Government
Office for Science

The Internet of Things: making the most of the Second Digital Revolution

A report by the UK Government Chief Scientific Adviser

Contents

Foreword

It is clear that we live in a world of permanent technological revolution. Countries like the UK will only succeed if we show a relentless drive for leadership and innovation.

At the CeBIT trade fair in March 2014, I restated my ambition to make the UK the most digital nation in the G8. Part of achieving that goal is making the very best of today's digital technology. But it also means being ahead of the curve for tomorrow's.

That is why I asked Sir Mark Walport, the Government's Chief Scientific Adviser, to write this review.

The Internet of Things is a transformative development. Technologies that could allow literally billions of everyday objects to communicate with each other over the Internet have enormous potential to change all of our lives.

These technologies are a way of boosting productivity, of keeping us healthier, making transport more efficient, reducing energy needs and making our homes more comfortable.

Electricity meters that talk to the grid to get you the best deals. Health monitors that keep an eye on your heart rate. Cars that avoid congestion further up the motorway.

As this review rightly makes clear, this is not the time to get carried away with potential. Delivering on this opportunity will require a lot more hard work, creativity and leadership. The UK government, working with business, the research community and the public, stands ready to provide it.

We are on the brink of a new industrial revolution. I want the UK to lead it.

Rt. Hon David Cameron MP

Executive summary

The Internet of Things describes a world in which everyday objects are connected to a network so that data can be shared. But it is really as much about people as the inanimate objects. Many millions of us already carry ‘smart’ phones in the UK but a phone is not smart. It helps its user to make smarter decisions.

Smartphones are only the beginning. In the future we will carry sensors that measure our health and how we move around the environment in which we live. These will help us to socialise and navigate the world in ways that we can barely imagine.

There is a danger of trivialising the importance of the Internet of Things through examples that are used to stereotype it - for example, the ‘fridge that orders fresh milk’. The Internet of Things has the potential to have a greater impact on society than the first digital revolution.

There are more connected objects than people on the planet. The networks and data that flow from them will support an extraordinary range of applications and economic opportunities. However, as with any new technology, there is the potential for significant challenges too. In the case of the Internet of Things, breaches of security and privacy have the greatest potential for causing harm.

It is crucial that the scientists, programmers and entrepreneurs who are leading the research, development and creation of the new businesses implement the technology responsibly. Equally, policy makers can support responsible innovation and decide whether and how to legislate or regulate as necessary. Everyone involved in the Internet of Things should be constantly scanning the horizon to anticipate and prevent, rather than deal with unforeseen consequences in retrospect.

At the 2014 CeBIT Trade Fair in Hanover, the Prime Minister commissioned the Government Chief Scientific Adviser to review how we can exploit the potential of the Internet of Things. An advisory group, seminars and evidence from more than 120 experts in academia, industry and government have informed this review.

Vision

Our first two recommendations are about leadership.

Recommendation 1: *Government needs to foster and promote a clear aspiration and vision for the Internet of Things. The aspiration should be that the UK will be a world leader in the development and implementation of the Internet of Things. The vision is that the Internet of Things will enable goods to be produced more imaginatively, services to be provided more effectively and scarce resources to be used more sparingly.*

Achieving this vision will deliver significant economic and societal benefits over the next 10 years. The Internet of Things creates enormous opportunities for the private sector and government should do only what government needs to do. This leads on to the second recommendation of the review:

Recommendation 2: *Government has a leadership role to play in delivering the vision and should set high ambitions. Government should remove barriers and provide catalysis.*

There are eight areas for action:

- Commissioning
- Spectrum and networks
- Standards
- Skills and research
- Data
- Regulation and legislation
- Trust
- Co-ordination.

Commissioning

Government is committed to the increased delivery of services using the most efficient and effective technology - and digital technologies are at the forefront. In this role government is an important purchaser of technology and has the opportunity to encourage innovation by expert commissioning of products and services.

Recommendation 3: *Government must be an expert and strategic customer for the Internet of Things. It should use informed buying power to define best practice and to commission technology that uses open standards, is interoperable and secure. It should encourage all entrants to market; from start-ups to established players. It should support scalable demonstrator projects to provide the environment and infrastructure for developers to try out and implement new applications.*

Government departments should be prepared to take appropriate risk by supporting demonstrator projects. These must be scalable and security should be an integral part of their design. They should go beyond simple deployments of commercially available technology. Departments should recognise that the market for Internet of Things applications will be shaped by disruptive small enterprises, as well as by large companies. In order to fulfil their potential, these projects will require a culture of innovation, testing, learning and scaling.

Pilot programmes that receive public financial support should produce open data for use by all as frequently as possible. Government should not attempt to anticipate a single 'killer app' or every possible use for the Internet of Things, but should use demonstrator projects as tools to frame public conversations about these technologies and how to embed best practice.

The Milton Keynes smart city, funded by Innovate UK, is a good example of this approach. It is currently testing Internet of Things applications to support better public services for citizens. Government could explore opening up this, and similar pilots, to enable companies and individuals to develop applications or deploy devices. There is a powerful opportunity for crowd-sourced innovation. The NHS, in particular, should facilitate improvement in health and social care provision, efficiency and accountability by expert commissioning and rewarding innovative health and social care providers. Other sectors offer similarly attractive opportunities, obvious examples being energy and transport.

Spectrum and networks

It is too early to be certain of the exact network requirements created by Internet of Things technologies. Many applications use relatively small amounts of bandwidth and can innovate within existing spectrum bands. However, existing mobile or Wi-Fi networks may not always be suitable for millions of sensors requiring low power to communicate small amounts of data. The UK may therefore need a stable, low power, wide area network to supplement the existing fibre infrastructure.

Recommendation 4a: *Government should work with experts to develop a roadmap for an Internet of Things infrastructure.*

As the network infrastructure for the Internet of Things will be delivered by diverse providers, there is a risk that this will result in independent, fragmented or partial networks, damaging connectivity with the potential to reduce network resilience. This is the case for mobile phone networks, in which two people standing side by side have access to different networks, (according to their network provider) with widely different signal strengths. In contrast, retail banks have collaborated so that the holder of a credit or debit card can obtain cash from the cashpoint of any of the major UK retail banks.

Recommendation 4b: *Government should collaborate with industry, the regulator and academia to maximise connectivity and continuity, for both static and mobile devices, whether used by business or consumers.*

Government could consider selling licensed spectrum space for the Internet of Things to guarantee future capacity and provide a source of funding.

Standards

Standards play a central role in enabling the creation of markets for new technologies. As is typical for emerging technologies, commercial partnerships are driving competing standards for the Internet of Things. Left unchecked, this carries a risk of restrictive standards being set and enforced by monopolistic providers, and of fragmentation inhibiting the interoperability of devices, slowing growth and reducing the opportunities for entrepreneurs.

For the Internet of Things to flourish, interoperability must apply across all parts of the system, including the transmission networks and the data being transmitted. Data and devices must have proportionate "security by default". Standards must protect against cybercrime and national security threats, and help to ensure that the system is trustworthy and trusted. They should also support energy efficiency, as this will help increase the range of potential applications and manage the burden on energy supply.

Government can shape standards and support new market entrants through its commissioning practices. Funding scalable demonstrators is an excellent way both to enable innovators to develop new business models rapidly, and to ensure that standards are fit for purpose. This report outlines examples of potential opportunities, by sector, in chapter four.

Although the UK cannot unilaterally adopt a standard and hope for global consensus, a clear government position will give companies and consumers confidence in the UK market. Government should play a leading role in seeking to achieve wider consensus with other governments and standards bodies, and could host international events to seize the initiative and demonstrate UK leadership.

Recommendation 5: *With the participation of industry and our research communities, Government should support the development of standards that facilitate interoperability, openness to new market entrants and security against cybercrime and terrorism. Government and others can use expert commissioning to encourage participants in demonstrator programmes to develop standards that facilitate interoperable and secure systems. Government should take a proactive role in driving harmonisation of standards internationally.*

Skills and research

There are important opportunities for government to be catalytic in the development of skilled people. A broad range of skills will be key to the design, development, installation and maintenance of the Internet of Things. For example, there is a shortage of technically adept installers who have hybrid skills as electricians and IT technicians. System architects, who can apply knowledge of advanced digital technology to classical engineering challenges, will be essential. We need highly educated and qualified researchers and developers across multiple disciplines to create the applications that will deliver greatest benefit to users.

Computational thinking and interpreting evidence should be an essential part of the education curriculum, building skills and helping people to make informed decisions about everyday use of the Internet of Things. Computer programming, including rigorous study of algorithms and representations of data, underpins the specialist skills needed. These must be integrated into learning at school and in tertiary education and training.

The Civil Service itself needs skilled people if it is to be an expert customer and enabler of these technologies, and should accelerate efforts to increase digital, data and technical capability as part of the next phase of Civil Service reform.

Recommendation 6: *Developing skilled people starts at school. The maths curriculum in secondary school should move away from an emphasis on calculation per se towards using calculation to solve problems. Government, the education sector and businesses should prioritise efforts to develop a skilled workforce and a supply of capable data scientists for business, the third sector and the Civil Service.*

Data

Government has made important progress on open data. However, much of the data released to date is enabled to be human-readable, and not machine-readable. Government should ensure that all public bodies and regulated industries are mandated to publish reliable machine-readable data through open application programming interfaces, subject to appropriate data protection safeguards. Data held by the Office for National Statistics could be an important test case.

Government should also consider policy to protect the UK from data monopolisation in private companies, particularly where this may harm consumers or suppress innovation.

Recommendation 7: *Open application programming interfaces should be created for all public bodies and regulated industries to enable innovative use of real-time public data, prioritising efforts in the energy and transport sectors.*

Regulation and legislation

Legislation should be kept to the minimum required to facilitate the uptake of the Internet of Things. It should enable more efficient public and private services in areas such as healthcare, energy and transport, and should aim to minimise threats and harms.

However, the introduction of Internet of Things technologies is likely to create new regulatory challenges in some areas of government policy. For example, the introduction of autonomous vehicles may significantly reduce road traffic incidents, but is unlikely to eliminate them completely. New questions of liability and protections for citizens and businesses will inevitably arise. Resolving these questions will be a critical factor to enable the introduction of more radical opportunities and may pose novel regulatory and governance challenges.

