THE INTERNET OF THINGS

A UKeiG WHITE PAPER

UK eInformation Group

THE INTERNET OF THINGS

A UKeiG WHITE PAPER

MARTIN DE SAULLES, UNIVERSITY OF BRIGHTON

Published by UKeiG, the UK eInformation Group of CILIP, the Chartered Institute of Library and Information Professionals

www.ukeig.org.uk

Published in April 2016

Series: UKeiG White Paper: 2016/01

ISBN: 978-1-870254-16-8

Abstract

This White Paper presents an overview of some of the key issues surrounding the development and deployment of the collection of technologies commonly referred to as the Internet of Things (IoT).

The technological underpinnings of the IoT are discussed in the context of a rapidly developing new field of technology and with an acknowledgement that there is some way to go before commonly accepted standards are agreed upon and that the commercial case, particularly in the domestic sphere, for the IoT is yet to be made. Examples of current IoT deployments across a range of sectors are presented.

This paper also explores some of the social issues surrounding the IoT where security and privacy concerns are inhibiting the diffusion of IoT products and services and where much work needs to be done if end-users are to accept this new technology.

Driving the development of IoT technologies is the demand for data and the potential for a revolution in how we understand our environments through the embedding of sensors and computational intelligence in everyday objects. The collection and analysis of this data will create new types of companies and change the business models of many existing ones. It is uncertain what the IoT landscape will look like in 2020 but the opportunities for data experts are considerable.

The paper concludes with a note on the potential relevance of IoT to libraries.

Table of Contents

1. Introduction

1.1 What is the Internet of Things?

The Internet of Things (IoT) is an area of technology many people are at least aware of, although it has been interpreted in different ways over the last 15 or so years leading to widespread confusion. This has not been helped by some of the overblown claims for its significance by technology vendors and analysts.

The term, IoT, dates back to 1999 when Kevin Ashton, then a brand manager at Proctor and Gamble (P&G), saw the potential for RFID chips to help streamline the supply chain for companies like P&G. Public and academic libraries have witnessed the impact that the humble RFID chip has had on the checking in and out of books by users leading to a more efficient service. Writing 10 years later, he reflected on how the internet and World Wide Web (WWW) had developed since the early 1990s and how the next phase of development would be more focused on direct communications between computers:

> "Today computers—and, therefore, the Internet—are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings—by typing, pressing a record button, taking a digital picture or scanning a bar code……The problem is, people have limited time, attention and accuracy—all of which means they are not very good at capturing data about things in the real world." [1]

The capturing and sharing of data by computers without the direct input of humans is at the heart of the IoT. This is where the "Things" play their part, as every-day, familiar objects, as well as less familiar ones, are fitted with sensors, processors and radio chips allowing them to share data on their operations and their environment.

The technology analyst company, Gartner, defines the IoT as:

> "…the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." [2]

These objects may include domestic items such as light bulbs, fridges, door locks and thermostats as well as industrial equipment including jet engines, bulldozers, air quality sensors and factory production lines. The rapidly decreasing cost of embedding these technologies into objects has been accelerated by the widespread adoption of smartphones and the component industry which has sprung up to make the GPS chips, accelerometers, processors and radio chips embedded in the more than 3 billion smartphones in use globally.

So while the IoT does not refer to a specific technology, it does describe a set of technologies and, more importantly, their functionality. This functionality allows data thrown off from the "things" to

[1] Kevin Ashton, "That 'internet of Things' Thing," *RFiD Journal* 22, no. 7 (2009): 97–114.
[2] Gartner, "IT Glossary," available at http://www.gartner.com/it-glossary/internet-of-things/

be used to deliver new and improved services, increase industrial productivity, reconfigure business models and provide new insights into the environments in which we live and work.

1.2 Why the IoT is Important

Anyone who has worked in the information industry over the last 20 years, whether as an information manager, librarian, data scientist or on the vendor side may, with some justification, be sceptical about some of the claims being made for the impact that the IoT is going to have on our lives. New technologies are often over-hyped by those with a vested interest in promoting them. The rise of knowledge management (KM) as a new way to manage the information and knowledge assets of an organization throughout the 1990s led to many unrealistic claims about how KM approaches and technologies would transform the workplace. Tom Wilson [3] provides a useful analysis of the KM phenomena with the title of his 2002 paper, "The Nonsense of Knowledge Management", giving a clue as to his approach. More recently, "social business" technologies have tried, with varying degrees of success, to introduce elements of public social network services into the workplace to streamline internal communications and help with information sharing. Perhaps a common failing of all these workplace technologies is the struggle they have with integrating technology with the working practices of individuals. People often have a habit of subverting or resisting the imposition of technical solutions to the way they communicate with others.

So is the IoT another over-hyped technology destined to disappear when the next "new thing" comes along? This seems unlikely, partly because the IoT refers to a diverse set of technologies, protocols and services but also because real benefits are already being seen across a range of industries as well as in our domestic lives. Technology industry analysts, IDC, estimate that the IoT market was worth $656 billion in 2014 and will reach $1.7 trillion by 2020 [4]. The strategy consulting firm, McKinsey & Company believe the impact of the IoT on the global economy could be as high as $6.2 trillion by 2025 [5]. Any market forecast looking more than several years into the future needs to be treated cautiously but the growing body of data showing historic and current IoT market estimates indicates this is a real area of growth. The technologies underpinning the IoT are already being deployed and products and their associated services are currently available in the marketplace, as this White Paper demonstrates in the following sections.

