things: Choice, Control and Opting Out

The Babel family of 2020 embraced IoT to their benefit. This may not be the ideal situation for all consumers, and a big part of consumer choice, control and empowerment is the ability to 'say no' and 'opt out' of a connected world. Will this be possible in a (more) connected world?

Opting Out of Connected Products

A few years ago, non-smart phones, cars and appliances were common. Today, it is becoming increasingly difficult to avoid them, with almost every manufacturer releasing connected 'things' as an industry standard. For example, it is difficult to find cars without any connected parts or onboard computers, and replacing or repairing a 'dumb' phone is becoming very uncommon. Connectedness is a consumer state that is hard to avoid.

Social Exclusion

As new technology is adopted widely and accepted into the mainstream, those without smart 'things' may experience social exclusion or discrimination as connected 'things' become the norm. This is a current issue for those without social media, email or smartphones, as they are often excluded from some social situations, events or unable to meet productivity expectations. The Guardian's **Mark Honigsbaum** raises a more novel consumer issue – social discrimination based on fitness levels. If wearables become so prevalent that they create a 'quantified self' culture, those that do not track their progress or share it with others may not *"meet norms for appropriate body weight, good health or physical activity, [and] will be labelled deviants or somehow made to feel inadequate"*[155].

Controlling and Opting Out of Data Collection

Eventually, the data *collected* from devices will become more valuable than the *sale* of devices (if not already the case). Unless there is clear and sufficient consumer demand for 'opt-out' choices, manufacturers may choose to deny consumers the ability to exclude themselves from some or all data collection. At an individual level, consumers should be allowed to 'pick and choose' which features to enable and disable. For example, the ability to allow a smart fridge to use weight sensors, but not scan the barcodes of food products. At a public level, opting out of a Connected Habitat is far more difficult – sensors embedded into public spaces, facial recognition CCTV cameras and more may be impossible to avoid. Connected Habitats will present new domains of ethical, privacy and consent concern.

Internet of Things and Consumer Protection

The Babel family experienced a lot of grief from a tiny, cheap device. Their grief did not end there – there were practical, regulatory and legal hurdles to seeking redress for their faulty connected 'thing'. First, the manufacturer refused to help because it wasn't a legitimate version of their product. Then

[155] Mark Honigsbaum, 'Fitbit is the start of a revolution in digital health, but is it good for us?', *The Guardian* (online) (21 June 2015) <http://www.theguardian.com/commentisfree/2015/jun/21/fitbit-digital-health-revolution>

efforts under consumer protection laws failed. Even if they pursued the manufacturer directly, there are huge practical considerations like cost and geographical or jurisdictional barriers. Is the product even considered 'faulty' if hacked or unreasonably hackable? What if the software 'fault' causes an injury or damage to property, not just an inconvenience?

The OECD's Digital Economy Outlook 2015 sees consumer protection and empowerment as one of the key determinants of consumer IoT adoption, including *"adequate information disclosure, fair commercial practices including quality of service, and dispute resolution and redress"*[156]. The Australian consumer regulation protecting consumers is (mostly) governed by one piece of legislation – the *Competition and Consumer Act 2010 (Cth)*, and in particular, Schedule 2 **'Australian Consumer Law' ("ACL")**. Some consumer law issues relevant to IoT are identified and discussed below.

Liability of Manufacturers for Goods with Safety Defects

One issue that sits between IoT security, privacy and consumer protection is that of product liability for IoT goods or services that are not sufficiently secure. As discussed earlier, IoT security is no longer a data or privacy problem – it is a *safety issue*. If a connected device is insecure *by design*, or its software is insufficiently secure, should this be considered a 'safety defect' in certain products? While smart cars or bionic implants are obvious candidates, what about smart appliances that, if misused, can be dangerous, such as smart ovens or home security lock systems? Above, the Babel family was lucky to be out of their house when it was 'hacked', otherwise it would have been very unsafe.

Part 3-5 of the ACL deals with the liability of manufacturers for goods with safety defects. The manufacturer is liable if a safety defect caused loss or damage to an injured individual, other goods, land, buildings or fixtures. A **'safety defect'** is defined in s 9(1) of the ACL: '*the safety is not such as persons generally are entitled to expect*', with further considerations listed in s9(2) ACL. Consumers are growing to *expect* better security standards in their devices, especially in trusted brands. At the same time, they may also *expect* the device to be vulnerable to hacking, as a widely known and accepted caveat of using the Internet. Ascertaining the correct level of 'expectation' is difficult.

'Faulty product software' is a relatively unexplored area of product safety and liability. This is complicated further because there are no statutory minimum standards for a product's software or digital security, making it difficult to determine liability. Law firm **Norton Rose Fulbright** predicts that *"courts... may face complicated factual scenarios in tort claims relating to such devices... in the absence of contractually or legislatively-defined liability parameters"*[157]. **Michael O'Brien** lists some hypothetical case studies in the context of IoT products:

1. The malfunction of an IoT product due to a software glitch, resulting in property damage or physical injury
2. A malicious cyber-attack as a result of insufficient software or hardware security causes property damage or physical injury

[156] Chapter 6: 'Emerging Issues: The Internet of Things' in OECD, *OECD Digital Economy Outlook 2015* (15 July 2015) <https://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm> p.266

[157] Norton Rose Fulbright, *Big Data and the Internet of Things: Protecting rights, controlling use and extracting value* (Report, 2015) <http://www.nortonrosefulbright.com/knowledge/publications/123228/big-data-and-the-internet-of-things>
p13

3. Unauthorised access via data breach, compromising private or personal information[158].

Consumer Guarantees for Connected Goods and Services

Part 3-2 of the ACL deals with consumer guarantees when purchasing goods or services. Specifically, s54 of the ACL is a guarantee of 'acceptable quality', including 'free from defects' and 'safe'. Multiple factors are considered like nature of the product, price, representations and relevant circumstances. Above, the Babels probably should not have expected 'acceptable quality' since they knowingly purchased a cheap, non-legitimate product. However, this will depend on the 'factual matrix' and circumstances – did the product *look* illegitimate? Did the vendor look reputable or legitimate? Was the price so low (relative to the usual retail price) that a reasonable consumer could not expect that the item was legitimate? Did the product include registration codes or authentication?

The lack of case law on the application of consumer guarantees to telecommunications services creates some uncertainty. IoT products rely on a complex interdependence of Internet services like IoT applications, cloud services or other digital applications or processes. This means consumers may be faced with a confusing mix of causation when attempting to assert their rights under a consumer guarantee.

Identifying Fault

IoT will complicate **identifying 'fault' in a value chain**. In most connected products, there are a number of 'contributors' – from the manufacturer, software developer, hardware component suppliers and network providers to the individual app developers and the end-user. Each one (or more) of these 'links' in the 'value chain' can be the cause of a defect or fault, and attributing blame is an emerging issue in a connected world. Does the fault lie with the consumer for not updating the software, or with the software developer for forming vulnerabilities, or with the retail service provider for not 'pushing' manufacturer software updates quickly enough? Perhaps it may come down to *reasonableness* – was the software updated expediently enough after a vulnerability was discovered? Who is liable if this vulnerability is considered a 'fault'? What if a patch is released too slowly to sufficiently mitigate loss? What if the consumer is slow to install a timely update?