The Internet of Things already poses challenges in the sensitive area of personal identity and privacy. The scale of personal information, particularly locational and financial information, which is collected by existing technology, is huge. This data collected will only increase as we use more and more Internet of Things technologies. This is an area that is already covered by both legislation and regulation. The Information Commissioner will need to maintain the necessary capacity to handle the challenges of balancing benefits and harms in the area of personal data.

Good regulation and legislation will be needed to anticipate and respond to new challenges. Government should ensure that it is considering carefully and systematically the impact of emerging technologies in policy, delivery and operational planning.

Recommendation 8: *Government should develop a flexible and proportionate model for regulation in domains affected by the Internet of Things, to react quickly and effectively to technological change, and balance the consideration of potential benefits and harms. The Information Commissioner will play a key role in the area of personal data. Regulators should be held accountable for all decisions, whether these accelerate or delay applications of the Internet of Things that fall within the scope of regulation.*

Trust

Public acceptability and trust are central to the implementation of the Internet of Things. Public debate often centres on privacy concerns and information security but new targets for criminal subversion and terrorism will also be created. Like any new technology it should not be considered generically as 'good' or 'bad'. Each use needs to be considered specifically. In the future, the issue will be less about whether people 'trust' the Internet of Things but instead whether the private and public sector providers and operators demonstrate that they are trustworthy.

A major data breach or cyber-attack is likely to have extremely damaging consequences on public attitudes. Therefore, data governance and security considerations are not optional extras but should be considered at the beginning, and throughout the lifecycle of Internet of Things applications. It will be essential to have guidelines on the use and handling of the data generated.

Recommendation 9: *The Centre for Protection of National Infrastructure (CPNI) and Communications and Electronics Security Group (CESG) should work with industry and international partners to agree best practice security and privacy principles based on "security by default".*

All participants in this disruptive technological revolution should foster public discussion and debate. Government has no exclusive role here but should play its part in the public debate.

It should not be forgotten that almost a quarter of UK adults do not use the Internet on a daily basis. Assisted digital and digital inclusion programmes should be expanded to ensure that these include the risk of the Internet of Things deepening "digital disenfranchisement".

Coordination

Clear external communication of the vision for the Internet of Things by Government, coupled with the provision of a stable policy environment, are important to facilitate private sector investment. Equally important is a shared vision and cross-governmental co-ordination of policy development and support. All parts of government will be affected by the Internet of Things and have a role in its effective implementation. Therefore, careful oversight is needed to coordinate funding and support of the relevant technologies.

Innovate UK, Engineering and Physical Sciences Research Council (EPSRC), the Digital Economy Catapult and Tech City are all making important contributions to develop the complex ecosystem of the Internet of Things. These and organisations in the private sector must talk to each other and wherever possible co-ordinate their activities and funding. In the nuclear industry, Nuclear and Innovation Research Advisory Board (NIRAB), is starting to revolutionise the co-ordination of the sector.

Recommendation 10: *The Digital Economy Council should create an Internet of Things advisory board, bringing together the private and public sectors. The board would have a remit to: co-ordinate government and private sector funding and support of* *the relevant technologies; foster public-private collaboration where this will maximise the efficiency and effectiveness of implementation of the Internet of Things; work with government to advise policymakers when regulation or legislation may be needed; maintain oversight and awareness of potential risks and vulnerabilities associated with the implementation of the Internet of Things; and promote public dialogue. To be effective this board should be supported by an adequately funded secretariat.*

We are on the verge of an extraordinary revolution in which the digital world becomes completely embedded throughout the manufactured and engineered products on which advanced societies depend. These products are the descendants of the manufactured goods from the first industrial revolution. The role of a small number of enlightened engineers and manufacturers in the UK in the creation of the industrial revolution is uncontested. Nearly three centuries later, in a very different world, there is the opportunity for our best educators, scientists, engineers, designers and manufacturers to collaborate to ensure that the UK plays a leading role in the next industrial revolution.

About this review

This review has three main objectives. The first is to explain what government can do to help achieve the potential economic value of the Internet of Things. The second is to set out what Internet of Things applications can do to improve the business of government – maintaining infrastructure, delivering public services and protecting citizens. The third is to distil this evidence into a set of recommendations.

To illustrate the opportunities and threats, the review sets out the implications of applying Internet of Things technologies in a selection of major economic sectors. These have been selected on the grounds of their relevance to government. They are not intended to be a comprehensive list of the technologies' possibilities.

The Prime Minister commissioned this review from the Government's Chief Scientific Adviser, Sir Mark Walport. Experts from academia, industry, think tanks and government have contributed. Ministers with a specific policy interest were also invited to comment on the review's scope and recommendations prior to publication.

The recommendations set out in this review are primarily for government to take forward. However, successfully delivering them will require a close partnership with industry, the UK research base, the public, other national governments and international organisations.

The Internet of Things has an extremely broad definition and many links to other emerging technologies, such as robotics, data analytics and artificial intelligence. This review does not attempt to describe all these in detail but notes that government needs to take a similarly far-sighted approach to all of them.

FIGURE 1:
Internet of Things: review in numbers

CHAPTER 1: The ecosystem

The Internet of Things is not a new concept. The term was coined in the late 1990s, and many of the essential components like semiconductors and wireless networks have existed for decades.

The Internet of Things is made up of hardware and software technologies. The hardware consists of the connected devices – which range from simple sensors to smartphones and wearable devices – and the networks that link them, such as 4G Long-Term Evolution, Wi-Fi and Bluetooth. Software components include data storage platforms and analytics programmes that present information to users. However, it is when these components are combined to provide services that real value is created for businesses, consumers and governments. Some of these are discussed in chapter four.

Figure 2:
Internet of Things ecosystem

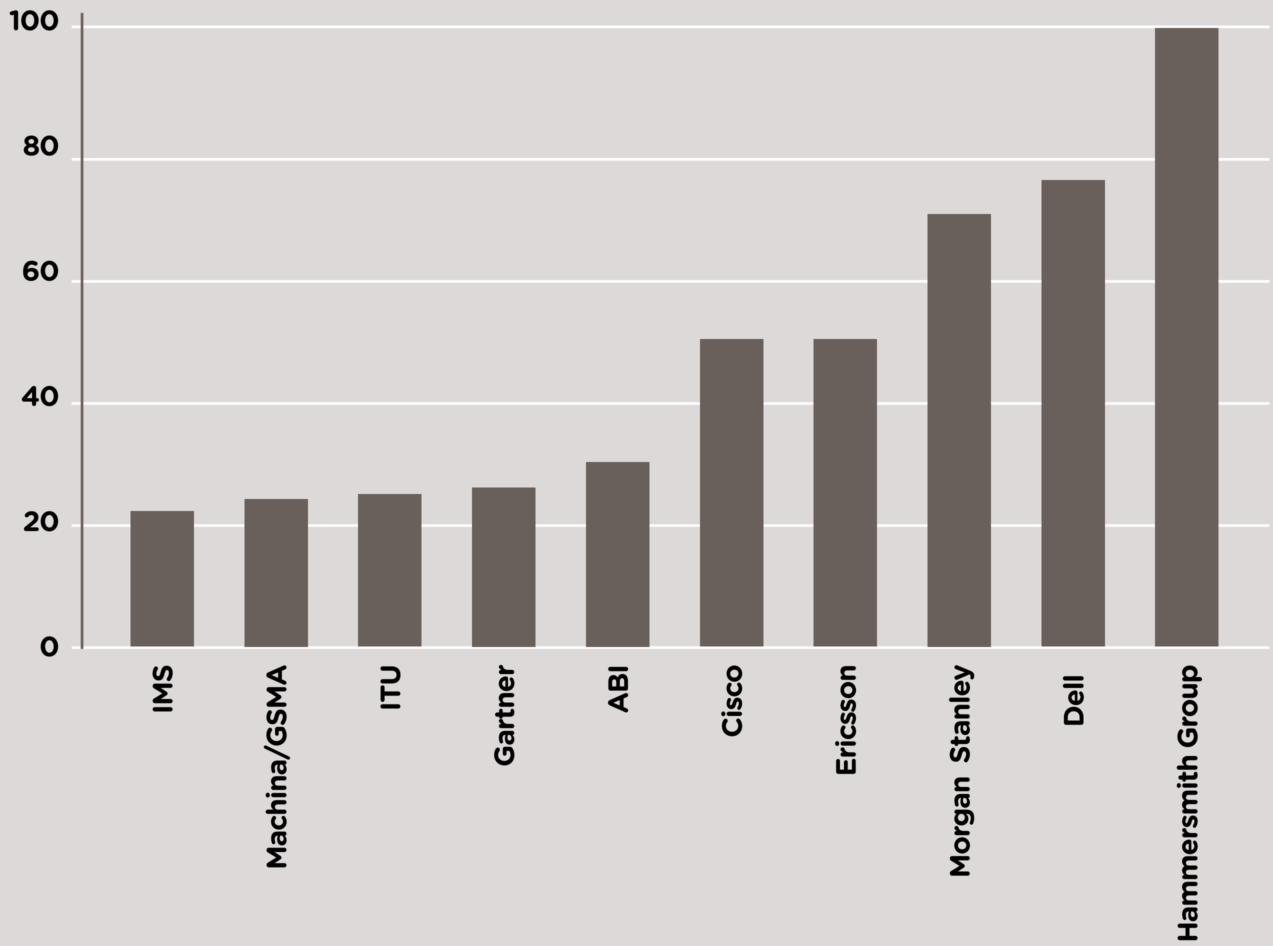
Today, there are about 14 billion objects connected to the Internet.[1] Industry analysts estimate the number of connected devices could be anywhere from 20 billion to 100 billion by 2020.

Mobile access to the Internet, coupled with the rapid growth of the smartphone market, has begun to create consumer demand for the Internet of Things. There are a number of underlying trends driving the new Internet of Things ecosystem.

Trends

The first significant trend is the availability of *cheaper semiconductors*.[3] Collecting complex and valuable data would not be possible without economically viable sensors, controllers and transmitters. For Internet of Things devices these chips also need to be small enough and powerful enough to blend invisibly into the physical world.