Having defined what the IoT is and why it is an area of significant interest to anyone who works with data and information services, the following sections will go into more detail on some of the key issues relating to its deployment. Section 2 examines how the IoT is having an impact in the workplace, the home, our cities as well as more intimately in how we monitor our bodies. Section 3 focuses on the most important aspect of IoT deployments, the data which is generated from the "things". As will be shown, it is the data outputs which are driving many of the business models

[3] Tom Wilson, "The Nonsense of Knowledge Management," *Information Research* 8, no. 1 (2002): 8–1, Available at http://www.informationr.net/ir/8-1/paper144.html
[4] Steven Norton, "Internet of Things Market to Reach $1.7 Trillion by 2020: IDC," June 2, 2015, http://blogs.wsj.com/cio/2015/06/02/internet-of-things-market-to-reach-1-7-trillion-by-2020-idc/
[5] Harald Bauer, Mark Patel, and Jan Veira, "The Internet of Things: Sizing up the Opportunity | McKinsey & Company," 2014, http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity.

emerging from this new technology. In Section 4 security issues surrounding the IoT are examined with a focus on the implications for personal privacy if IoT does become embedded in our daily lives. Finally, Section 5 looks at some of the key players in this sector and provides some tentative predictions as to how the market may evolve in terms of the companies driving IoT adoption and the platforms they are building, while Section 6 brings the discussion back to libraries.

2. Deploying the Internet of Things

2.1 IoT in the Home

Most mainstream media coverage of the IoT focuses on how household devices are being fitted with sensors and connected to the internet to create the "smart home". The "smart fridge" has been talked about for over a decade. This, supposedly, will be able to tell us what food is inside it and automatically order milk and eggs etc. as they run low. Reality has not yet managed to deliver this dream. White good vendors continue to try and bring the fridge into the twenty first century but the best on offer so far is one which can email you pictures of your fridge's contents while you are out shopping [6].

However, while a true smart fridge is still over the horizon, other "smart" household items do exist. Perhaps the most prominent are smart thermostats and energy meters which can monitor in real time the amount of energy being used within a home and allow users as well as utility providers to remotely manage temperatures around the house. In the US, the Nest thermostat links the central heating boiler to the internet and is able to determine whether a room is occupied, learn about individual user's temperature preferences and, via mobile apps, provide users the ability to control the heating system from anywhere. Smart meters provide utility providers as well as users with up-to-the-second data on energy usage making the days of the human meter reader numbered. While these may not seem particularly radical innovations, as they only really enhance the functionality of existing devices, it is the ability to monitor data in real time which offers the most potential. Google clearly sees these data streams as valuable judging by its purchase of Nest in 2014 for $3.2 billion. In the UK, the Hive thermostat, from British Gas, offers similar functionality. In the US, Nest users can agree to let their energy providers take control of the thermostat to adjust temperatures at times of peak demand. This offers cost-saving benefits to consumers but also allows utilities to more efficiently balance network load demands.

Internet-connected thermostats such as Nest and Hive show how our homes may evolve in an IoT age but there is clearly some way to go before the "smart home" becomes a reality. This is partly because many traditional household goods manufacturers do not have the technical expertise in working with the technologies which make up the IoT. Washing machines, fridges, dishwashers and door locks have evolved incrementally over the previous 50 years to become more efficient at the jobs they do but have not radically changed in design or function over that time. There is also the issue of IoT "solutions" often looking for problems to solve. It is not clear whether domestic users really want to be able to control their white goods from their phones or are interested in the marginal operating cost savings which may accrue from smarter devices. Samsung, Apple and Google

[6] Rich Brown, "Touchscreen Refrigerators and Talking Everything at CES 2016," *CNET*, January 10, 2016, http://www.cnet.com/news/touchscreen-refrigerators-and-talking-everything-at-ces-2016/.

are all rolling out products and platforms to connect our household devices to the internet and give us more control over them but, as with the early days of the personal computer (PC), compatibility between these systems and their communication protocols is an issue. PCs did not become pervasive until a dominant platform emerged as a result of the work between IBM, Intel and Microsoft. Most domestic users do not want to invest the time or have the expertise to solve the interoperability issues currently inherent in many home automation systems. While some of the larger vendors claim to offer systems which can allow your wifi-enabled light bulbs to talk to your smart home hub via a phone app the evidence shows this is not always simple or straightforward [7]. Discussion fora dedicated to helping users solve these issues are active places as consumers struggle with problems such as software updates and patches for their fridges [8]. As one commentator has observed:

> "The market as it is today is rife with the current trend by OEM companies to "stick a chip in it" in order to connect it to the internet and render it "smart", without any real value to the consumer." [9]

These problems will be solved as companies iterate on their products and learn what the market actually wants and how to deal with issues of interoperability. Lessons from the evolution of the PC, internet and smart phone sectors have shown us how technical platforms upon which others can innovate generally meet with greater success than closed, proprietary systems [10].