Representatives from major Australian Internet Service Providers **("ISPs")** are all concerned about liability and customer complaint handling[159]. In interviews, each of them stressed how ISPs, as the network providers, have become the first point of contact for consumers faced with technical or network difficulties. **Ana Tabacman** from Optus encourages proactive consumer awareness campaigns, particularly from government. Evidently, there are many variables in identifying fault in connected 'things' – a future challenge for consumers, businesses, regulators and the judiciary.

Connected 'Things' and Autonomous Contracting

Connected 'things' will supposedly learn consumption habits and can be programmed to provide personalised recommendations or make purchases autonomously. If done properly, this could

[158] Michael O Brien, 'The Internet of Things: The Inevitable Collision with Product Liability', *Product Liability Advocate* (online) (2 February 2015) <*http://www.productliabilityadvocate.com/2015/02/the-internet-of-things-the-inevitable-collision-with-product-liability/*>

[159] Interview with Ana Tabacman, Optus (via telephone, 1 June 2015); Interview with Andrew Scott, Telstra (via telephone, 28 May 2015); Interview with Sean Alexander, Vodafone Hutchison Australia (in person, 2 June 2015); Interview with Steve Dalby, formerly iiNet (via telephone, 4 June 2015).

revolutionise consumer convenience – but what happens if the device enters into a transaction that the consumer didn't want, based on an inaccurate prediction or pre-programmed habit? Is it a valid transaction?

Internet of Things and Environmental Implications

The environmental implications of so many small, disposable connected devices present a significant challenge for governments and officials, but by harnessing the power of data analytics and improved energy expenditure, a 'net benefit' for the environment may result[160].

IoT device disposal, waste management and recycling is one of the biggest environmental concerns of a connected world. If the forecasts are correct, hundreds of billions of cheap, connected things will flood the market. Each of these will need resources to manufacture and will eventually need to be replaced. If manufacturing is done responsibly (making them recyclable and using recycled materials), the disposal and recycling effort will be less burdensome. It is uncertain whether existing initiatives like TechCollect or the National Television and Computer Recycling Scheme are sufficient to address the anticipated influx in connected 'things' – but therein lies an opportunity for those that can create a solution.

On the other hand, a connected IoT ecosystem may ***save*** **more power than it consumes**. Consider, for example, the Babel home – it went into 'energy saving mode' when no one was at home, the Babels were able to monitor each device's consumption to identify leaks and practice 'smart' energy expenditure. The savings may be bigger on a *public scale*. Smart grids and individual management may bring unprecedented energy consumption savings. A 2013 report by **AT&T** and **Carbon War Room** anticipated that IoT could cut 9.1 billion tons of greenhouse emissions by 2020, being 18.6% of the total emissions in 2011[161]. A 2014 paper by **Intel** lists some more environmental applications of IoT:

- Low-cost air and water quality monitors that capture real-time data on pollution.
- Low-cost water sensors that detect both nutrients and pollutants in water supplies.
- Smart power and water grids that better identify leaks enable predictive maintenance and manage flows of electricity and water consumption.
- Connected Car fuel consumption systems and traffic analytics that minimise congestion and better direct traffic flow, minimising air pollution.
- 'Precision agriculture' that deliver the ideal amount of water, pesticides and fertiliser.
- Ambient weather sensors that predict weather conditions[162].

[160] Klint Finley, 'The Internet of Things Could Drown Our Environment in Gadgets' *Wired* (online) (5 June 2014) <*http://www.wired.com/2014/06/green-iot/*>
[161] Matt Cullinan, *Machine to Machine Technologies: Unlocking the Potential of a $1 Trillion Industry* (Research Report, The Carbon War Room and AT&T, February 2013) <*https://carbonwarroom.com/sites/default/files/reports/M2M%20Technologies%20(Carbon%20War%20Room).pdf*> p.5
[162] Intel, *The IoT and Energy and Environment Policy Principles* (Report, 2014) <*https://www-ssl.intel.com/content/www/us/en/policy/policy-iot-energy-environmental.html*> *pp. 2-3*

Recommendations for Consumers

Early adopters must stay informed, choose their uses carefully and be aware that choices may not be durable

Education and information must be at the forefront of consumers' minds before making any purchases or using any IoT services. This report provides a summary of some of the issues that IoT will raise, and may assist consumers in identifying what IoT does, how it does it, where it does it and what that means for them. However, this report is not comprehensive and it is recommended that consumers proactively educate themselves about the services they use. **Robert Gregory**, partner of law firm Maddocks, has the following advice for consumers: *"Do your best to understand what the device is, how it works (at a functional level) and what the consequences of using it may be. Be cautious about your privacy and disclosing your personal information. Make informed decisions about choosing devices and apps from sources worthy of your trust"*[163]. The OECD Digital Economy Outlook 2015 contains an excerpt of purchasing considerations for IoT dementia equipment **(Figure 27)**[164] – an excellent starting point for the types of questions that consumers should be asking. An informed consumer is an empowered consumer, and an informed consumer can make better choices and shape a better IoT market, with privacy, security and control at its core.

Box 6 What to consider when purchasing IoT equipment related to dementia (adapted)

Questions for professionals working in dementia

- What are the limitations of the technology to be used?
- Does the technology connect to other devices? If so, is compatibility an issue?
- Does the use of the technology match what the manufacturer has produced it for?
- Is battery life an issue? Who will be responsible for battery management?
- Does the product need to be waterproof?
- What can go wrong with the chosen technology?
- If the technology fails, what are the associated risks of the failure?
- What are the maintenance arrangements for the product and is it covered by a warranty?
- Who is responsible for equipment testing and how often will this take place?

Questions for individuals, families and carers

- How does it work, who will show me how to use it, are the instructions easy?
- Do I need a phone line or internet connection to use the technology?
- Who do I contact if something breaks or if I have a problem?
- Do I need to change batteries or charge them, and how often do I need to do this?
- Who will install the equipment and will I experience any disruption to my life?
- If my needs change, will the technology still support me?
- What evidence or information is there to help me decide what technology I need?
- Is there a helpline I can call if I have any concerns?
- Is there a response service that will come out if a particular alarm is triggered?

Source: Alzheimer's Society, 2014.

Figure 27 – Consumer IoT Purchasing Tips. Source: OECD.

[163] Interview with Robert Gregory, Maddocks law firm (via online correspondence, 9 June 2015)
[164] Chapter 6: 'Emerging Issues: The Internet of Things' in OECD, *OECD Digital Economy Outlook 2015* (15 July 2015) <https://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm> p 270

Avoid communication breakdown: Assess specific communications standards in use by each device

Interoperability is crucial for an ideal IoT ecosystem. Before purchasing any connected 'things', consumers must ensure that they are aware of how the rest of their IoT ecosystem communicates and operates. Most Connected Home products will connect to the home Wi-Fi, a very common standard. However, many smaller devices do not, and consumers may want to ensure the following:

1. Each device in their 'IoT ecosystem' can communicate with other necessary devices.
2. Each IoT application will synchronise with other IoT applications (where required).
3. The IoT service works fluently with the consumer's preferred cloud service (for instance, Dropbox has universal compatibility, but Google Drive and Apple iCloud may have *more limited* functionality for non Google/Apple devices).
4. If consumers invest in a 'hub' (such as Google's OnHub or Samsung's SmartThings Hub), they should ensure that each desired device synchronises with the 'hub' effectively.
5. Do some research on how their data is stored, and whether it can be migrated to another IoT service if they wish to switch products or brands down the track.
6. Look for IoT services that give as much control and data management as possible – either in a 'privacy dashboard', 'opt in/opt out' options, robust privacy policies or other means.