Figure 3:
Industry estimates for connected devices (billions) in 2020[2]

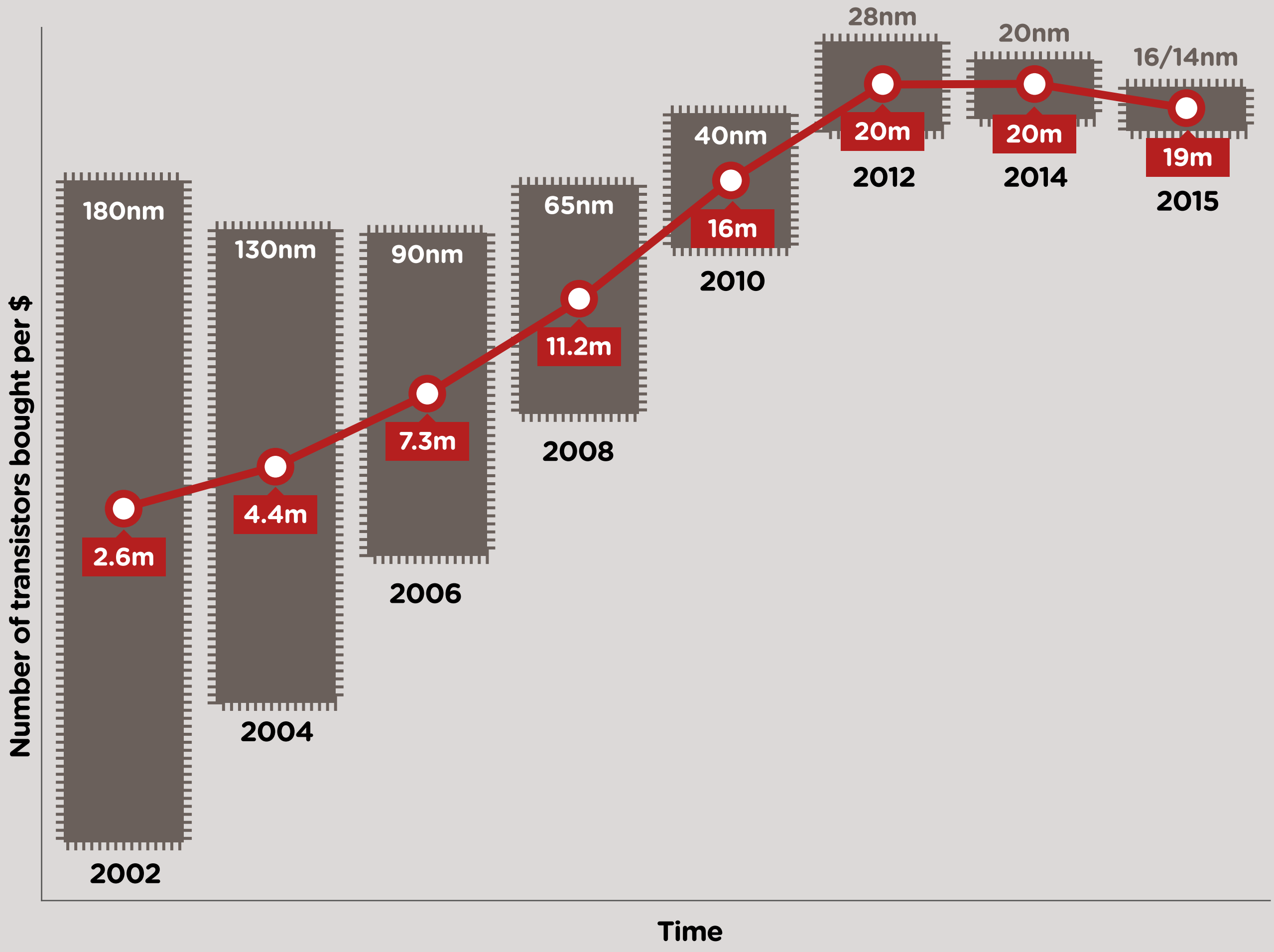


1 'Internet of Things Connections Counter', Cisco Systems, 2014
2 http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10; https://www.abiresearch.com/market-research/product/1016390-over-30-billion-wireless-connected-devices/; 'Forecast: The Internet of Things, Worldwide 2013', Gartner, 2013; 'The State of Broadband 2012: Achieving digital inclusion for all', Broadband commission, 2012; 'The Internet of Things: How the next evolution of the Internet is changing everything', Cisco Systems, 2011; 'Towards 50 Billion Connected Devices', Ericsson Research, 2010; 'The Internet of Things: Networked objects and smart devices', The Hammersmith Group, 2010; http://www.marketplace.org/topics/tech/indie-economics/2020-there-will-be-10-web-connected-devices-human; 'The Connected Life: A USD 4.5 trillion global impact in 2020', GSMA and Machina Research, 2012; http://www.itpro.co.uk/626209/web-connected-devices-to-reach-22-billion-by-2020
3 'The Internet of Things is Now', Morgan Stanley, 2014

Thanks to a huge demand for better microchips from the smartphone and tablet market, their cost has fallen significantly. Processors can be bought for $2, sensors for $1 and Bluetooth chips for even less.[5]

The second trend is *wider network availability* and increased capacity. Fixed line, wi-fi and mobile networks have expanded to meet the demands of the 2.3 billion Internet subscribers around the world.[6] The number of IP addresses available for devices to connect to the Internet has grown from 4 billion to 340 trillion, trillion, trillion in 35 years.[7] Wireless networks have opened up access to objects that could not have been connected in a static computing environment. In addition to the growing availability of wireless, fibre-optic broadband networks are steadily reaching more homes and businesses, increasing the bandwidth available.[8]

Figure 4
Moore's Law[4]
Number and length of transistors bought per $



4 http://hexus.net/tech/news/cpu/65901-arm-updates-midrange-cpu-roadmap-cortex-a17/
5 'The Internet of Things is Now', Morgan Stanley, 2014
6 'ICT Facts and Figures 2014', ITU, available from http://www.itu.int/en/ ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.
7 'Factsheet: IPv6 – The Internet's vital expansion', ICANN, 2007
8 'The Communications Market Report', Ofcom, 2014

The third trend is in *data management and storage*. For many years, data servers took up a large proportion of IT budgets. The rise of open-source software, commoditised hardware and cloud-based data storage has forced down costs, and made it simpler to keep and organise much larger datasets.

The fourth trend is the development of ever more *powerful analytics and applications*. New techniques and technologies have been developed to exploit the data bounty that has been created by the three preceding trends. Machine learning techniques and algorithms are becoming a business necessity in many industry sectors, enabling them to make sense of vast quantities of data in near real-time.

Uncertainties

Taken together, these trends have the potential to make the Internet of Things part of everyday life. However, it would be misleading to suggest that the future for these technologies is certain. Emerging technologies are subject to hype, and the implicit assumptions we make about how and when technologies develop should not be taken for granted. In fact, technology analysts Gartner suggest that the Internet of Things is currently at the 'peak of inflated expectations'.[9]

As with the Internet, applications of the Internet of Things are developing organically, with experimentation in every sector. The first source of uncertainty is that there are relatively *few established business models* for achieving profitability.[10] Until these become clear, it is reasonable to expect caution from businesses developing and buying these technologies. Early developments may come from industry giants with economies of scale that mean large investments for incremental benefits are viable. However, the existing information technology capability of many governments and large businesses is likely to be insufficient to harness the volume and variety of data generated by the Internet of Things.[11] Disruptive new firms may try to break into existing markets or create new ones through innovative new ideas.

A second source of uncertainty is the question of *standards*. There are not yet any clear 'winners' for interpreting the data from devices or for connecting them to one another. Competing platforms and industrial coalitions[12] are emerging; and there are many different infrastructures that will form Internet of Things networks.

This is a familiar position for an emerging technology at an early stage of development and there are two main risks. One is that a single organisation or group could drive anti-competitive standards for the entire ecosystem, reducing the potential economic benefit to society. The other is that unless dominant standards ultimately emerge, it will be very difficult for the system to achieve a framework that allows openness, interoperability and security.

The third source of uncertainty is *security and trust*. Given trends towards smaller and cheaper components, it is possible to imagine that almost any physical object could be connected to a network in the next decade. Whether such an outcome is desirable or necessary is a different question. It is highly likely that users will want some specific devices kept away from open networks for reasons of security, privacy or commercial sensitivity. The extent and nature of these 'off-grid' devices is very hard to predict.

9 'Hype Cycle for the Internet of Things, 2014', Gartner, 2014
10 'The Internet of Things Business Index: A quiet revolution takes place', The Economist, 2013
11 http://www.wireless-mag.com/Features/30805/iot-security-must-be-fixed-for-the-long-term-says-beecham-report-.aspx
12 For example: the Industrial Internet Consortium; Thread Group; Apple and IBM partnership; Android ecosystem.

Cyber security challenges are evolving quickly. Billions of additional connected devices in new locations and applications will create new challenges. Examples of connected devices being hacked are increasingly commonplace. Researchers carried out a cyber-attack that allowed them to control steering and braking of a car.[13] Security vulnerabilities were exposed in a baby monitor device, enabling the hacker to shout at a sleeping child.[14]

These new possibilities amplify existing problems. In the baby monitor case, it demonstrated that the owner failing to change the default password was a part of the device's vulnerability. The Internet of Things will also require complex systems to work together, designed and managed by different organisations. Today's threats, such as viruses and malware, could have even larger implications when it requires significantly more co-ordination and systems to patch the vulnerabilities they exploit.

Governments and agencies are already taking note. For example, the US Government Accountability Office has published a paper advising the US Food and Drug Administration to expand its consideration of Information Security for certain types of medical devices.[15] In the UK, GCHQ has conducted research that estimates that 80% or more of successful cyber-attacks could be defeated by implementing simple cyber security standards.[16] Straightforward measures such as regular security patches, firewalls and appropriate passwords all make a substantial contribution to reducing risk.