2.2 IoT in the Workplace

It is important to recognize that elements of what we now refer to as the IoT have existed in a number of industrial sectors for over 40 years. These were often referred to as telemetry systems whereby machinery could be remotely monitored through the use of sensors and wireless transmitters. Typically, such systems were used to monitor environmental variables such as temperature or humidity with the data generated staying within closed systems and used for very specific purposes. The rise of cheap and powerful sensors and microprocessors from the consumer-oriented smart phone industry, pervasive mobile networks and low-cost, powerful backend data analytics platforms have brought telemetry into the internet age. Often referred to as machine-to-machine (M2M) systems, the industrial IoT is at a more advanced stage than the domestic one.

A large driver of the industrial IoT are the cost savings which can be realized by businesses through the more efficient tracking and monitoring of industrial processes and equipment. The mining sector is adopting the IoT to both raise operating efficiencies and improve safety levels. Embedding sensors in digging and tunnelling equipment allows for real-time monitoring of moving parts and hydraulic

[7] Tim Bradshaw, "The Smart Home Is Still Too Clever for Its Own Good," *Financial Times*, October 22, 2015, http://www.ft.com/cms/s/0/f9a260f4-743a-11e5-a129-3fcc4f641d98.html?siteedition=uk#axzz4469NG0Qj.
[8] Google Product Forum, "Can't Sign in to Google Calendar on My Samsung Refrigerator - Google Product Forums," 2014, https://productforums.google.com/forum/m/#!msg/calendar/UhfpcwO0X0c/paA4iQNen9IJ.
[9] Theo Priestley, "The Smarthome Industry Is Dumb And Broken," *Forbes*, December 15, 2015, http://www.forbes.com/sites/theopriestley/2015/12/15/the-smarthome-industry-is-dumb-and-broken/.
[10] Annabelle Gawer, ed., *Platforms, Markets and Innovation* (Cheltenham: Edward Elgar, 2009); Jonathan Zittrain, *The Future of the Internet* (London: Penguin Books, 2008); Barbara van Schewick, *Internet Architecture and Innovation* (Cambridge, MA: MIT Press, 2010).

systems allowing predictive maintenance which can improve the uptime of machinery and prevent costly breakdowns [11]. In the aviation sector, modern jet engines from GE and Rolls Royce now have sensors with wireless capabilities fitted as standard. These provide real-time operating data to control centres on the ground with a typical engine generating 10 terabytes of data per 30 minutes of flying time [12].

Adding a data reporting layer of functionality to mechanical objects is helping users of this equipment to improve their operating efficiencies but is also changing the nature of the companies providing this kit. They are having to adapt from being simply manufacturers to providing services as well. Some companies see this as an opportunity to provide more profitable, value-added services to their customers. However, the move to becoming service providers as well as manufacturers presents a number of challenges in terms of adjusting business models or even creating new ones. At the macro level, this can be seen across entire economies, particularly those with a strong industrial base such as Germany. Just as the manufacture of PCs and, more recently, smart phones has largely become a commodity business with very low profit margins, so other industries are threatened by the rise of the application of software and connectivity to physical objects. The automobile industry is one of them:

> "That strikes a particular chord in Germany. Some fear its carmakers, which directly or indirectly employ one in seven workers nationwide, could be demoted to low-margin metal bashers, while American tech giants make most of the money by providing the software and the in-car entertainment - and perhaps, in time, designing the cars themselves." [13]

German automobile manufacturers and their supply chain partners are investing in new car designs, functionality and configurations to try and prevent this happening. Bosch, an automobile component manufacturer as well as tool maker announced in early 2016 that all its devices would be IoT-enabled by 2020 with a supporting back-end for data analytics it calls the Bosch IoT Cloud [14]. These initiatives are part of a broader, government-backed initiative launched in 2011 which the Germans call "Industrie 4.0" and which it is hope will help the transition from a manufacturing industrial base to a more service-oriented one. In the US, GE, a manufacturer of jet engines, locomotives and other heavy industrial equipment is also investing heavily in making its products "smarter". A spin-off from these investments has been the launch of its Predix data analytics platform which is available as a service to third parties wishing to upload and analyse their own data. Data services are becoming a major income stream for GE with its GE Digital division bringing in $5 billion of revenue in 2015 [15].

[11] Robert Spence, "Examining the Internet of Things and Its Impact on the Mining Industry in 2016," *Mining Global*, February 2016, http://www.miningglobal.com/tech/1825/Examining-the-Internet-of-Things-and-its-impact-on-the-mining-industry-in-2016.

[12] ITU, "Measuring the Information Society Report" (International Telecommunications Union, 2015).

[13] "Does Deutschland Do Digital?," *The Economist*, November 21, 2015.

[14] Timothy Seppala, "Bosch Is Building Its Own Internet of Things Cloud Network," *Engadget*, March 10, 2016, http://www.engadget.com/2016/03/10/bosch-iot-cloud/.

[15] "General Electric: The Industrial Internet Of Things - The Company Is Already Winning," *Seeking Alpha*, February 28, 2016, http://seekingalpha.com/article/3938056-general-electric-industrial-internet-things-company-already-winning.