Build a Connected Home that is manageable, serviceable and user-friendly

According to a 2012 report by the **International Telecommunications Union** (ITU), building the Connected Home will involve 5 key 'players' (**Table 6**)[165]:

Table 7 – The 'players' in a Connected Home

Network Provider	Device Provider	Platform Provider	Application Provider	Application Customer
Provides the network infrastructure, such as fixed/wireless broadband, telephony or wireless services.	The company or manufacturer providing each and every connected 'thing', such as your smartphone, TV, car or smart toaster.	Provides the 'platform' that manages the devices and data in your 'ecosystem' – including data storage, processing and device management.	The developer that provides the application(s) that you use to view, manage and control your IoT devices and ecosystem.	This is the end-user and the beneficiary of the IoT products and services.
Examples: Telstra, Optus, Vodafone, iiNet, TPG.	**Examples**: Samsung, LG, Apple, Sony, Tesla, Nest.	**Examples**: Apple's HomeKit, Google's Brillo, Amazon Web Services, Samsung Smart Home.	**Examples**: Samsung for SmartThings, Apple's Home app, Nest app.	**Examples**: you, your family, your employees, patients, citizens.

[165] International Telecommunications Union (ITU), *Recommendation Y.2060 (06/12): Overview of the Internet of Things* (ITU Report, 2012) <https://www.itu.int/rec/T-REC-Y.2060-201206-I> Appendix 1 pp 10-13.

This is also a handy table to refer to when identifying standards – will the Platform Provider effectively manage all of your devices? Is one app available on two different devices, and if so, do they synchronise with each other? One entity may take on multiple 'provider' roles. For instance, Telstra could provide the network and some IoT devices, Samsung could provide devices, a platform and applications, or Google and Nest could one day be the sole provider of all five.

Protect your privacy and security: know your product, know its limitations and be aware of the context of its usage

Privacy and security are quickly becoming selling points for consumers, and rightfully so. These two components work well together – a more secure device (via manual override features, encryption, stronger authentication systems and more) means better privacy from external parties. It is harder to compromise, and if it is compromised, the data is less accessible. Privacy, trust, security and user control are quickly becoming key considerations when using IoT products or services. Informed consumers will consider all four of these before making decisions.

Consumer Reports Magazine gives the following IoT-specific recommendations for consumers:

1. Password-protect IoT devices;
2. Read the privacy policy;
3. Find the 'off' toggle for features you don't want;
4. Turn off connected devices when not in use;
5. Install security updates regularly; and
6. Purchase non-connected versions of products if you do not need the online features[166].

ZDNet also gives the following six recommendations for protecting a Connected Home:

1. Change all passwords (especially avoiding using the 'default' password') and make them strong and unique (or use a password vault such as LastPass);
2. Heighten default privacy and security settings;
3. Use strong encryption methods on the home Wi-Fi;
4. Install updates quickly and frequently;
5. Opt for a wired (not wireless) connection (for added security, use a separate network); and
6. Be careful when buying second-hand IoT devices [167].

[166] 'Privacy tips for the Internet of Things' *Consumer Reports Magazine* (online) (30 April 2015) <http://www.consumerreports.org/cro/magazine/2015/06/privacy-tips-for-the-internet-of-things/index.htm>

[167] Charlie Osborne, 'How to protect your connected home and Internet of Things devices', *ZDNet* (online) (13 October 2015) <http://www.zdnet.com/pictures/how-protect-your-connected-home-and-internet-of-things-devices/2/>

Recommendations for Internet of Things Product and Service Providers

Adopt the elements of the 'IoT Design Manifesto'

The IOT Design Manifesto is an unofficial code of conduct compiled by a number of design professionals and developers. While these recommendations apply specifically to the 'design' of IoT products and services, they can also be applied universally. The recommendations are paraphrased in **Table 7** below.

Table 8 – Elements of the 'IoT Design Manifesto'

Avoid the Hype	Design Useful Things
Aim for the Win-Win-Win	Keep Everyone and Every 'Thing' Secure
Build and Promote a Culture of Privacy	Collect Data Selectively
Transparency Between IoT Parties	Empower Users
Design for Longevity	Work Towards the Greater Good

Adopt the recommendations of the OAIC

User privacy is and will grow to be one of the biggest consumer considerations in acquiring IoT products and services. The first step towards proactive privacy processes begins with compliance. The **Office of the Australian Information Commissioner** makes ongoing recommendations for business so they may be compliant and proactive, including:

1. Undergo regular and comprehensive **Privacy Impact Assessments** (PIAs). Australian privacy consultant and industry expert **Roger Clarke** has provided a brief introduction to PIAs on his blog, and the OAIC website outlines a 10-step guide to conducting a PIA.
2. Follow the **OAIC Privacy Management Framework**.
3. **Take a holistic approach to the treatment of consumer data and personal information**. Many businesses collect different 'streams' of information. In and of themselves, they may not be considered 'personal information', but when considered as a whole, consumers may be 'reasonably identifiable' from the de-identified data that you hold.
4. **Take 'reasonable steps' to protect *all data*, not just personal information.** The OAIC has issued 10 tips for doing so.

Adopt a policy of data minimisation

Data minimisation refers to *"the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it"*[168]. This has a number of practical, commercial and ethical benefits. Firstly, large data sets are an attractive target for thieves, cyber attacks, and cyber-espionage. Minimising data collected would also minimise the attractiveness of the data 'honey pot'. Secondly, the more data that is retained, the more likely that the data will be intentionally, or accidentally, mishandled, or leaked, by employees or third-parties. Thirdly, it reduces the cost of retaining and securing consumer data, especially if the data held is superfluous. Some studies show that a large majority of data collected is not being used. McKinsey cited the example of an oilrig

[168] US Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, January 2015) <*https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*> p 21

where 99% of the data was not used by decision-makers[169]. Fourthly, it minimises the need to process and analyse data that is of no use. Finally, it maximises compliance with regulatory requirements, as the less data that is stored, the less risk that its collection or handling will breach legal requirements or that it will 're-identify' users.

