GSR discussion paper

Regulation and the Internet of Things

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 25 June 2015.

Table of Contents

Regulation and the Internet of Things

Author: Prof. Ian Brown, Oxford Internet Institute, University of Oxford, United Kingdom[1]

Executive summary

This discussion paper examines the implications of the Internet of Things (IoT) for individuals, businesses and societies, and particularly the issues that telecommunications and other regulators will need to consider as IoT systems proliferate in developed and developing economies.

Broadly speaking, IoT refers to the addition of communications and sensing capabilities to a very wide range of physical objects. In the next decade, technology companies and consulting firms expect tens of billions of IoT devices to be deployed – from parking meters, thermostats, cardiac monitors, tires, roads, car components, to supermarket shelves and many other types of physical object – driven by an ongoing rapid reduction in the cost of sensors, processing and networking technologies.[2] IoT devices can share data directly using protocols such as Wi-Fi and Bluetooth, and via mobile phone networks and specialised radio networks, as well as over the global Internet.

As well as device manufacturers, network operators, application platforms and software developers form a broader ecosystem of companies developing IoT services. Data analytics services, often cloud-based, are also important components of IoT systems.

IoT systems support a broad range of applications, from monitoring and managing individual health and wellbeing, improving energy efficiency, increasing industrial process quality and reliability, to reducing traffic congestion and enabling the development of new products and services – especially based on pay-per-use charging.

IoT devices will have the biggest societal impact where they are used together in larger, inter-connected, systems. At the macro-level, two of the areas of greatest IoT development and investment are smart cities – where infrastructure and building systems will improve the efficiency and sustainability of a whole range of urban activities – and smart power and water grids. Closer to the individual, "connected vehicles" with hundreds of separate sensors will be safer, more reliable, and able to participate in sophisticated congestion management systems. And population health and wellbeing – a challenge to governments around the world as populations grow older, with a corresponding increase in age-related chronic conditions – could be significantly enhanced with IoT-based systems used by individuals, carers, primary care doctors, and hospitals. Devices such as insulin pumps and blood-pressure cuffs can monitor patients and report warning signs of conditions such as diabetes and heart disease.

The public and private sector are continuing to fund significant levels of IoT research and development, in areas such as modularity, reliability, flexibility, robustness and scalability. But the basic capabilities needed for many applications are already well understood, and becoming available through smartphones and other standard platforms. These devices will also address some of the cost issues that have held back growth in the past, although cost and reliability remain issues for large-scale systems, as does connectivity. A significant

opportunity is the greater use of open data and Application Programming Interfaces (APIs), which can enable a higher level of innovation in IoT systems.

As IoT systems grow, issues of connectivity (with machines and humans) and addressing become more important. Enabling peer-to-peer connections between devices can increase the reliability of communications, compared to requiring a large and complex global network, and matches the common use case of an individual discovering and interacting with nearby devices. But where devices must be globally reachable – most likely, via the Internet – a large address space is required to individually identify each one. Meeting this requirement would be an additional benefit of global adoption of the next version of the Internet Protocol, IPv6.

The purpose of this paper is to raise awareness among the ICT regulatory community of the changes led by the advent of IoT, examining the challenges and opportunities to understand how this is impacting consumers, businesses, governments and society at large. There are particular regulatory implications for licensing and spectrum management, switching and roaming, addressing and numbering, competition, security and privacy – some familiar to telecoms regulators, and other areas where different regulators typically take a lead.

The Internet of Things

What?

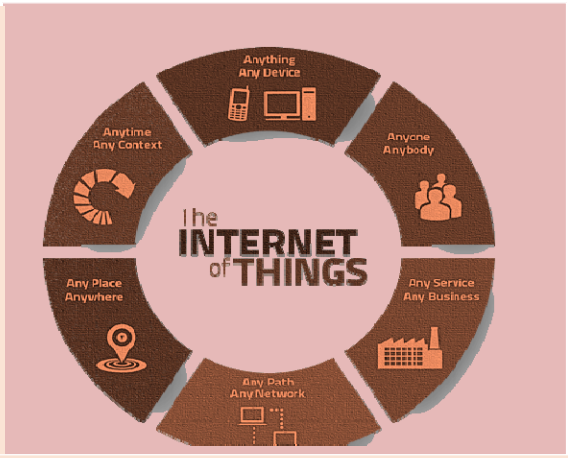
"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication" (ITU-T)

Who?

Device manufacturers, network operators, application platforms, software developers and (cloud-based) data analytics services providers

How?

Connection of IoT devices via Wi-Fi, Bluetooth, mobile phone networks, specialized radio networks, global Internet



Main current areas of investment

- **Smart cities**
- **Smart metering & grids**
- **Connected vehicles**
- **Healthcare**

Main Impacts

- **Monetary/economic impact: trillions of dollars annually within a decade**
- **Societal impact: Smart cities – infrastructure, transport and buildings – by improving efficiency and sustainability of a whole range of urban activities; smart power and water grids (smart meters)**
- **Individual impact: e.g. transport safety through "connected vehicles"; population health and wellbeing can be enhanced, enabling e.g. care at home**

Challenges

- **Cost needs to fall, reliability needs to improve**
- **Issues of connectivity, user interfaces and addressing**
- **Regulatory implications for licensing and spectrum management (access required to 300 MHz-3GHz but also NFC at 13 MHz or EHF bands, AM/FM bands in VHF range, Wi-Fi and 4G mobile networks), standards (interoperability e.g. ITU-T's initiative IoT-GSI), competition (e.g. impact on competitiveness of different markets, customer lock-in due to fixed SIMs in each device etc…), security and privacy ("by design" approach desirable)**