2.2.1 IoT and Information Work

There is considerable evidence showing how the IoT is having an impact on traditional industrial sectors such as mining and car manufacturing. As the evidence of Bosch and GE show, the data generated by smart devices and equipment requires new backend systems to capture, store and analyse it. As this data is processed and transformed into meaningful information, those organisations which can derive strategic value from it will be the winners. The first wave of internet innovation has transformed how we access information through search engines such as Google but, with the exception of marketing data, has not really changed the types of data available to organisations. Online databases have been around since the 1970s and the World Wide Web (WWW) and search engines can be seen as extensions of those, albeit more powerful, comprehensive in their coverage and easier for end users to access. However, this next wave of innovation promises to add new types of information as the physical world becomes connected with the virtual world. Being able to manage and make sense of this data will require information workers to enhance their existing skills as well as develop new ones:

> "According to the global consulting firm, McKinsey & Company, the United States is facing a shortage of 140,000 to 190,000 people with the deep analytical skills necessary to translate all of this newly acquired data into meaningful information. And, where there is great demand combined with insufficient supply, there is an increase in price." [16]

Clearly there are opportunities for information workers who can master these skills and move into the world of big data and analytics.

2.3 IoT in the City

As populations continue to move to built-up areas with the associated pressures on housing, transport and health, many see the development of "smart cities" as a way to improve the living conditions of urban dwellers. It has been estimated that the number of urban residents is growing by almost 60 million a year and that more than 60% of the world's population will be living in cities by 2050 [17].

Street lighting is a good example of how the application of relatively simple sensors and controllers can provide for safer roads and save local authorities money. 10% of the UK's 7 million street lights are fitted with smart sensors from Telensa which allow their operators to control the lights centrally and respond to localized needs as well as monitor for maintenance and repair. An installation of sensors on 33,000 lights in Doncaster in 2015 will save an estimated £1.3 million a year in energy costs [18].

[16] Jennifer Priestley, "Society's Demand for 'Big Data' Creating Shortage of Skilled Workers," *Saporta Report*, June 29, 2014, http://saportareport.com/societys-demand-for-big-data-creating-shortage-of-skilled-workers/.
[17] Shane Mitchell et al., "The Internet of Everything for Cities" (San Jose, CA: Cisco, 2013).
[18] Shane Hickey, "The Innovators: The Smart Systems Driving Motorists towards Smarter Cities," *The Guardian*, April 3, 2016, http://www.theguardian.com/business/2016/apr/03/the-innovators-the-smart-systems-driving-motorists-towards-smarter-cities.

In London the AirSensa initiative aims to install 10,000 air quality monitoring sensors on buildings around the capital to allow real-time tracking of pollution levels [19]. It has been estimated that 29,000 premature deaths occur in the UK each year from air pollution with many of the pollutants invisible to the human eyes and noses [20]. An objective of projects such as that from AirSensa is to provide citizens and urban planners with up-to-the-minute data on pollution levels allowing more informed decision making on journey planning, transport routing and housing developments.

2.4 IoT and Our Bodies

The intersection of the IoT and our bodily processes is perhaps the most controversial area of this new technology. Being able to track and evaluate how our bodies are performing offers all sorts of potential health benefits both at the personal level but also at a broader societal level as well.

Fitness trackers which users wear such as the Fitbit have been available for several years and, more recently have evolved into more powerful devices such as the Apple Watch and Samsung Gear Fit. These can typically measure pulse rates, body temperature and physical activity. For athletes as well as those wishing to keep an eye on their exercise levels they provide useful information which can improve levels of physical performance.

Where the decision to wear a fitness tracker is a personal one and the data from it never leaves the control of the user, there is little debate about the ethics of this technology. However, when users are encouraged to wear them by their employers or health insurance providers the issues around control and surveillance start to become obvious. Employers in the US can offer their workers up to a 30 percent discount on health insurance premiums for participating in company wellness programs, some of which involve the wearing of fitness trackers [21]. A report from the Pew Research Center solicited the views of experts in the application of IoT technologies to various aspects of our personal and work lives and showed serious concerns about the potentially intrusive aspects of this technology, particularly with respect to wearables:

> ““Every part of our life will be quantifiable, and eternal, and we will answer to the community for our decisions. For example, skipping the gym will have your gym shoes auto tweet (equivalent) to the peer-to-peer health insurance network that will decide to degrade your premiums.” [22].

Whether or not this rather pessimistic view of the future becomes a reality, it does raise legitimate questions about who actually owns the data generated by IoT devices whether in our homes or on our bodies. The next section considers this and explores how data is driving the adoption of the IoT.

[19] “About AirSensa - Realtime Atmosphere Monitoring,” 2016, http://www.airsensa.org/about.php#.

[20] Public Health England, “Estimates of Mortality in Local Authority Areas Associated with Air Pollution,” April 10, 2014, https://www.gov.uk/government/news/estimates-of-mortality-in-local-authority-areas-associated-with-air-pollution.

[21] Hamza Shaban and Jacqueline Wernimont, “Big Doctor Is Watching,” *Slate*, February 27, 2015, http://www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html.

[22] Janna Anderson and Lee Rainie, “The Internet of Things Will Thrive by 2025,” *Pew Research Center*, 2014, http://www.pewinternet.org/2014/05/14/internet-of-things/.