Give consumers tools of empowerment

Taking a consumer-first approach should be adopted at each step of the value chain – from design and sale to support and ongoing experience. There are a few specific steps that IoT businesses can take:

1. **Create an information 'control hub'** where users can see, manage, control and delete the information that is held about them in an intuitive, transparent and user-friendly manner.
2. Adopt the **EU WP29 Report Recommendations** on consumer data protection. These are:
    a. *Conduct a privacy impact assessment* before releasing a device.
    b. *Delete raw data* from the device as soon as it has been extracted.
    c. *Follow privacy-by-design* and privacy-by-default principles.
    d. In a *user-friendly way, provide a privacy notice*, and obtain consent or offer the right to refuse.
    e. *Design devices to inform* both users and people interacting with them (e.g., people being recorded by a camera in a wearable technology) of the data processing by the entity providing the device.
    f. *Inform users* of data that has been collected and enable them to access, review and edit that data before it is transferred.
    g. Give users *granular choices* on the type of processing as well as time and frequency of data gathering[170].
3. Make it **easy to revoke consent**. While most IoT services and applications cease collecting data the moment the user uninstalls or unsubscribes from them, others do not. The ability to revoke consent permanently or temporarily should be as seamless as the ability to grant it.
4. **Create 'opt out' features**. The choice to 'opt out' is multi-faceted – consumers can be given the option to opt out of some product features and not others, or to simply opt out of the service completely. For example, when using a smart fridge, consumers should be able to select which (of the many) features they want, and switch off the rest as easily as one would toggle Wi-Fi on a smartphone. Citing an earlier example, this may involve 'opting in' to the weight sensors feature of a smart fridge, but 'opting out' of the barcode scanner.
   Another recommended 'opt out' application is the **ability to turn a 'smart thing' dumb again**; for example, the ability to switch off the 'smart' features of a smart fridge and limit it to simply refrigerating food. This has a number of benefits: it gives a consumer *manual* control over a product, it can mitigate a compromised network, it appeals to the privacy-conscious, and it gives consumers greater choice in the IoT marketplace.

---

[169] McKinsey&Company *The Internet of Things: Sizing up the opportunity* Executive Summary (June 2015) <http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity> Exhibit 3, p 25.
[170] Giulio Corragio, 'The Internet of Things: EU vs US guidance' *DLA Piper Publications* (online) (9 June 2015) <https://www.dlapiper.com/en/australia/insights/publications/2015/06/ipt-news-q2-2015/internet-of-things-eu-vs-us-guidance/>

Implement privacy, security, choice and useability 'by design'

One of the most common recommendations from the IoT reports, studies and think tanks preparatory to this report is the adoption of a 'privacy by design' (**"PbD"**) or 'security by design' (**"SbD"**) policy. This refers to engineering a product with privacy or security in mind throughout the entire design process. PbD and SbD are both supplementary and complimentary to consumer trust, a key driver for consumer adoption of IoT products and services. This notion is supported by **Sachin Babar et al** of Aalborg University, who constructed a 'cubic' security model for IoT[171] (**Figure 28)** where these three elements were the 'dimensions'.

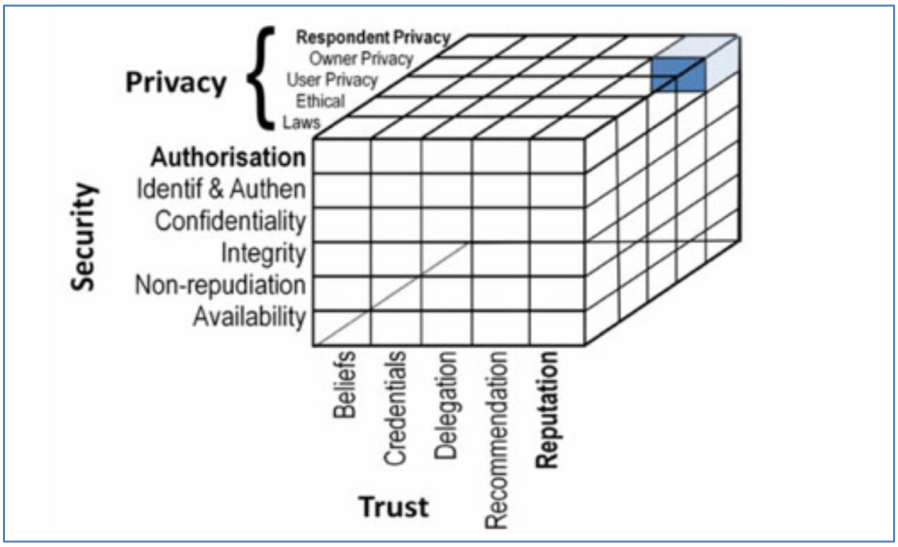


Figure 28 – Babar's Security Model for IoT. Source: Sachin Babar et al.

Privacy by Design

PbD is the most common recommendation to come from the hundreds of sources used for this report. Adopting PbD is a formal policy position of the Victorian Privacy Commissioner[172] and encouraged by the OAIC[173] and NSW Privacy Commissioner[174]. In 2009, **Ann Cavoukian** published the **7 Foundational Principles of PbD**:

1. Proactive not reactive; Preventative not remedial;
2. Privacy as the default;
3. Privacy embedded into design;
4. Full functionality – Positive-sum, not zero-sum;
5. End-to-end security – Full lifecycle protection;
6. Visibility and transparency – Keep it open; and
7. Respect for user privacy – Keep it user-centric[175].

---

[171] Sachin Babar et al., 'Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)' (2010) 189 *CCIS* 420- 429 <*ftp://ftp.inf.puc-rio.br/pub/docs/FomularioSolicitacoes/MarkusEndler-04-14.pdf*>

[172] Commissioner for Privacy and Data Protection, *Privacy by Design* <*https://www.cpdp.vic.gov.au/practitioners/privacy/privacy-by-design*>

[173] OAIC, *Privacy by Design (PbD)* <*http://www.oaic.gov.au/privacy/privacy-topics/privacy-by-design-pbd/*>

[174] Interview with Elizabeth Coombs, NSW Privacy Commissioner (via telephone, 5 June 2015)

[175] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Report by the Office of the Information and Privacy Commissioner, Ontario, Canada, August 2009) <*https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf*>

Security by Design

As alluded to earlier in this report, a poorly designed IoT security process can prove fatal or catastrophic. **Eileen Yu** of ZDNet notes that most IoT devices are 'not secure by design', citing one source as saying *"by default, these devices come from a lower point of security and are entering a world filled with very sophisticated adversaries"*[176]. There is no shortage of commentary on how IoT should be secured. After extensive stakeholder consultation, the **FTC** made a number of security policy recommendations in its January 2015 IoT report:

1. Undergo frequent security risk assessments;
2. Test security before launch;
3. Retain safe service providers;
4. Implement reasonable and secure access control measures;
5. Implement a policy of data minimisation;
6. Train employees on good security practices;
7. Take a 'defence-in-depth' approach;
8. Monitor the product's life cycle[177].

Jason Perlow, senior tech editor at ZDNet, lists some more IoT-specific security recommendations: move to IPv6 stack for IoT devices, use the IPSec standard for M2M and M2Cloud communication, use stronger encryption keys for Wi-Fi networks, add multi-factor authentication and finally, develop (or collaborate with) a 'one app solution' for managing security and software across devices[178].

Accessibility by Design

Creating more accessible IoT products and services, both for the elderly and consumers with disabilities, will require forethought, innovation and intuitive design concepts. The complexity in designing for the elderly or those with disabilities is that there are countless ways in which inaccessibility or usability issues may arise. It is difficult, if not impossible, for a 'one size fits all' solution.