13 http://www.wired.com/2014/08/car-hacking-chart/
14 http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home
15 'Medical Devices: FDA should expand its consideration of Information Security for certain types of devices', GAO, 2012
16 http://www.gov.uk/government/speeches/karen-bradleys-speech-to-the-finance-services-cybercrime-summit

CHAPTER 2: Adopting the Internet of Things

The Internet of Things is as much about people as it is about technology. It is impossible to anticipate all the social changes that could be created by connecting billions of devices. The effects of the Internet of Things will depend on take-up by individuals, businesses and governments. These actors will be influenced by public perceptions of benefits and risks. The early involvement of publics can help developers and policymakers to understand and respond to their concerns. Using this evidence, the benefits and risks can be more carefully balanced

The importance of public perception on the successful adoption of emerging technologies is well documented.[17] In the case of technologies such as genetic modification and stem cell research, public debate has shaped markedly different regulatory environments across the world. This has allowed some countries to safely realise their potential more quickly than others.

Building support and addressing concerns

Research shows that support for technological and scientific advances is strongly influenced by the degree to which individuals believe that they or wider society would directly benefit.[18]

Even when a majority of people are convinced that a new technology can offer major benefits, many will also express concerns. Where people feel insufficiently informed to weigh up risks and benefits, they tend to be more polarised in their views.

Public perceptions of the Internet of Things are still developing, but evidence from public engagement studies into similar emerging technologies highlights recurrent themes that are likely to be relevant:[19]

- Concerns about privacy, safety and security and related demands for accountability and (anticipatory) governance.
- Desire for competition, choice (including opt-out choices) and questions of unintended consequences and liability.
- Clarity on who is in control and who is driving the development and direction of research.
- Consideration for the winners and losers from the introduction of technologies and concern if the changes are perceived to exacerbate inequality.

There are two major implications government can draw from analysis of previous experiences with new technology. The first is that early involvement in constructive dialogue on specific applications or specific problems that an applied technology could resolve are far more effective than discussing technologies in an abstract sense. Structured discussions can help scientists and policymakers understand different views, putting society's needs at the centre of technological development. There is evidence to suggest that deliberative dialogues on emerging technologies can help.[20]

The second implication is that any public conversation on the Internet of Things is likely to be more constructive if it is framed around issues that affect large sections of the population. Applications that tackle energy efficiency, transport systems or healthcare will aid constructive engagement more effectively than applications directed towards individuals, such as household appliances and the infamous connected fridge.

17 The Internet of Things: the case for public voice', ScienceWise, 2014
18, 19, 20 Ibid.

Changing mind-sets

Of particular importance are the closely related issues of privacy, safety and security to the safe uptake of the Internet of Things.

Although the Internet of Things can be conceived of billions of benign devices transmitting tiny amounts of data, value will be generated from aggregating and analysing large quantities of it. There is considerable research into novel techniques to secure connected devices, networks and data individually. However, protecting whole systems will become just as important as protecting individual components. In addition, people will be an integral part of those systems.

Many companies already buy and sell data about people's whereabouts, habits and preferences. For example, retail beacons interacting with mobile phones can track customers' movements around a store and offer them personalised discounts.[21] There are also isolated examples of controversial use of data, such as an online dating website selling data about people's drug and alcohol consumption.[22] As more and more data is aggregated it may reveal aspects of the individual, system or environment that may be unexpected or intended to remain private. For example, information extracted from a building's heating controls, lighting and sensors might reveal information about an individual, such as when they are in the building.

Fraudsters, activists and phishers are increasingly abusing weak security and poor security behaviours. The present and future value of data – and the inherent risks in handling it – will need to be carefully considered by the government, businesses and the public.

The kinds of potential risks created by the Internet of Things extend beyond nuisance hacks on personal data. Complex organised attacks on systems are also possible. The computer worm Stuxnet is a well-known example of the latter. It was designed specifically to attack an industrial control system operating Iranian fast-spinning centrifuges. Malicious code collected information and changed the behaviour of the system, causing the physical mechanism to tear itself apart.

Although the Stuxnet attack was an unusual case and not directly applicable to most UK infrastructure, it provided a vivid illustration of the malign possibilities in these technologies. Stuxnet has already changed mind sets, energising efforts in hunting out component vulnerabilities in systems by governments and businesses.

The scale of connectivity brought about by the Internet of Things may ultimately require more people and organisations to develop a new approach to security, bringing it nearer to the forefront of their decision-making. An increasing proportion of applications are only likely to be used with confidence if people trust the security and private data protection associated with them. A future enriched by the Internet of Things is likely to be one where good security practice supported by robust system design is an essential part of everyday life.

21 http://internetretailing.net/2014/09/beacons-get-vote-of-confidence-with-roll-out-across-uks-largest-shopping-centre/
22 http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party

CHAPTER 3: Economic potential

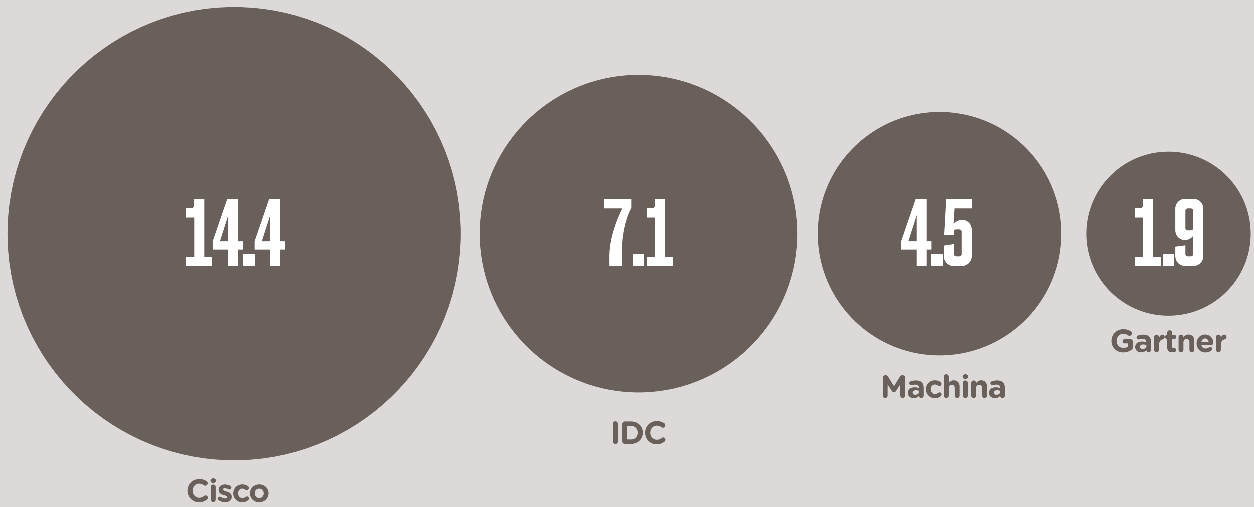
As with any set of emerging technologies, it is impossible to accurately predict the future value to the UK of the Internet of Things. Technology analysts Gartner estimate that the Internet of Things is still 5-10 years away from unlocking significant economic value, citing a lack of standardisation as the main obstacle to rapid progress.[23]

However, the potential gains are extraordinary. According to McKinsey, the Internet of Things has the potential to add $6.2 trillion to the global economy by 2025.[24] Other estimates range from $1.9 to $14.4 trillion of global economic value added by 2020.[25] The UK has competitive strengths on which to build, and growing clusters of highly innovative activity that could capture a share of this value.

Finding the benefits

The Internet of Things will affect different sectors of the economy at different speeds. Approximately 25% of global manufacturers are already using Internet of Things technologies.[26] This is anticipated to grow to over 80% by 2025, leading to a potential global economic uplift of $2.3 trillion in manufacturing alone.[27] Mining company Rio Tinto already attributes over $300 million in savings to these technologies.[28]

Figure 5:
Industry projections for Global Economic Value of the Internet of Things in 2020 ($ trillions)[25]



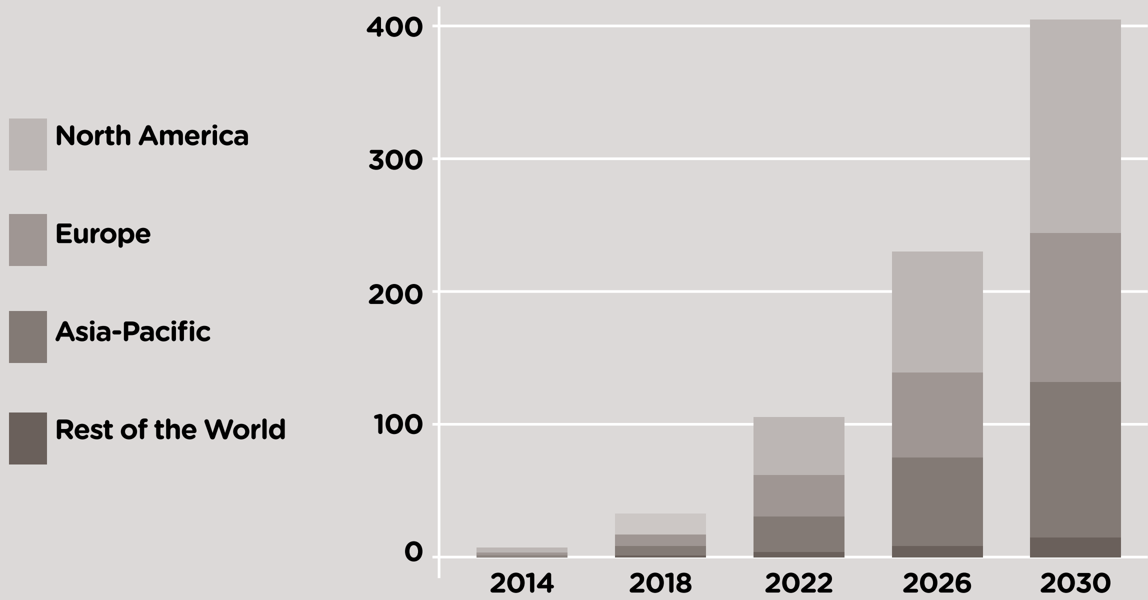
23 'Gartner's Hype Cycle Special Report for 2014', Gartner Research, 2014
24 'Disruptive technologies: advances that will transform life, business, and the global economy', McKinsey Global Institute, 2013
25 'Forecast: The Internet of Things, Worldwide, 2013', Gartner, 2013; 'Worldwide and Regional Internet of Things (IoT) 2014-2020 Forecast: A Virtuous Circle of Proven Value and Demand', IDC, 2014; 'Embracing the Internet of Everything to capture your share of $14.4 Trillion', Cisco Systems, 2013; 'The Connected Life: A USD 4.5 trillion global impact in 2020', GSMA & Machina Research, 2012
26 'The Internet of Things Business Index: A quiet revolution takes place', The Economist Intelligence Unit, 2013
27 'Disruptive technologies: advances that will transform life, business, and the global economy', McKinsey Global Institute, 2013
28 'The Internet of Things is Now', Morgan Stanley, 2014