3. Data as a Driver of IoT Adoption

3.1 The Transition from Products to Services

In Section 2.2 we saw that a number of established manufacturing companies are attempting to make the transition from being simply makers of products to adding a service layer to their offerings. This is partly to avoid the commoditization of their core outputs but also to allow a potentially more profitable business model. Adding data services to their commercial offerings adds value for their customers and differentiates them from their competitors. At the heart of this transition is the recognition that the data outputs from IoT devices are where the real value lies for both users and producers. Gartner has estimated that the worldwide business intelligence and data analytics market will reach $16.9 billion by the end of 2016 [23].

3.2 Data Outputs

In Section 2.2 we saw how the 130 year-old industrial company, Bosch has built its own IoT cloud service and is connecting its entire product range, allowing its customers to monitor and control Bosch products from their phones. In the UK, domestic goods manufacturer, Dyson appears to be adopting a similar strategy. In March 2016 it announced a range of air purifying devices which would have online connectivity via the Dyson Link phone app built into it. This marks a move for the company into providing information services:

> "The app will allow Pure Cool Link owners to monitor the air quality, temperature and humidity within the home, set air quality limits, see air quality history and start the fan remotely or on a schedule to clean up the air." [24]

While this information may be useful for individual domestic users to track the air quality in their homes, it is the aggregation of this data which may provide real value for Dyson. If the app is widely used within millions of households the data being collected by the company could be valuable to a variety of third parties from public health bodies to organisations wishing to sell on other services.

Google's success is built on the aggregation of billions of data points about our search habits which it sells on to advertisers. Google's parent company, Alphabet, on the 8 April 2016 had a stock market valuation of $522 billion [25]. Approximately 90% of the company's revenues are derived from advertising showing how the "data exhaust" of something as innocuous as web searching can be monetized when it is collected at scale.

The importance of scale as a value-adding factor for data sets can also be seen with another Google product, Google Maps. At a basic level, Google Maps operates like any other satellite navigation

[23] Gartner, "Gartner Says Worldwide Business Intelligence and Analytics Market to Reach $16.9 Billion in 2016," February 3, 2016, http://www.gartner.com/newsroom/id/3198917.

[24] Samuel Gibbs and Damian Carrington, "Dyson Launches Pure Cool Link Air Purifier to Clean up Household Air," *The Guardian*, March 31, 2016, sec. Technology, https://www.theguardian.com/technology/2016/mar/31/dyson-pure-cool-link-air-purifier-wi-fi-internet-of-things.

[25] Google Finance, "Alphabet Financials," April 8, 2016, https://www.google.com/finance?q=google&ei=ZXMHV7H-JMbKU83cg4AI.

system by linking map data with the GPS coordinates of the user. However, by combining internet connectivity with the movements of the more than 1.5 billion users of its mobile operating system, Android has added a new layer of value. By tracking the movements of Android phones users, Google is able to provide real-time traffic updates to its Map's users showing where delays are on the roads ahead and offering re-routing advice to optimize journey times [26].

The move into building data services alongside more traditional product ranges is exemplified by the US sportswear company, Under Armour. In 2015, Under Armour bought two fitness tracking app companies, MyFitnessPal and Endomondo for more than $500 million [27]. These acquisitions gave the company access to the health and fitness data of approximately 120 million users across Europe and the US. While the user bases of these apps provide obvious marketing opportunities for a sportswear company it is the aggregation of the data which monitors the health status of millions of amateur athletes along with their dietary habits which may offer the real value.

The success of these services point the way to how value may be extracted from future IoT data sets but also raises issues of personal privacy and data ownership.

3.3 Data Ownership

Most people are aware that companies like Google and Facebook make their money by collecting and monetizing their personal data. It is a generally accepted trade-off that, in exchange for the convenience of efficient web searching and keeping up with our friends online, we are prepared to give up some of personal privacy. However, there are signs that this mutual understanding may be coming under strain. As personal data becomes more valuable to those collecting it, users, regulators and pressure groups are starting to question what rights the individual has in controlling who is able to access information about their online and offline habits. IBM's $2.6 billion purchase in early 2016 of Truven Health Analytics, a holder of the health records of more than 200 million patients in the US demonstrates the hunger for data which technology companies have [28].

In Europe, data protection legislation is designed to give individuals rights over what can and cannot be done with their personal data and places obligations on organisations which hold this data. Tensions arise, however, as technology moves faster than legislators and organisations operating outside the EU are often subject to less stringent oversight. With companies such as Google, Facebook and Apple operating from the US, the ability of the EU to enforce data protection legislation is limited to a so-called "safe harbor" agreement whereby US companies agree to comply with aspects of EU legislation. These have recently come under strain with a ruling from the

[26] James Guszcza, Harvey Lewis, and John Lucker, "IoT's about Us: Emerging Forms of Innovation in the Internet of Things," *Deloitte Review*, no. 17 (2015): 66–83.

[27] Sara Germano, "Under Armour Acquires MyFitnessPal for $475 Million," *Wall Street Journal*, February 4, 2015, sec. Business, http://www.wsj.com/articles/under-armour-to-acquire-myfitnesspal-for-475-million-1423086478.