'Opt-out' by Design

For effective implementation, it is recommended that 'opt-out' options be built in to both hardware and software. One example is 'manual override' options, which give users the ability to enable and disable specific features as they are needed. Another example is 'incremental' or 'dynamic' consent models, where each feature requires permission before it uses another hardware-enabled feature (such as location or microphone). This concept has been successfully implemented in Apple's iOS and Google's Android OS mobile platforms[179].

---

[176] Eileen Yu, 'IoT devices not secured by design' *ZDNet Australia* (online) (3 March 2015) <*http://www.zdnet.com/article/iot-devices-not-secured-by-design/*>

[177] US Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, January 2015) <*https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*> piii

[178] Jason Perlow, 'Secure or not, IoT is everywhere. Get used to it.' *ZDNet* (online) (14 August 2015) <*http://www.zdnet.com/article/iot-everywhere-get-used-to-it/*>

[179] Larry Seltzer, 'Mobile app permissions: Who does it right?', *ZDNet* (online) (28 October 2014) <*http://www.zdnet.com/pictures/mobile-app-permissions-who-does-it-right/*>.

Implement widely-accepted, open technical connectivity standards

Developing a set of interoperability and interconnectivity standards is the single most pressing requirement of IoT development and the single largest obstacle to IoT reaching its forecasted potential. Inadequate standards are bad for everyone – *"Developers will be reluctant to create devices, since they do not know if they will comply with any future standards. Similarly, end users may be reluctant to buy devices, because they are unsure if what they buy will be interoperable with existing or future products of the same type"*[180]. This is essential for maximising consumer benefit of IoT, and this can only be done by identifying and adopting dominant standards.

The **Comms Alliance IoT Report** made the following recommendation, and subsequently formed a working group of Australian industry representatives to develop a solution:

> *Develop minimum network/service security guidelines for the IoT service chain, from sensor/actuator, to network, to data. This needs to consider both security from attack and service resilience.*[181]

One commentator in **McKinsey**'s May 2015 IoT report stressed that IoT standards are in an ambivalent state: *"If you come out with them too early, they get ignored, and if you force adoption, they stifle innovation. If standards are set late, then companies with other existing standards will fight tooth and nail"*[182].

According to **McKinsey**, the 'winning standard' will have the following characteristics:

1. Clear value to all stakeholders (for example, reduced costs or technical advantage)
2. Part of a strong ecosystem (support across the industry and from other major players)
3. Allowance for a rapid rollout and scale-up, as well as easy adoption[183].

While defining standards may, on face value, be more of a regulatory issue, it is the author's tentative opinion that the market will develop leading standards quicker than policymakers will – by way of market forces or industry collaboration. Additionally, this stance coincides with the first recommendation to government and policymakers (below): 'innovate, wait, then regulate'.

---

[180] McKinsey&Company and Global Semiconductor Alliance (**GSA**), *Internet of Things: Opportunities and challenges for semiconductor companies* (May 2015) <http://www.gsaglobal.org/wp-content/uploads/2015/05/1.-GSA-McK_Report-IoT_Text_Executive-Summary.pdf> p11.

[181] Communications Alliance, *Enabling the Internet of Things in Australia* (online) (2015) <http://www.commsalliance.com.au/__data/assets/pdf_file/0009/50967/Enabling-the-Internet-of-Things-for-Australia.pdf> p 93.

[182] McKinsey&Company and Global Semiconductor Alliance (**GSA**), *Internet of Things: Opportunities and challenges for semiconductor companies* (May 2015) <http://www.gsaglobal.org/wp-content/uploads/2015/05/1.-GSA-McK_Report-IoT_Text_Executive-Summary.pdf> p 13.

[183] Ibid.

Recommendations for Government and Policymakers

Innovate, Wait, *then* Regulate

IoT remains a relatively new concept, and is still developing. Any *IoT-specific* regulation at this point may stifle innovation and prevent the market from growing organically. Based on the literature herein and interviews conducted, this report concludes that IoT-specific regulation should *only* be an option if the IoT market is failing or lacking, and even then should *only* address the particular market failure. Earlier this year, the **FTC** stressed that IoT-specific legislation would be *"premature, given the rapidly evolving nature of [IoT]"*[184]. **Robert Hillard**, partner at Deloitte, says that 'the race to IoT is a marathon' and stresses the importance of letting market forces work before regulating[185].

It is the conclusion of this report that any attempts to pre-emptively regulate IoT will be counter-productive. The author's opinion on excessively pre-emptive regulation echoes that of Rachel Dixon, cited earlier in this report; it will be attempting to form a solution without a problem.

Clarify the application of consumer guarantees to telecommunications services

As identified earlier, the lack of case law on the application of consumer guarantees to IoT in particular and telecommunications services generally creates some uncertainty. IoT goods and affiliated IoT services will become increasingly interdependent, and a defective service may render the associated good useless. Regulators have a role in clarifying this uncertainty through guidance notes and case law with the IoT consumer in mind.

Become a market leader and early adopter

The public sector and citizens stand to be the biggest beneficiaries of IoT. An economy-wide adoption of IoT is now inevitable, and by leading the market in IoT uptake, the government has the resources to help *create* an ideal domestic IoT market. By adopting new technologies and investing in secure, privacy-conscious IoT businesses, it will have a number of **industry and economic benefits**:

1. Early citizen and employee exposure to IoT.
2. Early identification of issues by an entity with the resources to address them.
3. Deeper and hands-on IoT experience for regulators, policymakers and public servants.
4. Catalysis of economy-wide IoT discussion and debate.
5. Greater foreign direct investment.
6. Future-proofing Australia's digital infrastructure at the perfect time to do so (with the current rollout of nbn's network).
7. The more efficient, streamlined and cost-effective delivery of government services
8. Contracts may be awarded to IoT businesses that best address consumer IoT issues, effectively *creating* an attractive domestic IoT market.
9. Potential standardisation of IoT, if a single standard is selected and invested in.

---

[184] Steven D Gravely and Erin S Whaley, 'The "Internet of Things" – Is Legislation Coming?'*Troutman Sanders* (online) (4 February 2015) <http://www.troutmansanders.com/the-internet-of-things--is-legislation-coming-02-03-2015/>

[185] Robert Hillard, 'The race to the internet of things is a marathon' *Information Driven Business* (online) (22 February 2014) <http://www.infodrivenbusiness.com/post.php?post=/2014/02/22/the-race-to-the-internet-of-things-is-a-marathon/>

By investing in IoT, the public sector is in a position to pre-emptively address any inhibitors of IoT early, and pave the way for strong growth in the Australian IoT market.

Develop a clear stance on private-sector use of publicly collected data

If the public sector adopts IoT in the delivery of government services, especially in the development of 'smart cities', staggering amounts of public data will be collected. How this data is handled and shared with the private sector is something that will need to be carefully managed. This is being addressed in a recent report by the Department of the Prime Minister and Cabinet[186].

Identify, define and regulate Connected Human data

Identifying, categorising and regulating Connected Human data will be a new challenge for state and federal privacy regulators. Earlier, this report discussed the possibility of activity tracker data being labelled as 'sensitive information', and thus having different implications under privacy law. The government should take a proactive approach in discussing this new area of policy, or one day that decision may be left up to a state or federal privacy commissioner by way of determination.