Other sectors of the economy could gain similarly striking benefits. Morgan Stanley suggests that near real-time analysis of weather data using Internet of Things technologies could create a $20 billion global opportunity for the agricultural sector.[29] The same study suggests that the introduction of radio-frequency identification (RFID) chips to improve inventory management in the retail sector (excluding food) could save UK businesses £3 billion.[30] GB Smart Grid estimates £19 billion of savings might be achieved in the energy sector by upgrading the UK's network to a 'smart grid'.[31] ABI Research forecasts a doubling of cars with Internet of Things applications every four years in Europe.[32]

There are significant potential benefits to the wider economy and to public services. More robust safety measures in autonomous vehicles and smart transport infrastructure could reduce the £34.3 billion annual cost for traffic incidents.[34] Better road traffic management could help to alleviate congestion, saving up to £8 billion.[35] Rolling out healthcare applications is another area with significant possibilities – a trial in Yorkshire saved the Airedale NHS trust £330,000 in the first year by moving the need for 124 unplanned admissions.[36]

Governments will benefit hugely. Cisco identifies four drivers of potential public sector savings: employee productivity, cost reduction, improved citizen experience and increased revenue. The analysis estimates that over 25% of an estimated $19 trillion global market value available up to 2022 can be realised by the public sector.[37]

Figure 6:
Registered Vehicles with Internet of Things applications[33]



29 'The Internet of Things is Now', Morgan Stanley, 2014
30 Ibid.
31 'GB Smart Grid: a race worth winning?: a report on the economic benefits of smart grid', Ernst and Young, 2012
32 ABI Research World Market Forecast 2013-2030
33 'Smart Cars and the IoT', ABI Research, 2014
34 'Reported Road Casualties in Great Britain: 2012 Annual Report: A valuation of road accidents and casualties in Great Britain in 2012', DfT, 2013
35 Cisco PowerPoint presentation, 2013
36 'Internet of Everything: Bringing the future to life', Cisco Systems, 2014
37 'The Internet of Everything: Global public sector economic analysis, future to life', Cisco Systems, 2014

A competitive UK

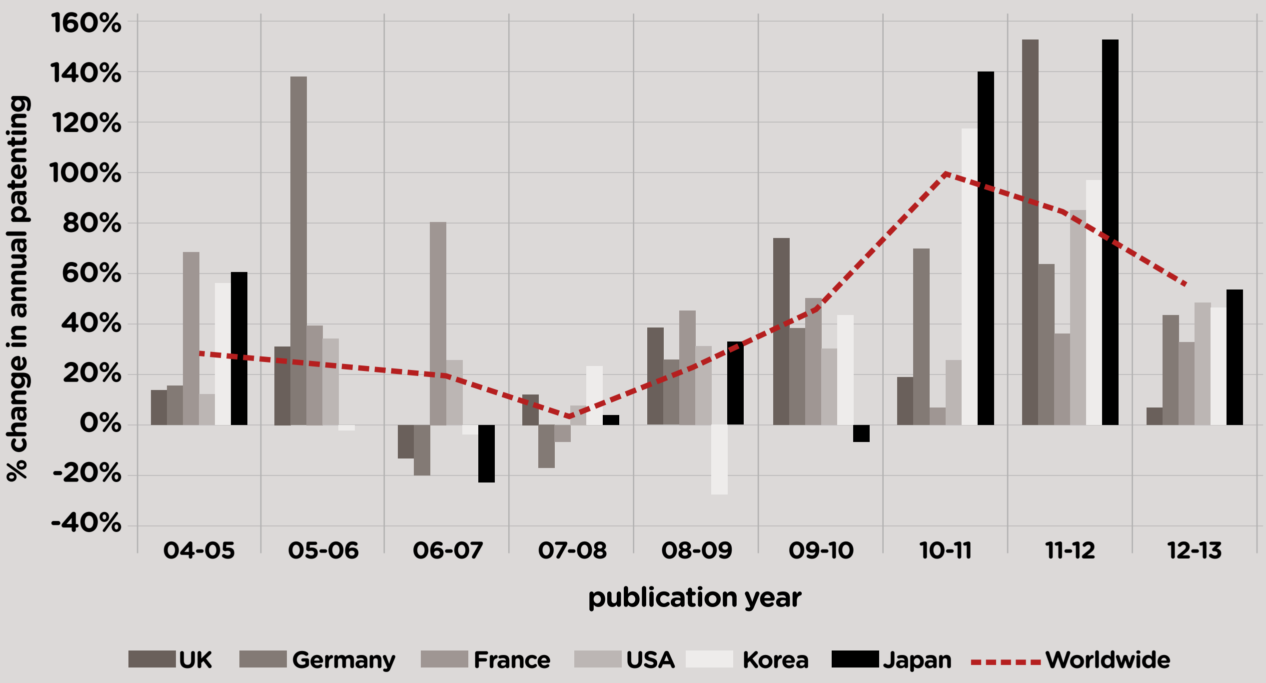
Patents are a crude proxy for innovation, but they can be a useful indicator of where leading edge technologies or applications are being developed. Analysis by the Intellectual Property Office suggests there is no definitive trend towards global leadership in any single country.

The UK is well placed to be among the emerging world leaders in reaping the benefits from Internet of Things technologies and services. Cambridge, London and Liverpool have emerging clusters of companies. Tech City is growing small digital businesses across London and the rest of the UK.

The UK has strong capabilities in the supply side (high technology manufacturing, telecommunications and digital services) and the demand side (health and social care, transport, retail and utilities).[39] It has world-class digital infrastructure, a positive regulatory environment, and a record of adapting to support emerging technologies. Innovate UK is already investing £45 million in small-scale Internet of Things demonstrators.[40]

There are indications that the UK could do more to build on these strengths. Cisco estimates that the UK gained $28 billion in economic value from applications of the Internet of Things in 2013, compared to $53 billion of potential value.[41] Their analysis goes on to say that companies can realise this further potential by 'connecting the unconnected' and taking market share from less agile companies.

Figure 7:
Year-on-year UK patenting activity for Internet of Things technologies[38]



38 'Eight Great Technologies: The Internet of Things', Intellectual Property Office, 2014
39 'Industrial Strategy: UK sector analysis', BIS, 2012
40 http://www.gov.uk/government/speeches/cebit-2014-david-camerons-speech
41 http://internetofeverything.cisco.com/en-gb/explore/full#/country/uk

CHAPTER 4: Applying the Internet of Things

This review's recommendations are informed and illustrated by a series of light touch case studies developed primarily through workshop discussions with technology practitioners and experts. The case study sectors were chosen on the basis of their potential application to public services. They are not intended to be a comprehensive list of the possibilities created by Internet of Things technologies.

In practice, the value of Internet of Things technologies will be fully demonstrated when different applications and devices work together seamlessly within and across different sectors, as they might in a future smart city.

TRANSPORT

High-performance computing, data collection, analytics and open data are powering progress in transportation. Mobile computing has enabled consumers to use an increasing range of applications to book services and plan trips. By connecting up the different strands of multi-mode journeys, the Internet of Things could significantly improve the way we travel.

The number of sensors in motor vehicles and public transport systems is growing. Today's average family car has more processing power than the first lunar lander. Many manufacturers of electric vehicles now offer applications that can remotely monitor battery power and schedule charging.

Looking further into the future, fully autonomous vehicles could ultimately be integrated into a transport system of smart roads, traffic lights, signs, streetlights and parking. Part of that vision is being demonstrated in Newcastle, where a trial system gives signals to drivers about when to adjust their speed if traffic lights are about to change.[42] Parking sensors and autonomous pods (unmanned people carriers) are being tested in Milton Keynes. The Department for Transport announced in July 2014 that autonomous cars would begin trials on UK roads in January 2015.[43]

The rest of this section discusses three significant opportunities created by applying the Internet of Things to transport: better passenger journeys, increased safety and more efficient transport of goods.

Passenger journeys

Customer surveys have repeatedly identified information about the journey as a critical factor in determining the quality of a passenger's experience.[44] London City Airport is trialling Internet of Things applications to improve customer experience and passenger flow, providing users with accurate "doorstep to destination" data.

Sensors placed throughout the airport are connected to a control centre and the data is aggregated.[45] Passengers can use a smartphone application to get information about queue times and to order from shops. The airport can use the data to model passenger flow, deploy staff to increase efficiency and identify building design improvements.

By linking near real-time data from different transport systems, passengers will be able to plan their journeys with greater certainty. They will be able to see an entire route, how different modes of transport connect, and access information about maintenance and delays. Better information may encourage the use of more sustainable forms of transport as part of the journey.[46]

42 This is currently being demonstrated as part of the Compass4D trial WI-FI.compass4d.eu/en/cities_02/Newcastle/newcastle.htm
43 http://www.gov.uk/government/news/uk-government-fast-tracks-driverless-cars
44 'Rail Passenger Experience Report', Office of Rail Regulation, 2014
45 Using the HyperCat standard enables data aggregation. http://www.hypercat.io
46 'Door to Door: A strategy for improving sustainable transport integration', DfT, 2013

Making data open and aggregated will require significant effort from transport operators. Transport for London has demonstrated some of the benefits, enabling third parties to design mapping, route planning and scheduling applications. Their approach has created a new market for applications that serve individual passenger needs. Other transport providers, particularly local authorities, should follow this lead and make their data accessible to encourage developers.

As well as making the process of getting from A to B more efficient, the Internet of Things could change the vehicles in which we make those journeys. Satellite navigation is already able to gather traffic data and re-route drivers. Sensors in cars will provide drivers with further information about driving conditions, road closures and traffic incidents. Smartphones and on-board screens will increasingly provide the interface between vehicles and their data rich environment.