[28] Steve Lohr, "IBM Buys Truven for $2.6 Billion, Adding to Trove of Patient Data," *The New York Times*, February 18, 2016, http://www.nytimes.com/2016/02/19/technology/ibm-buys-truven-adding-to-growing-trove-of-patient-data-at-watson-health.html?nytmobile=0.

European Court of Justice that this agreement is not valid [29]. A legal resolution to this will no doubt be found as too much is at stake in terms of the ability of European citizens to use services from Google, Facebook and other technology companies. However, it raises broader questions about data ownership in a future IoT world where both the granularity and breadth of personal data collected on individuals exponentially increases.

At the moment there is a sense that the scales are tipped in favour of the companies collecting the data as they have the technical skills to manage it and the financial incentive to monetize it. However, it is possible that solutions may be found to allow individual users to also gain a financial benefit from selling their data to interested third parties rather than simply giving it away [30] [31]. The technical challenge of building and running such a system would be immense and it is not clear that enough individuals care enough to drive such an initiative forward. However, if "personal data is the new oil of the internet" [32] then ownership rights will need to be agreed and formalized in law in the same way they have been for physical assets for many centuries.

Perhaps part of the answer lies in the evolution of data exchanges which can act as clearing houses for all types of data being spun out from the IoT [33]. Initially, these would be focused on the needs of commercial entities which have the resources, knowledge and financial incentive to trade data across them. However, if these exchanges become established parts of the IoT value chain then it is possible they could be used by individuals to make money from their personal data.

4. Security and the IoT

Security is obviously an issue for all aspects of the internet both at the commercial but also the personal level. While it is impossible to know the exact figures, it has been estimated there are more than 90 million cyber-attacks on organisations each year costing a total of $575 billion [34]. In a world potentially moving from 5 billion connected devices in 2015 to 25 billion by 2020, the growing risk of security breaches is obvious [35].

[29] Samuel Gibbs, "What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?," *The Guardian*, October 6, 2015, sec. Technology, https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

[30] Jaron Lanier, *Who Owns The Future?* (Penguin, 2014)

[31] Afra Mashhadi, Fahim Kawsar, and Utku Gunay Acer, "Human Data Interaction in IoT: The Ownership Aspect," in *2014 IEEE World Forum on Internet of Things* (IEEE, 2014), 159–62, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6803139.

[32] Klaus Schwab et al., "Personal Data: The Emergence of a New Asset Class" (World Economic Forum, 2011).

[33] Jim Morrish, "The Emergence of Data Service Exchanges: Liquidity for the IoT" (Machina Research, 2015).

[34] "The Cost of Immaturity," *The Economist*, November 7, 2015, http://www.economist.com/news/business/21677639-business-protecting-against-computer-hacking-booming-cost-immaturity.

[35] Gartner, "Gartner Says 4.9 Billion Connected," 2014, http://www.gartner.com/newsroom/id/2905717.

4.1 Points of Failure

As more devices become connected to the internet the scope for hackers to find weak points through which to steal or compromise data also increases. This is exacerbated by the entry of device manufacturers into the IoT marketplace which have no previous experience in building secure, connected "things". On top of this is the issue of irregular or even non-existent firmware updates. As software becomes embedded in devices from door locks to thermostats, it is becoming apparent that security will be a key concern of the IoT. Even technology giants such as Apple have been known to sell products with software vulnerabilities:

> "In 2011, security researcher Charlie Miller found that chips in Apple laptop lithium ion batteries were shipped with default passwords, allowing anyone who discovered the password and learned how to manipulate the firmware to potentially install malware that infects the computer and gives a hacker a persistent hold on it even after the operating system is reinstalled. To demonstrate the firmware vulnerability, he altered the firmware of Apple laptop batteries to trick them into reporting a low charge that would cause the charger to overcharge them until they were bricked." [36]

While Apple has addressed the issue described above, other companies building household IoT devices are still producing vulnerable products. A fundamental point of weakness for the smart home is that it is only as secure as its weakest point. A recent demonstration of the ease with which a smart kettle could be remotely hacked and then used as a Trojan horse to access other devices within the same home was shown by security expert Ken Monro in London:

> "So I can sit outside of your place with a directional antenna, point it at your house, knock your kettle off your access point, it connects to me, I send two commands and it discloses your wireless key in plain text." [37]

While an insecure kettle may be a security hazard the data which could be taken from it is not particularly sensitive. However, other connected devices within the home do transmit very private data which users would not want "leaking" out onto the public internet. Recent examples of baby monitoring devices being easily hacked with live streams of sleeping babies being posted online by hackers as well as voices of strangers being transmitted back to the children do raise serious concerns for privacy and personal safety [38].

[36] Kim Zetter, "Why Firmware Is So Vulnerable to Hacking, and What Can Be Done About It," *WIRED*, February 24, 2015, http://www.wired.com/2015/02/firmware-vulnerable-hacking-can-done/.

[37] Darren Pauli, "Connected Kettles Boil Over, Spill Wi-Fi Passwords over London," *The Register*, October 19, 2015, http://www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots/.

[38] Eleanor Ross, "Voices Heard Coming from Baby Monitors as Parents Are Warned of Hacks," *The Independent*, January 30, 2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked-parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html.