Introduce a data breach notification regime

In Australia, there is currently no *obligation* for entities to disclose to the public whether they have suffered a data breach. Mandatory data breach notifications have long been on the radar of policymakers[187]. This comes on top of recommendations from the PJCIS, academics, the OAIC, top-tier Australian law firms and David Seidler, the Google-ACCAN Intern 2014.

On 3 December 2015, the Attorney-General's Department released the long-awaited exposure draft amendment that would create a data breach notification scheme in Australia, along with a discussion paper and explanatory memorandum[188]. IoT will enable more data collection, more sensitive data to be collected and more covert means of data collection. It is imperative that the public is informed when their personal or sensitive information has been compromised. This report strongly encourages any interested party to make a submission to the Attorney-General's Department by 4 March 2016, and bear in mind the future of IoT and data collection in Australia.

[186] Department of the Prime Minister and Cabinet, *Public Sector Data Management Project* (Research report, July 2015) <*https://www.dpmc.gov.au/pmc/about-pmc/core-priorities/public-data-branch-within-dpmc/public-sector-data-management-project*>.
[187] Rohan Pearce, 'Mandatory data breach notification still on government's agenda' *Computerworld* (online) (11 August 2015) <*http://www.computerworld.com.au/article/581640/mandatory-data-breach-notification-still-government-agenda/*>
[188] Attorney-General's Department, 'Serious Data Breach Notification' (3 December 2015) <*https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx*>.

Form a national, multi-stakeholder, inter-agency Internet of Things body

It is recommended that the public sector form a multi-stakeholder, inter-agency IoT body that is responsible for compiling research, and advising on the implementation of an effective national IoT policy (if one is required in the future). The purpose of this body would be advisory, and would ideally release ongoing reports on the progress of IoT development, and peripheral policies, in Australia.

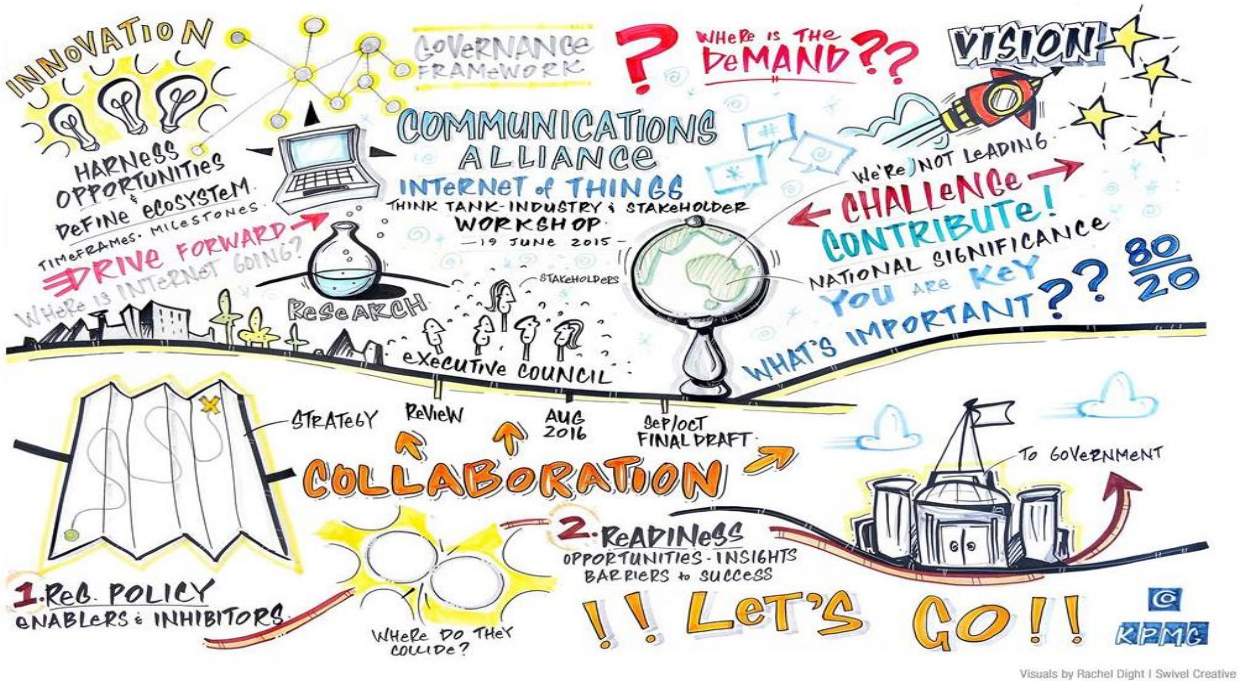


Figure 29 – IoT in Australia. Source: Communications Alliance IoT Think Tank (hosted by KPMG)

Following the **Comms Alliance IoT Report**, released October 2015, the Communications Alliance has formed six industry work streams, each focusing on one of six issues raised by the aforementioned report – collaborative Australian IoT industry; sectoral engagement; open data and privacy; spectrum availability; IoT security; and IoT start-up innovation[189]. Current participants include nbn, Telstra, KPMG, federal government departments, Google, Alcatel-Lucent, nbn, Optus, a number of law firms and other relevant industry players including ACCAN.

Conclusion

IoT is not 'coming' – it is here. IoT will not raise *new* privacy or security concerns – it will complicate and supplement existing ones. New technology brings uncertainty and distrust, but these should be seen as opportunities to innovate and develop new standards of consumer empowerment and protection. The good news is that IoT is still relatively new, and its foundation is still being built. Building the IoT with longevity and scale in mind is key to addressing consumer issues.

[189] Communications Alliance Ltd, 'Internet of Things' <http://www.commsalliance.com.au/Documents/Publications-by-Topic/IoT>.

As with most things, the IoT can be utopian or dystopian, but in reality, it will fall somewhere in between. Market solutions should be allowed to dictate the formation of the market, and if market failure is identified, regulators should be *prepared* to act, having already gathered research, public input and weighed the implications well in advance. In **Ray Bradbury**'s short story *The Veldt*, the Hadley family thought about *"turning the whole house off for about a month"* to *"live sort of a carefree one-for-all existence"*. With the right approach to IoT, we can achieve this existence by turning our houses *on*. It is not too late to do so, and consumers should lead the charge and *form* the IoT market that they can benefit from. This involves a digital government, a responsive industry with seamless interoperability, IoT-ready networks and telecommunications providers, and above-all, informed consumers.