Sensors could also enable more sophisticated traffic management by measuring and transmitting the precise speed and location of every vehicle on the road, in near real-time. Opportunities for the future could include combining location data with projected routes to simulate a whole-journey congestion map to route vehicles around anticipated bottlenecks. Such a development could significantly reduce congestion, bringing economic and environmental benefits.

The context of these sophisticated Internet of Things applications is important. It may make economic sense to automate transportation processes in certain environments, such as motorways and cities. In dense urban environments, these processes might eventually become fully automated. However, the software needed to resolve the challenges of full automation for tens of thousands of vehicles is incredibly complex. In addition to the technical challenges, autonomous vehicles individually and collectively raise fundamental questions such as:

- Regulation – currently a passenger must be able to assume immediate control.
- Ethics – if a crash is unavoidable, how does a car choose between multiple negative outcomes?
- Liability – is the manufacturer, the transport system operator, or the passenger liable?
- Social norms – will tacitly accepted 'rules of the road' norms need to be codified?

For autonomous vehicles to deliver to their full potential, it will be essential to consider and resolve these issues, learning from large-scale demonstrations and further research.

Increased safety

The Department for Transport has estimated that road traffic incidents cost the UK £34.3 billion in 2012[47] and that 90% are caused by human error.[48] While the economic productivity gains that might be made available by perfectly safe and fully driverless cars are years away, a more achievable benefit in the shorter term is to help reduce road traffic accidents.

Sensor technology should be able to anticipate collisions and automatically take evasive action, helping to reduce their occurrence and severity. Manufacturer Nissan has declared its 'zero emissions, zero fatalities' ambition for the autonomous cars it produces in 2020.[49]

Autonomous vehicles could offer additional benefits to specific sections of society, such as the elderly and less able. These potential benefits will become increasingly

47 'Reported Road Casualties in Great Britain: 2012 Annual Report: A valuation of road accidents and casualties in Great Britain in 2012', Department for Transport, 2013
48 https://www.abi.org.uk/Insurance-and-savings/Topics-and-issues/Driverless-cars
49 Message to Investors from Carlos Ghosn, President and Chief Executive Officer of Nissan, 2014

important as the UK population ages. For example, the Future Cities Catapult is experimenting with Internet of Things technologies to encourage innovative new services that will make navigating cities easier and more enjoyable for people with sight loss.[50]

The Internet of Things could also play an important part in vehicle maintenance and safety, helping to identify failing components and to optimise service scheduling. For example, RAC is offering a device that can be retrofitted to your car. It identifies mechanical problems and reduces the risk of an incident.[51]

Transporting goods

Better sensors will increase the quality and value of data about supply chains, providing rich data on the location and condition of goods. This should support a 'circular economy', where tagging a product from point of manufacture to recycling at the end of its life enables new ways to optimise resource use. For example, savings made in waste disposal can be used to encourage people to recycle.

The most important barrier to tracking many goods is the difficulty in connecting sensors throughout their journey. Connection requires the ability to share data between warehousing, transport and retail networks. Further progress could be made by agreeing common standards, catalysed by demonstration projects and government support.

The Internet of Things will also create opportunities to automate freight carriers. For example, the running of heavy goods vehicles on motorways could be automated to form platoons. This would enable vehicles to run at set intervals and standard speeds; maximising fuel efficiency. A prototype system has been developed by Mercedes.[52]

Security, reliability and regulation

As with many Internet of Things applications, transport raises important questions about public preferences and trust in the technologies. Surveys have identified that 95% of Brazilians are currently favourable towards autonomous vehicles. Only 28% of Japanese people held the same opinion.[53]

There will be challenges in bringing complex new technologies into mainstream transport infrastructure. For example, the widespread adoption of autonomous vehicles will not happen successfully before two fundamental engineering challenges are addressed: developing a vehicle with very high reliability; and creating a machine-to-human interface that is easy for users to operate. Reliability challenges will include managing the unpredictable interactions with pedestrians, conventional vehicles and unexpected events, such as road works or incidents. Meanwhile, applications in mass transit systems raise significant security issues.

Autonomous vehicles illustrate a new type of regulatory challenge. If every vehicle could track the speed and location of every other vehicle on the road, it would follow that every speeding car could in principle be penalised. The same could be said of every 15-second pause on a double yellow line with a parking sensor. This would have significant implications for regulators, for what is understood by proportionate enforcement, and for drivers' behaviours.

50 http://futurecities.catapult.org.uk/project-full-view/-/asset_publisher/oDS9tiXrD0wi/content/project-cities-unlocked
51 'How the IoT will Impact B2B & Global Supply Chains', OpenText
52 http://www.wired.com/2014/10/mercedes-making-self-driving-semi-change-future-shipping/
53 'Customer Experience Report', Cisco Systems, 2013

ENERGY

The UK's energy system is evolving. We are consuming less fossil fuel for heating, powering appliances, and transport. 14% of electricity was generated from renewable sources in 2013, a 300% increase from 10 years ago.[54] More than half of this came from intermittent sources such as wind power.[55] Solar photovoltaic generation, from rooftop micro-generation to multi-megawatt solar photovoltaic farms, is also growing in capacity.

The UK's energy infrastructure was built for a centralised model of generation, distribution and supply. It is now being stretched by the dynamic needs of energy suppliers and consumers. The Internet of Things could accelerate this trend.

Econometric modelling commissioned by the Smart Grids Forum estimates that £27 billion of infrastructure investment is required to cope with forecast demand growth to 2050. Building a smart grid could reduce costs by 33% compared with traditional approaches.[56]

Decentralised energy production and smart grids already exist in UK cities and on industrial estates. In rural areas, the emphasis is on adaptation of electricity distribution networks and innovative commercial arrangements to enable connections to onshore wind and solar photovoltaic farms as quickly and economically as possible.

By 2025, digital technology may define the electricity system almost as much as the physical engineering. The Internet of Things could enable the transformation of our existing system, with far reaching impacts on consumers, suppliers and the infrastructure that connects them. However, the rapid intake of new technologies requires the right incentive structures for distribution network operators.

The Internet of Things creates three major opportunities in the energy sector: reducing energy demand, managing patterns in demand and supply, and driving innovation.

Reducing energy demand

The £10.9 billion smart meters programme is the biggest government investment to date in Internet of Things technologies. By 2020, the national communications infrastructure will connect up to 53 million electricity and gas smart meters in homes and small businesses. A Home Area Network and linked in-home display will provide near real-time energy consumption information, and a central regulated body will control access to the data.

Heating accounts for 79% of UK domestic energy use.[57] Evidence suggests that smart meters may initially provide 2-3% reduction in energy use through changes in behaviour.[58] However, many people will use energy savings in one area to enable themselves to achieve a higher level of comfort overall, instead of "banking" the financial and environmental benefits.[59] If meters are combined with thermostats, weather sensors and boilers, energy savings could range from 6-29%.[60] These technologies have the potential to reduce energy bills, carbon emissions and overall demand for electricity.

There are other savings to be had in areas of domestic energy consumption. A

54 Renewable Energy in 2013, DECC
55 http://www.renewableuk.com/en/news/press-releases.cfm/2014-07-31-new-uk-record-nearly-15-of-electricity-from-renewables-more-than-half-from-wind
56 'Smart Grid: a race worth winning?: a report on the economic benefits of smart grid', Ernst and Young, 2012
57 'The Future of Heating: A strategic framework for low carbon heat in the UK', DECC, 2012
58 'Smart Meter Rollout for the Domestic Sector (GB)', DECC, 2011
59 'The Rebound Effect: an assessment of the evidence for economy-wide energy savings from improved energy efficiency', UKERC, 2007
60 'Assessing the Use and Value of Energy Monitors in Great Britain', BEAMA, 2014; 'Hive Energy Saving Report', British Gas, 2014

marketplace of smart appliances that link to the Home Area Network, on which energy pricing data is available, would build on the benefits.

An important opportunity presented by smart meters is helping to bring more people out of fuel poverty by supporting them in using energy efficiently, including by giving easier access to lower cost 'time of use' tariffs.

Managing energy patterns

Matching energy demand with supply is one of the biggest challenges for the energy sector over the next decade.[61] More intermittent energy generation combined with a greater number of battery powered devices (such as electric vehicles and mobile devices) could exacerbate pressures in all parts of the system.

Smart meters will give consumers and businesses better feedback and more control over their energy use, as well as providing electricity distribution companies with a more sophisticated means of managing the risk of an interruption to supply.

Smart meters could help smooth out demand if supported by dynamic 'time of use' tariffs that reflect variable generation costs. The Internet of Things will also increase the potential for intelligent supply-side management. Smart grids will respond to changes in demand by balancing supply with storage and intermittent sources; and by maintaining supply to essential systems, even down to the level of individual devices. The use of battery storage in connected devices (such as electric vehicles) may be used to shift load away from peak demand.

In the future, government may need to explore storage incentives for households and small businesses, or to create additional flexibility by allowing mechanisations such as Distribution Network Operators to pay customers for providing storage capacity.

Driving innovation

The Internet of Things could create new business models for the provision of energy services. For example, new forms of demand management may lead to creative alternatives to traditional energy consumption patterns. In some parts of the USA, smart grids are being deployed to increase system resilience against 'super storms' that cause extensive disruption to electricity supplies.

Richer and open data, alongside energy market reform, would create opportunities for new tariff models. Consumers may benefit from options that more closely reflect their individual energy demand patterns.

Deploying Internet of Things technologies in energy is not without risk. To achieve the potential economic and societal benefits, three main threats must be managed: increased energy demand; insufficient security; and variable access.

Increased energy demand

The devices that enable integrated smart home services, such as heating, lighting, and electric vehicles will require energy to operate. Although the power drain of an individual sensor is likely to be minimal, in aggregate the Internet of Things may significantly increase electricity demand. This could be offset by changes to when the electricity is used, thereby reducing peak demand, but further research and modelling will be necessary to understand the implications.

Security and standards

The Internet of Things will increase the complexity of the energy system, particularly the

61 http://www.britishgas.co.uk/products-and-services/gas-and-electricity/tips-and-advice/understanding-energy-prices.html

electricity network. Unless resilience is carefully built in this is likely to increase the risk of cyber or physical attack by creating multiple new points of vulnerability. Security issues must be considered from the outset in both individual devices and whole systems.