4.2 Security Solutions

More than 60 years of computing have shown that hackers will always find a way to break into systems whether at home or in the workplace. A common approach is still the use of phishing attacks where users are tricked into clicking on insecure links in emails and websites or persuaded to give out personal information such as user names and passwords. Education plays a part in preventing such attacks and anti-virus software is widely used across all computing platforms.

However, where devices such as smart kettles, door locks, thermostats and security cameras are set up once by humans and then left to run independently the scope for malicious activity to be successful increases.

Security advisors, not surprisingly, recommend that we make sure all our connected devices have the latest firmware updates and security patches installed. However, the reality of the situation makes this complex and, in some cases, impossible. If suppliers do not release software updates in time or go out of business then malicious hackers will find it much easier to compromise systems. In the home, the development of smart hubs from large vendors like Google, Apple, Amazon and Samsung may point the way to a more secure smart home. These could utilize strong authentication and encryption technologies as well as security monitoring to track possible vulnerabilities on the network. However, the reality is that security will be one of the key issues facing IoT developers and, unless viable solutions are found, will hinder the diffusion of this emerging technology across the home and workplace.

5. The Future of the IoT

> "Given no one a few decades ago successfully predicted how the world would be today, we might wonder whether we have any hope of predicting how it will be 10, 20 or 50 years from now. Yet we are compelled to try. We are not passive observers of an unfolding drama, but actors shaping the story — and with a strong interest in how it turns out." [39]

Predicting how the technological landscape will evolve over the longer terms if generally a futile exercise. The rapid and unforeseen rise of the internet as a consumer-oriented network caught most analysts and telecommunication companies off-guard in the early 1990s. The pervasive diffusion of mobile phones beyond business users a few years later was similarly unexpected. However, while predicting the specific characteristics of new technologies and which ones will succeed in the marketplace is an inaccurate science, there are some lessons from history which can help us understand which business strategies might be appropriate in a rapidly evolving sector such as the IoT.

[39] Stephen Cave, "Is Predicting the Future Futile or Necessary?," *Financial Times*, January 8, 2016, http://www.ft.com/cms/s/2/5815c14a-b2e7-11e5-b147-e5e5bba42e51.html.

5.1 Platforms, Standards and Consortia

Just as Microsoft and Intel created the PC as a platform for innovation in the 1980s and 1990s so Google and Apple have created mobile phone platforms over the last decade which are driving a new generation of software innovation [40]. The objective for these companies is build a technological platform, combining hardware and software, in a way which gives them control over its direction of development but is also open enough and provides the financial incentives to encourage third parties to build applications to run on top of the platform.

This strategy is being applied by a number of companies in the race to build IoT platforms for the home. At the software level, Apple has adopted a more proprietary model with its HomeKit platform which requires third parties to be certified for their devices to run on it. Google has adapted its Android operating system to create Brillo, a more open platform which the company hopes will be as successful as Android has been for smart phones. Samsung has its SmartThings hub which aims to allow devices from a range of other companies communicate with each other, avoiding the need for multiple home hubs and conflicting communication protocols. It is far too early to see which, if any, of these platforms will succeed. Opinion is divided whether Google will maintain Brillo as an open platform if it becomes successful [41] and there are technical questions surrounding the ability of Samsung to create a secure and reliable central IoT hub for the home [42]. IoT initiatives across the industrial sector are the scene of commercial battles and competing consortia to establish dominance in both the communication protocols linking devices as well as the backend software platforms where the analysis of the captured data takes place. Figure 1 presents a simplified model of the technology stack underpinning the IoT and some of the specific applications sitting on top of it.

The diverse nature of the IoT and the way it cuts across domestic and industrial boundaries means there will not be a single platform or company which dominates the entire sector. Some companies will succeed in particular industry verticals where they already have experience or are able to offer a

[40] Gawer, *Platforms, Markets and Innovation*; Annabelle Gawer and Michael A. Cusumano, "Industry Platforms and Ecosystem Innovation," *Journal of Product Innovation Management* 31, no. 3 (May 1, 2014): 417–33, doi:10.1111/jpim.12105; Annabelle Gawer and Michael A. Cusumano, *Platform Leadership: How Intel, Microsoft and Cisco Drive Industry Innovation* (Boston, MA: Harvard Business School Press, 2002).

[41] Stephen Glasskeys, "3 Reasons IoT Developers Should Steer Clear of Brillo OS," *ITworld*, June 23, 2015, http://www.itworld.com/article/2938527/operating-systems/three-reasons-iot-developers-should-steer-clear-of-brillo-os.html.

[42] Jacob Kastrenakes, "This Is Samsung's Grand Vision for the Internet of Things," *The Verge*, January 5, 2015, http://www.theverge.com/2015/1/5/7497537/samsung-iot-internet-of-things-vision-presented-at-ces-2015-keynote.