APPENDICES

Appendix 1 – ISO/IEC JTC 1 Drivers of Internet of Things (selective list)

DRIVER	DESCRIPTION
Technology Drivers	**Direct factors** include market access to low-power devices, other connected products, computing power, advanced sensor technology and advanced actuators. **Indirect factors** include the prevalence and publicity of technology forecasts and the market for complementary goods.
Ease of Use	IoT goods and services should be *"easy to use, easy to build, easy to maintain, and easy to repurpose"*
Seamless Connectivity	The ability for IoT products and services to interconnect and communicate at the *user level*. The notion of 'plug and play' comes to mind. Factors include: 1. Effective communication 2. Network compatibility 3. Unrestricted, timeless control 4. Sensory capacities 5. An easy and pleasant user experience 6. Consistent, accurate and useful interpretation of IoT data 7. Automatic capturing, communicating and processing of data based on *customisable* operator preferences
Data Management and Control	The ability to process, manage and control (large) data sets from IoT devices.
Security	Consumer confidence that IoT systems cannot be used for malicious or unauthorised intent.
Privacy and Confidentiality	Confidence that privacy is kept.
Regulation	Compliance with all regulations, including: 1. Health and safety regulations 2. Environmental regulations 3. Technical regulations
Infrastructure	Interoperability regardless of infrastructure (eg wired, wireless, internet, non-internet).
Awareness of Services	Many IoT service operate discreetly and seamlessly. However, consumers need to know of their existence..
Accessibility and Usage Context	Maximum adaption to individual accessibility and usability requirements, and context-rich qualitative outputs from quantitative data sets.
Cohesive Set of Standards	The harmonisation of IoT connectivity and communication standards, ensuring interoperability.

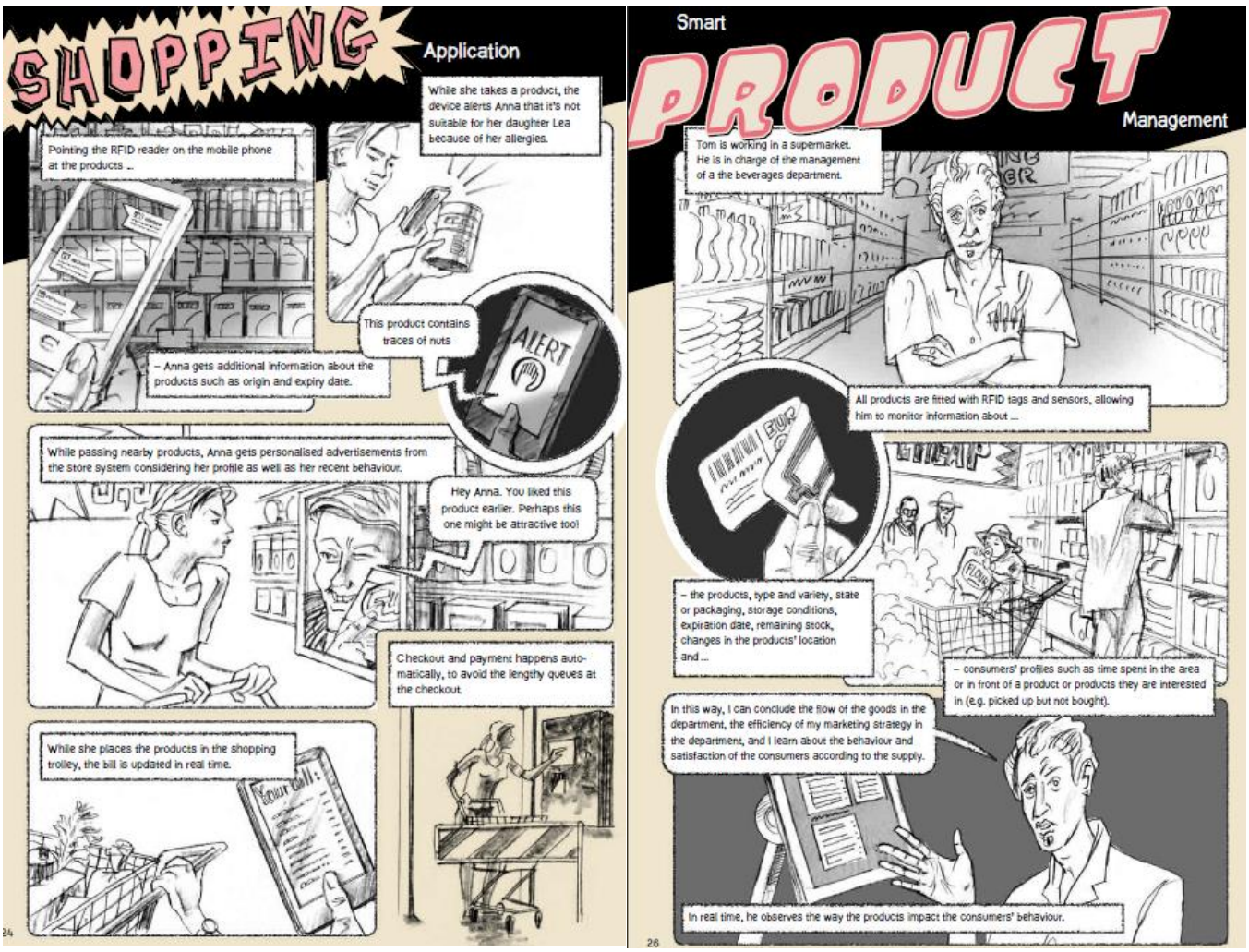
Appendix 2 – The Connected Human: Examples of Bio-Indicator Inferences*

Inference	How inference could be made
Sleep quality and patterns	**Method:** Sleep data, physical movement, *specific* instances of caffeine consumption, context (time and duration of inactivity) **Value:** Diagnosis, personal health tracking, personalised marketing (insomnia treatment, medicine), employee productivity monitoring.
Fitness levels	**Method:** Combination of heart rate, activity, steps taken, length of workouts, intensity of workouts (deduced from heart rate), blood pressure, body fat, calorie input and expenditure, physical movement. **Value:** Bridge the gap in medical research for data on *healthy* patients, personal tracking, professional athletes, promotional marketing, health insurance calculation.
Caloric Expenditure	**Method:** Body temperature, heart rate, activity intensity, muscle mass, BMI, resting metabolic rate and fitness level. **Value:** Personal tracking, dietary monitoring, medical diagnosis.
Caffeine consumption	**Method:** Heart rate (spike, plateau and dip consistent with stimulant intake), calorie input and expenditure. **Value:** Personal tracking, personalised advertising (towards coffee-drinkers), market research, remote health monitoring
Alcohol consumption	**Method:** Heart rate (consistent with depressant intake), caloric input, context (time and GPS location), breathalyser/alcohol sensor. **Value:** Personal tracking, remote health/alcoholic support group monitoring, personalised advertising (towards alcohol drinkers), market research, health insurance calculation.
Smoking habits	**Method:** photoelectric and ionization detectors, blood nicotine levels, respiratory inductance plethysmograph, gyroscope and accelerometer (hand gestures) *or* tobacco residue/smoke sensors. **Value:** Personal tracking, remote health/anti-smoking support group monitoring, personalised advertising (by both tobacco and anti-smoking businesses), cancer/medical/market research, health insurance.
Recreational drug consumption habits	**Method:** Heart rate (consistent with specific drug use - sharp and sustained spike for amphetamines), context (time and GPS location) **Value:** Criminal enforcement, court-ordered compliance, remote health/rehabilitation support monitoring, population research, health insurance calculation, employment, monitoring children or loved ones.
Stress Levels	**Method:** *Average* heart rate and *average* blood pressure, sleeping patterns, consumption of alcohol, cigarettes, drugs *(see above)*. **Value:** Diagnosis, population statistics, personalised marketing (for anti-stress products or pharmaceuticals), health insurance calculation, employee wellbeing, mental health medical research.
Location history	**Method:** GPS, altimeter, compass, Bluetooth/NFC sensors. **Value:** Commercial/criminal/state surveillance, personal tracking, tracking of ill, elderly or young loved ones, proximity marketing (such as walking around sections of a shopping centre), speed and distance (for purposes of car insurance), employee tracking and absenteeism, litigation evidence and military field usage.