Devices may collect large amounts of data, some of which may be personal. Doing so will offer many benefits, such as cheaper electricity from ‘time of use’ tariffs, remote operation, and manufacturer servicing on demand. However, the data could be misused to determine aspects of the users’ lifestyle, such as whether they are at home. Data from connected energy devices will need appropriate and proportionate security, and personal information will need to be protected. Consumers and businesses will use systems that are trusted and trustworthy.

Shared standards will help speed up the adoption of smart appliances, as competing models may mean multiple complex and expensive solutions all need to work together. The landscape is already highly complex. For example, Sigfox connects smart meters to the network, Zigbee connects meters to the Home Area Network, Thread connects Nest’s thermostat and Wi-Fi connects appliances from companies such as Bosch.

Variable access

Building a telecommunications infrastructure that provides for a single application of the Internet of Things will not achieve the greatest value for money. Incomplete network coverage could leave some areas or groups of people in the UK excluded from significant benefits. It may be that more incentives are required for investment in ’hard-to-reach’ areas, particularly rural communities with high incidences of fuel poverty. In addition, some users may not be able to access new technologies effectively, and their needs will need to be taken into account in future regulatory design.

HEALTHCARE

The Internet of Things could help shift healthcare from cure to prevention, and give people greater control over decisions affecting their wellbeing. In turn, these technologies could integrate the delivery of care, improve clinical outcomes and yield considerable cost efficiencies for the NHS. Telehealth – the delivery of remote health-related services – is increasingly feasible thanks to the rise of connected smart devices.

Current demographic trends strongly suggest major challenges for the NHS in the years ahead. The UK population could be the largest in Europe by 2050, and continue to grow steadily with more people living into very old age. This will inevitably put pressure on public services. A 2007/08 study estimated that the average value of NHS services for retired households was £5,200, 186% more than households with no retirees.[62]

Chronic conditions will also shape future demands on the health service. It is predicted that over the next 25 years the cost of the direct treatment of diabetes in the UK will increase from £9.8 billion to £16.9 billion[63] per year. The number of UK adults and children who are obese continues to grow.[64] Mental health impacts could be equally significant. Dementia is currently estimated to cost the UK £23 billion a year, with expenditure following a steadily upward trend.[65]

The potential for the Internet of Things to deliver benefits in healthcare is enormous, and much work is underway. This case study touches on three potential areas of opportunity: prevention and early identification, research and tailored healthcare.

Prevention and early identification

Clinicians will continue to play the central role in diagnosis. However, inexpensive connected devices can already monitor patients' vital signs – blood pressure, heart rate and blood sugar levels for example - in near real-time. The stream of health data can immediately alert users to anomalies and can be analysed with sophisticated software to support early diagnosis.

There are quantifiable benefits from early efforts to digitise healthcare, such as SMS reminders for clinical appointments reducing costly missed appointments.[66] Adding sensor and other data opens up new possibilities. For example, embedded sensors in homes are making it possible for the elderly and people with mental health conditions to safely lead independent lives for longer.[67]

Smart devices may also increasingly be used to help patients with chronic health conditions; this data could be monitored by clinicians, intervening as required. Taken together with safe "digital by default" approaches to communicating with healthcare professionals, such developments would reduce the need for routine and costly face-to-face appointments.

Despite the huge potential benefits, there are considerable challenges to deploy the Internet of Things at scale. Skilled professionals will be needed to interpret the data, and both they and the patients will need robust security and privacy safeguards in place.

62 http://www.parliament.uk/business/publications/research/key-issues-for-the-new-parliament/value-for-money-in-public-services/the-ageing-population/
63 http://www.nhs.uk/news/2012/04april/Pages/nhs-diabetes-costs-cases-rising.aspx
64 http://www.nhs.uk/news/2011/08August/Pages/half-of-uk-predicted-to-be-obese-by-2030.aspx
65 http://www.alzheimers.org.uk/site/scripts/documents_info.php?documentID=418
66 http://www.appointmentsms.com/Medical-SMS-Appointment-Reminder.aspx
67 http://www.mentalhealth.org.uk/content/assets/PDF/publications/starting-today-background-paper-4.pdf

Research

Connected devices significantly increase the potential to gather more sophisticated health data for use in epidemiological studies. For example, data taken from wearable devices could help uncover whether certain lifestyle patterns combined with particular genetics lead to predispositions or resistances to particular diseases.

Wearable devices could collect a broad range of data: diet; exercise; exposure to environmental factors (such as allergens, pollution and sunlight); and markers for mental health such as social interaction. Such data will provide general benefits and enable more personalised healthcare from a deeper understanding of the patient's unique lifestyle and history.

Smart objects have also already made it easier for people to track their activity and behaviour. Lifestyle devices nudge users to adopt a healthier lifestyle with data on the number of steps walked or calories burnt. By linking diet and exercise, and displaying the data, the user is incentivised to improve their health.

Some experts argue that applications and smart wearable devices will be a driving force for a healthier society.[68] However, it remains early days for these devices, and the evidence supporting the impact of wearable devices on lifestyle behaviours is still limited.

These technologies are not without risk. The Internet of Things creates three major threats in healthcare: data security and ownership, hardware security and interoperability, and change management.

Data security and ownership

Information about patients' personal health must be handled with great care. The amount of data potentially generated by connected healthcare devices is vast. At a minimum, most patients will to want to know what their healthcare data is being used for, why, where and by whom. Patients and clinicians need confidence that appropriate data protections and governance mechanisms are in place.

Putting in place protocols that unnecessarily limit the beneficial use of data could also be damaging, sacrificing huge research and treatment benefits. A large proportion of healthcare-related data collected by Internet of Things enabled lifestyle devices could be privately owned. Businesses may prefer to exert proprietary control over the data created by their devices. They may also store the data outside the UK, where users and the government will have less control over security.

Hardware security and interoperability

The reliability of healthcare devices may be a matter of life and death and their resistance to hacking is extremely important. The consequences of a malicious attack on a 'connected hospital', or hacking devices that provide life support, could have dire consequences.

Mobile devices such as pacemakers raise the important question of interoperability for connected devices. A connected pacemaker will require standards that are universally recognised so that data from life-critical monitors can be transmitted in any country the patient visits. As with other Internet of Things applications, healthcare has a clear need for interoperability and security to be an integral part of their development. The ability to upgrade them remotely, with security patches and other fixes, will also be essential.

68 http://www.ericsson.com/thinkingahead/the-networked-society-blog/2014/01/28/smart-devices-are-making-city-life-healthier/

Change management

By offering greater personal control over healthcare and remote monitoring, the relationship between people and clinicians may deepen and help us to lead healthier lives. Many patients will be unsure about new developments and will look to trusted professions for advice. Healthcare professionals must be well prepared to give advice about the opportunities and risks of new devices and systems.

The effects these technologies could have on training, skills, working patterns and funding prioritisation are all also significant. Therefore, specific applications will need to be carefully developed in consultation with those who will use and support them.

AGRICULTURE

As a field of human activity that was one of the very first to be transformed by technology, agriculture is well versed in taking advantage of new opportunities. The Internet of Things potentially offers another leap forward.

Field-based sensors can already measure soil moisture and communicate with weather stations for the latest forecasts. This data is used by large farming operations to determine how much water to apply to crops and when to apply it. Other sensors can collect data on temperature, light, soil acidity and fertiliser content. Animal tracking allows livestock to be monitored for disease and accidents – as well as providing opportunities for better husbandry.

As with many other sectors, the Internet of Things brings benefits in aggregate as well as to individuals. 'Smart farms' may share data with other farms, different parts of the supply chain, regulators and consumers.

This review discusses three major opportunities for agriculture: maximising yields, improving food traceability and tackling environmental challenges.

Maximising yield

The UK population is expected to grow to 77 million by 2050.[69] By contributing directly to the advancement of precision and automated agriculture, the Internet of Things could have an important role in meeting increasing demand for feed, food and raw materials.

A number of opportunities exist for 'smarter' farming and overcoming issues that limit crop yields. For example, sensor arrays can identify potentially damaging weeds – such as black grass – which hinder crop growth. Their location can be reported back to farm owners who then tackle problem areas more efficiently and accurately. These sensors could also ultimately interact directly with autonomous weeding machines.

Fully autonomous farms are still some years away. However, examples of applied agricultural robotics are emerging rapidly. A joint program led by Osnabrück and Wageningen Universities is using robots to identify and remove weed patches.[70] Robotic approaches based on smart small machines are also being pioneered at Harper Adams University.[71] Early evidence suggests that controlled traffic farming – where machinery drives along repeatable tracks with greater accuracy – could reduce machinery and input costs by as much as 75%.[72]

Smallholdings contribute 70% of global food production.[73] However, they have not been the target market for this level of precision agriculture to date. Through support for relevant demonstrator projects, governments might catalyse the development of uses that support small-scale farmers.

Improving food traceability

There is some evidence that consumers are increasingly concerned about the provenance of food they buy.[74] The Internet of Things could play a significant role in tracking food from 'farm to fork'. Sensors with geo-location capability can provide information to consumers concerning the origin of food and production methods. This might become particularly important for high value produce, where provenance is a key selling point.

69 http://www.ons.gov.uk/ons/interactive/uk-national-population-projections---dvc3/index.html
70 http://go.amazone.de/index.php?lang=1&news=26
71 http://www.bbc.co.uk/news/uk-england-shropshire-25967965
72 'Precision Agriculture: An opportunity for EU farmers – potential support from the CAP 2014-2020', European Parliament, 2014
73 'Towards a Green Economy: Pathways to Sustainable Development and Poverty Eradication', UNEP, 2011
74 'Food Traceability', European Commission, 2007

From a regulatory perspective, Internet of Things technologies could allow the tracking and tracing of foods through the supply chain and thus provide stronger incentives for farmers and food producers to observe 'best practice'. Higher quality crops and improved animal welfare could result. However, crops and food products sold in the same form as they are produced (such as vegetables) are easier to trace than processed foods such as meat or grains.