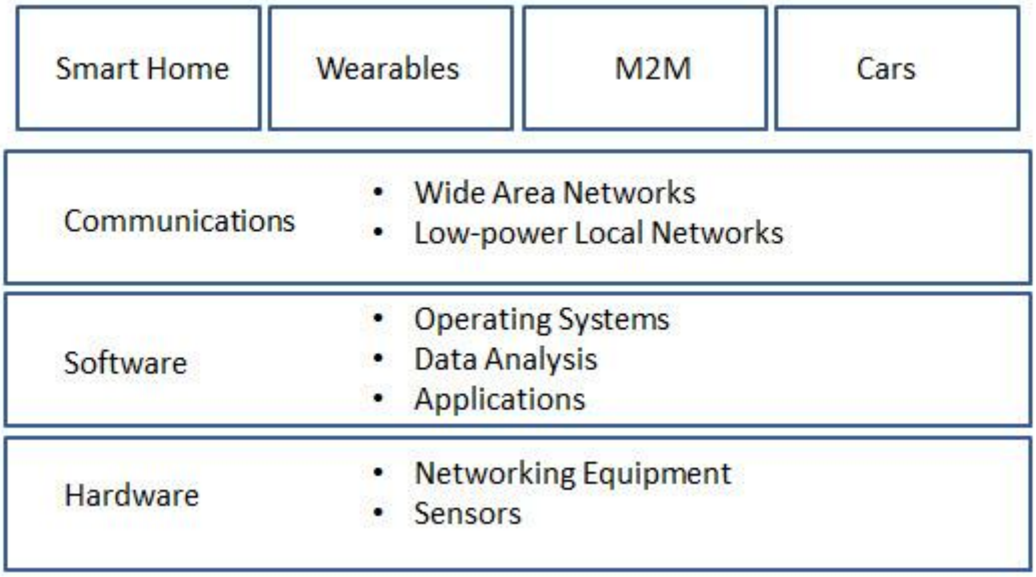

Figure 1. IoT Technology Stack

competitive advantage to their users while others will be able to lock users in to their software platforms or be able to differentiate their hardware through branding and functionality in a crowded marketplace.

5.2 Conclusion

This paper has provided an overview of some of the key current developments in the emerging IoT field of technologies. It is apparent that the term IoT is broad and, in some ways, not always helpful in describing a very broad and diverse set of technologies at the hardware, software and communication levels. In 2015, Gartner placed the IoT at the top of its annual Technology Hype Cycle, arguing that it was riding the "Peak of Inflated Expectations" [43]. There is undoubtedly some truth that a number of analysts and vendors have made overblown claims for the IoT as a technological fix for all manner of industrial and domestic problems. However, the reality is more nuanced and complex than either the boosters of the naysayers would have us believe. The technologies and applications described in this paper point the way to an emerging revolution in the ways that computing technologies are helping us better understand our environment. As sensors become embedded in and on our bodies, homes, workplaces and cities, the data they generate will have the potential to transform our lives. The extent to which this is for the common good will depend on who controls this data, how it is used and what safeguards are put in place to protect privacy.

[43] Gartner, "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor," August 18, 2015, http://www.gartner.com/newsroom/id/3114217.

6. Concluding Thoughts for Libraries

This White Paper has focused on the IoT in a general sense and explored some of the key technologies and companies driving its development. However, it is worth briefly considering how libraries and information professionals across the public and private sectors might be affected by the IoT. Section 3 showed how the demand for data is driving most IoT initiatives and discussed the implications of this for those expert in understanding and manipulating large data sets. At the institutional level, libraries themselves are experimenting with a range of IoT-related technologies. As was previously mentioned, libraries along with large companies such as P&G were early adopters of RFID chips for inventory management.

At a generic level, library buildings stand to benefit from the implementation of IoT technologies to building management systems whereby the monitoring and control of physical environments can be improved by better data collection. More specifically, the installation of pressure sensitive pads under library flooring could allow the tracking of users as they pass through the building and help build a data map of popular routes and potential bottlenecks [44]. Just as Disney now offers visitors to its theme parks smart wrist bands fitted with Near Field Communication (NFC) chips which allow for cashless purchases and access control, so libraries might want to experiment with this technology to encourage younger users to make better use of their services [45]. iBeacon transmitters which utilize Bluetooth Low Energy (BLE) technology are being deployed across a range of physical retail environments to offer shoppers special deals as they pass through stores. A number of libraries are already experimenting with this technology to enhance the information available to users when they visit the library [46].

These are just a few examples of how some of the current technologies which form part of the IoT ecosystem are currently or could be deployed to enhance library services. As with most other IoT technologies, they are at an early stage but point the way to how the IoT could help make connections between the physical environment of the library and the digital needs of users.

[44] Sean Voisen, "Designing a Pressure-Sensitive Floor," *Sean Voisen Blog*, August 12, 2013, http://sean.voisen.org/blog/2013/08/designing-pressure-sensitive-floor/.

[45] Sheli McHugh and Kristen Yarmey, "Near Field Communication: Recent Developments and Library Implications," *Synthesis Lectures on Emerging Trends in Librarianship* 1, no. 1 (March 2014): 1–93, doi:10.2200/S00570ED1V01Y201403ETL002.

[46] Sidney Eng, "Connection, Not Collection: Using iBeacons to Engage Library Users," *Information Today*, December 2015, http://www.infotoday.com/cilmag/dec15/Eng--Using-iBeacons-to-Engage-Library-Users.shtml.