Inference	How inference could be made
Illness or disorder	**Method:** Heart rate, blood pressure, various biological data (from implantable or ingestible 'things'), body temperature, **Value:** Personal tracking, monitoring ill, elderly or disabled loved ones, remote medical monitoring, disease detection/prevention, rehabilitation, medical research, personalised marketing (for medicine or treatments), health insurance calculation and disease tracking.
Nature and network of relationships	**Method:** Any dataset (particularly time and location) cross-referenced with the same dataset of another individual (Eg. A and B both exercised intensively in same location for one hour, inference of social association). When combined with other inferences, the nature of the relationship can be deduced with reasonable accuracy. **Value:** State/commercial/criminal surveillance, personalised marketing (building user profiles), corporate profiling, litigation evidence.
Sexual health and performance	**Method:** Usage data from connected wearables (sex toys, accessories, 'connected' condoms), heart rate data combined with movement sensors, duration, context (time, GPS location and proximity with other individual, pattern of similar, consistent data). **Value:** Surveillance, personalised marketing (lifestyle products, sexual performance/dysfunction pharmaceuticals), criminal investigation and evidence (sexual assault allegations), sexual health research, customisable settings on lifestyle accessories, improved intimacy in relationships.
Diet - what, when, how much	**Method:** Caloric input, pattern recognition software, user input, visual augmented reality products and services (such as optical wearables like Google Glass). **Value:** Personal tracking, dietary monitoring, remote health monitoring, medical research.
Type of exercise(s) performed	**Method:** Heart rate, movement sensors (accelerometer, gyroscope etc.) **Value:** Personal fitness monitoring, market research, rehabilitation.
Nutrition levels	**Method:** Complex biological data from ingestible or implantable devices, limited sensory data from wearables (blood glucose from smart contact lenses, physiological data from smart pills), nitrate sensors. **Value:** Personal fitness/health tracking, remote medical monitoring, dietary monitoring, medical research, personalised marketing (of multi-vitamins, for example).
Pollution and atmospheric/ environmental information	**Method:** Barometer, thermometer, hydrometer, other atmospheric or environmental sensors (dust particles, pollution, CO_2, radiation, electromagnetic feedback, air quality, airborne chemicals etc.) **Value:** Personal health, pollution monitoring and alerts, benefit to asthma, hayfever or allergy sufferers, real-time weather forecasting and military usage (chemical warfare agents).
more…?	

* This table was created entirely by the author using his personal knowledge of IoT devices, biological and physiological indicators and the operability of existing tech. While this information has been proof read by more informed parties, and most of these technical processes exist, it should be treated as hypothetical, and not factual.

Appendix 3 - The Alexandra Institute's Vision of Connected Retail[190]



[190] The Alexandra Institute, *Inspiring the Internet of Things* (Comic book, 2011) <https://iotcomicbook.files.wordpress.com/2013/10/iot_comic_book_original.pdf> pp 24-27.

Appendix 4 - Solove's 'Taxonomy of Privacy' (An Internet of Things Perspective)

Daniel J. Solove's 'Taxonomy of Privacy Invasions'[191]			
Information Collection	*Information Processing*	*Information Dissemination*	*Invasion*
• Surveillance • Interrogation	• Aggregation • Identification • Insecurity • Secondary Use • Exclusion	• Breach of Confidentiality • Disclosure • Exposure • Increased Accessibility • Blackmail • Appropriation • Distortion	• Intrusion • Decisional Interference
Explanation of Elements[192]			
The **first group of activities** that affect privacy involves information collection. • ***Surveillance*** is the watching, listening to, or recording of an individual's activities. • ***Interrogation*** consists of various forms of questioning or probing for information.	A **second group of activities** involves the way information is stored, manipulated, and used. • ***Aggregation*** involves the combination of various pieces of data about a person. • ***Identification*** is linking information to particular individuals. • ***Insecurity*** involves carelessness in protecting stored information from leaks and improper access. • ***Secondary use*** is the use of information collected for one purpose for a different purpose without the data subject's consent. • ***Exclusion*** concerns the failure to allow the data subject to know about the data that others have about them and participate in its	The **third group of activities** involves the dissemination of information. • ***Breach of confidentiality*** is breaking a promise to keep a person's information confidential. • ***Disclosure*** involves the revelation of truthful information about a person that impacts the way others judge their character. • ***Exposure*** involves revealing another's nudity, grief, or bodily functions. • ***Increased accessibility*** is amplifying the accessibility of information. • ***Blackmail*** is the threat to disclose personal information. • ***Appropriation*** involves	The **fourth and final group of activities** involves invasions into people's private affairs. • ***Invasion***, unlike the other groupings, need not involve personal information (although in numerous instances, it does). Intrusion concerns invasive acts that disturb one's tranquillity or solitude. • ***Decisional interference*** involves the government's incursion into the data subject's decisions regarding their private affairs.

[191] Table compiled by the author, content reproduced from Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 478-91.
[192] Ibid pp 490-91.

	handling and use.	the use of the data subject's identity to serve the aims and interests of another. ● ***Distortion*** consists of the dissemination of false or misleading information about individuals.	
How does this apply to the Internet of Things?[193]			
Interrogation is not relevant. *Surveillance* is a big privacy violation risk in the IoT. We will interact with hundreds of sensors daily, each picking up 'crumbs' of information as we go about our lives. Traditional surveillance concerns like CCTV are now more intimate with IoT in our homes and in our bodies.	Many of these areas are regulated by information privacy law. Most fall within the scope of 'Big Data' and not 'IoT' *per se*. *Aggregation* of smart things is essential for a fluent IoT ecosystem, and information processing is essential to 'sync' every 'thing' up around your life. *Identification* and *Insecurity* are discussed in separate sections of this report.	The areas most relevant to IoT are *disclosure, increased accessibility* and *appropriation*. Intimate data is collected seamlessly and if misused, can prove embarrassing, destructive or even fatal. IoT data is captured and processed by algorithms and humans to form accurate inferences. However, it can also be used to make inaccurate, misleading inferences that can impact consumers.	IoT is very vulnerable to privacy *invasion*. Advanced IoT ecosystems are designed to collect information subtlety (sometimes covertly) and 'in the background' - making it easy for consumers to have their data collected without informed consent. *Decisional Inference* is one of IoT's biggest opportunities *and* risks. Accurate data will spur a golden age of convenience and automation, but misuse will spur a golden age of surveillance, privacy intrusion and intrusive or misleading behavioural inferences.

[193] This section is entirely the author's original work.

Appendix 5 - The 13 Australian Privacy Principles (APPs)

Australian Privacy Principles — a summary for APP entities

from 12 March 2014

Australian Government
Office of the
Australian Information Commissioner

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

For private sector organisations, Australian Government, ACT Government and Norfolk Island agencies covered by the *Privacy Act 1988*

www.oaic.gov.au