Tackling environmental challenges

The Internet of Things has the potential to improve environmental protection while benefitting many different forms of agriculture. Livestock sensors are an early example of this trend. 3D accelerometers already allow near real-time monitoring of cows, detecting injuries and illnesses within the livestock.[75] This enables farmers to react faster to potential issues.

Farmers and society stand to gain even greater benefits by openly sharing data. For example, algorithms could analyse data for patterns in diseases, enabling the early adoption of preventative measures.

Smart farming methods would also help to tackle resource scarcity. For example, 70% of the world's fresh water is used in agriculture.[76] The conservation of water use – by using sensors to pinpoint exactly where and how much water is needed – could have substantial implications for managing water shortages. This is already an important issue in developing countries like India, but climate change is likely to increase similar pressures on the UK.

There are potentially three major barriers to rapid uptake of the Internet of Things in agriculture: incompatible equipment, a lack of infrastructure and a lack of specialist technical skills.

Incompatibility

The primary risk is a lack of compatibility between the software used in different machinery and systems. Interoperability allows devices to share information and to support decision-making and automation. The more data sharing there is between businesses in the supply chain, the greater the potential benefits to all.

Although many companies involved in the agriculture value-chain offer some form of precision agriculture services, there are few industry-led standards.[77] The International Standards Organisation communications protocol[78] allows compatibility between different branded tractors with any other farming implements. However, it does not incorporate new technologies such as steering systems, or non-machinery based data.

Where they exist, standards provide the opportunity for farmers to adopt machinery and systems from different brands and companies – removing the potential for monopolistic providers to dominate. Standards should go beyond merely allowing interoperability between machines. Data standards, including ways of presenting data, for ease-of-access by farmers, will enable a new data driven market to develop for both individual and aggregate services.

75 E.g. http://www.etrack-project.eu/
76 'Water at a Glance: The relationship between water, agriculture, food security and poverty', FAO
77 'The Internet of Things is Now', Morgan Stanley, 2014
78 ISO standard (ISO 11783).

Lack of infrastructure

Connectivity is also a significant obstacle to precision farming. Farms are often held back by their remote location. Internet access is often slow, if available at all. Signals for 3G and 4G networks are often limited too; and what signal there is can be split between several telecommunications operators. To overcome this difficulty, the Satellite Applications Catapult is encouraging the use of rural broadband via satellite.[79]

Limited bandwidth in rural areas is further constrained by high cost and intermittency. This can cause incomplete data collection – creating difficulties for thorough spatial analysis, or identifying patterns for future decision making. A widespread and reliable infrastructure is necessary for sensors and other technologies to communicate effectively in rural areas. Low-power, wide-area networks have potential, although data coverage is currently limited. Likewise, TV white space – recently reserved by Ofcom between 870-915MHz for machine-to-machine communications – may help to resolve the issue.[80] The Catapults are currently working on an infrastructure strategy, including interoperability systems and standards to integrate satellite and terrestrial communications systems to provide nation-wide coverage.[81]

Technical expertise

More sophisticated agricultural machinery combined with digital technology will demand new types of technical expertise. Agronomists will be required to work as, or with, data analysts to help farmers make decisions based on the best technical advice on land management and data science.

Relatively few Science, Technology, Engineering, Mathematics (STEM) graduates currently pursue careers in the agriculture sector. Some commentators take the view that this may be partly due to a perception that farming is not 'academic' or modern, or that higher education does not provide the right combinations of skills. Moreover, technology companies may fail to identify agri-tech market opportunities.

Universities and colleges will need to change if the Internet of Things is to be applied effectively to agriculture. In particular, the sector needs enhanced links between scientific, engineering and digital skills in agricultural engineering.

79 http://www.satelliteinternet.co.uk/
80 Part of the Digital Infrastructure Strategy, DCMS, 2012
81 'DCMS Digital Strategy: becoming digital by default', DCMS, 2012

BUILDINGS

Smart buildings could become the hub for a wide range of Internet of Things applications. Sensors are increasingly being installed in buildings to gather data about movement, heat, light and use of space. This information could allow Building Management Systems (BMS) to make near real-time alterations to a building's environment. Sensor data may also be analysed as part of designing subsequent buildings and systems.

The benefits and risks of smart buildings are further magnified when considering them at scale within a smart city. Living and working amongst smart buildings could have profound implications for the information we can access about our immediate environment, and how we behave in public spaces. There are already government initiatives supporting the development of smart cities in the UK, including a Smart Cities Forum that was set up to lead these efforts and build on the Information Economy Strategy.[82]

Buildings connected to the Internet of Things could create significant opportunities for cost minimisation through energy optimisation and predictive maintenance. A recent publication by the Royal Academy of Engineering highlights these advantages and others. It states:

"Recent advances in data gathering and analysis are opening up new possibilities for smart building technology. For the first time, building management systems have the capability to learn and even anticipate their occupants' needs and preferences for light, temperature and other services – saving energy through targeted supply. The ongoing expansion and upgrading of wireless networks and leaps in computing power mean that today's smart building designers possess the tools to use data to make the built environment more comfortable while reducing our carbon footprint."[83]

Optimising design and minimising costs

Connected sensors will show how occupants are actually using the space and whether this matches the architect's original intention. This level of detailed information would allow architects to take a more iterative and experimental approach to design, optimising environments according to the realities of their use.

Information from building sensors may ultimately be incorporated into real-time Building Information Modelling, sometimes described as BIM Level 3. This will allow online dashboards about buildings to be published, as well as annotating computer aided design representations of building systems with live measured values from building sensors. In turn, parameters of the BMS can be monitored and controlled remotely.

The installation of multivariable sensing and zone control, combined with high-performance BMS, provides opportunities for improving occupant comfort and minimising operational costs. It also potentially creates a new high-value service sector in Smart Facilities Management, in which third party service companies provide online and near real-time monitoring and control of buildings using data from internal and external sources.

It will be possible to go further by merging weather and information from other systems with building data. For example, a building system might make use of weather

82 Information Economy Strategy, HMG, 2013. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206944/13-901-information-economy-strategy.pdf

83 'Smart Buildings: people and performance', Royal Academy of Engineering, 2013

forecasts to predictively control cooling or heating, or it might combine information from the occupants' mobile devices to allow fine grain control of their environment.

Increasing comfort

Sensing and actuation in smart buildings is increasingly connected through wireless networks. Given the cost of a wireless transceiver, it makes sense to combine several measured variables in each device. Measurements could include: human presence[84]; temperature; humidity; and light level. The population of sensors forms an 'Intranet of Things', feeding their data into a host BMS, which itself is likely to be connected to the Internet. Additionally, output sub-systems like pumps, valves, heaters and lights could be controlled by the BMS through the local control intranet. A typical commercial building may ultimately connect several thousand monitoring and actuation devices to provide a rich flow of interpretable data.

Algorithms may soon be able to learn occupant behaviours and thus adjust the building settings to best satisfy user preferences. A spin-off will be the ability to detect when occupant behaviours deviate from norms. This might help a contractor to intervene sooner to maintain building performance levels.

As with other sectors, applying Internet of Things technologies to buildings will require safety and security to be built in from the start.

Security and safety

Relatively trivial events (such as a power cut) will become more complicated in an Internet of Things connected building. Interconnected systems may create a knock-on effect of failing routers and devices. Malicious cyber-attacks, focused on the wireless networks or internet links from the BMS to a cloud-based server, could artificially create similar effects.

The safe fusion of external data with internal building states will also require assurance of the provenance of that data. An attack on BIM sensors (such as thermostats) that produces false data could create issues with temperature control. Spoof attacks on fire alarms, CCTV or door locks could also create a false impression to those responsible for security.

Human nature will be a fundamental consideration in this; if a sensor is constantly triggered due to a hacker 'glitching' it, the maintenance team may think it is broken and turn it off.

Other potential risks include:

- Discovery of occupancy patterns, possibly down to the level of individuals' identities
- Private or sensitive information inferred from disparate, publicly available, open datasets
- Interception of wireless data communications and leakage of confidential information
- Virus and Trojan implantation at a device level as well as in the BMS itself.

Data ownership is further complicated by the details of property ownership. A building may be leased by one organisation to another, with building management controlled by a 3rd party. Engine manufacturers have been known to lease their engines to airframe operators; this model could be copied by construction companies controlling the whole life of a new build.

84 Typically using Passive Infrared (PIR) technology.

The trade-off between cost and risk in determining the level of required encryption in buildings is likely to change over time. In the future, the relative weakness of a building's BIM security may make it stand out against other similar properties. Insurance companies may take BIM security into account when conducting their risk assessments. This should eventually help create clearer incentives for the construction industry to put more secure BIM in place. However, in the short-term companies and organisations using Internet of Things technologies in buildings will need to find them trustworthy from their first day of use.

Acknowledgements

I would like to thank the many contributions and the support in conducting this review – Sir Mark Walport, Government Chief Scientific Adviser.

The expert panel for giving up their time to guide the review:
Prof Philip Bond, University of Oxford
Alastair Cook, Critical Insight
Prof Rachel Cooper, Lancaster University
Dr Lynne Coventry, University of Northumbria
Prof Sadie Creese, University of Oxford
Prof David De Roure, University of Oxford
Prof Hugh Duncan Griffiths, UCL
Prof Bill Dutton, University of Oxford
Dr Robert Ghanea-Hercock, Chief Scientist, BT
Tim King, Chief Technology Officer, BT Engineering Services
Prof Thomas Rodden, University of Nottingham
Dr James Scott, Microsoft Research
Alex Van Someren, Amadeus Capital
Dr Dave Watson, IBM
Prof Jeremy Watson, UCL

The Government Chief Scientist network for their advice throughout:
Prof Muffy Calder, Scotland Chief Scientific Adviser (CSA)
Prof Vernon Gibson, MoD CSA
Prof Nick Jennings, National Security CSA
Prof David MacKay, DECC CSA
Prof John Perkins, BIS CSA
Prof Bernard Silverman, HO CSA

The project team for synthesising the evidence into this report:
Davor Bokhari
Rebecca Brennan
Ben Edmonds
Oliver Grant
Andrew Greenway
Matthew Starr

Printed on paper containing 75% recycled
fibre content minimum.

First published December 2014
The Government Office for Science
URN: GS/14/1230

Design and Production: WordLink