1. Introduction

Plummeting electronics and communication costs have set the stage for a rapid expansion of the Internet of Things (IoT) – the billions of everyday physical items that now have sensors and network links, enabling them to remotely share data about themselves, their users and environment. In the next decade, technology companies and consulting firms expect tens of billions of IoT devices to be deployed, with a total annual economic impact in the trillions of US dollars.[3,4,5]

Companies manufacturing IoT devices are only one part of a broader ecosystem of organisations developing the IoT. The data created by devices can be shared via communications networks, platforms (including social media sites), and accessed and controlled by third-party applications – often running on users' smartphones (which themselves contain an increasingly diverse range of sensors).[6]

This discussion paper examines the concepts, technologies, and societal changes influenced by the IoT and related technical developments – which include convergence, cloud services, data analytics, the proliferation of sensors, measuring and monitoring humans, machines and things – that are leading to a shift from human-to-human communications, to machine-to-machine (M2M) and everything-to-everything communications.

The purpose of the paper is to raise awareness among the ICT regulatory community of the changes led by the advent of IoT, examining the challenges and opportunities to understand how this is impacting consumers, businesses, governments and society at large. The most important regulatory implications are in the areas of licensing, spectrum management, standards, competition, security and privacy.

Box 1: Republic of Korea's Master Plan for Building the Internet of Things

The government of the Republic of Korea has developed a master plan to use IoT to improve public administration; increase industrial productivity, efficiency and added value; and improve the safety and quality-of-life of individuals. It sees the country as a potential global leader in IoT products and services given its top-class ICT infrastructure and manufacturing capacities.

The plan aims to increase the domestic IoT market fourteen-fold over the seven years to 2020, with a 30% increase in productivity and efficiency in user companies. Because of the small domestic market, cooperation with global businesses is an important part of the strategy. Domestically, new software services in advanced manufacturing will enable growth of traditional industries and new software companies. The government will promote joint research and demonstration projects with the Trans-Eurasia Information Network, which connects 19 Asian and 34 European countries.

Information security is one key focus of the plan, with the government aiming to establish an information sharing and analysis framework with governments such as the US, Japan and EU. The country's IoT Innovation Center will provide a test-bed environment for security functions and promote security and privacy by design in IoT systems.

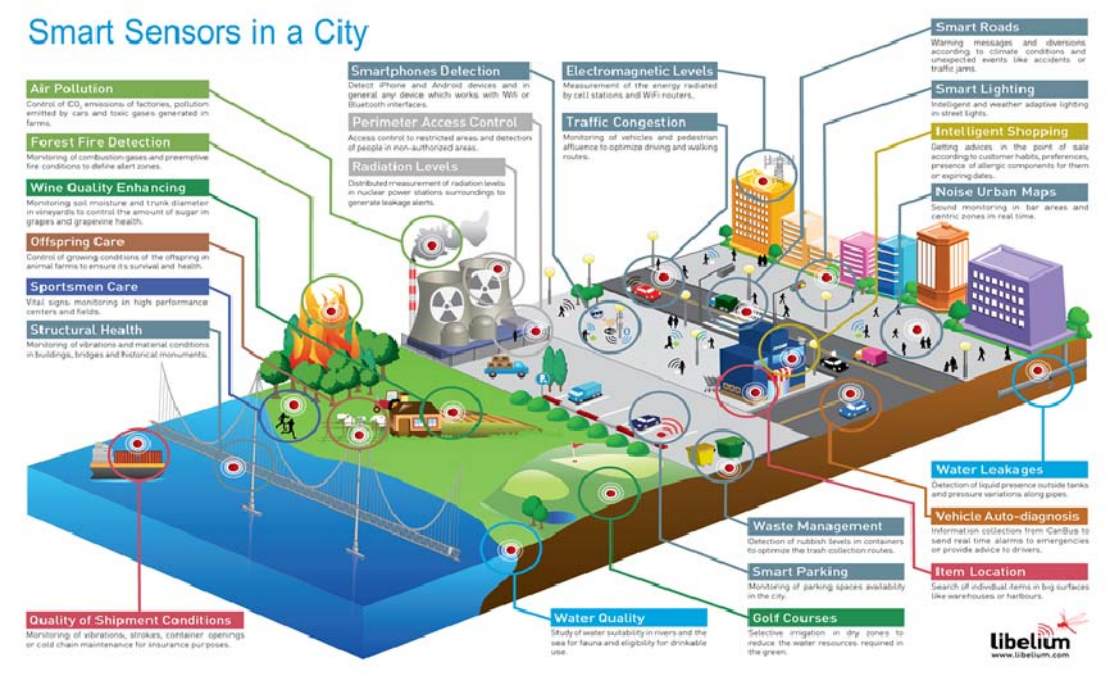
Source: Ministry of Science, ICT and Future Planning, Republic of Korea, 8 May 2014.

2. Internet of Things concepts and deployment

The ITU-T's definition of the Internet of Things (IoT) is "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[7] This refers to the network of remotely linked tags, sensors and actuators (motors and other mechanisms to cause an action within a device) that are increasingly being built into objects throughout the physical world, driven by ongoing rapid falls in the cost of microchips, sensors and communications capacity.

Collectively, with slightly different emphases, these technologies are also known as ubiquitous/pervasive computing, cyber-physical systems, smart environments/spaces/cities (shown in figure 1, and discussed in the next section), the industrial Internet (focused on manufacturing processes), and ambient intelligence.

Figure 1: Smart cities



Source: Libelium.

The term Machine-to-Machine (M2M) communication is used to refer to communication directly between IoT devices, often via cellular networks. The mobile industry association GSMA predicts between 1 and 2 billion M2M connections by 2020.[8] This has regulatory implications relating to switching and roaming, discussed further below.

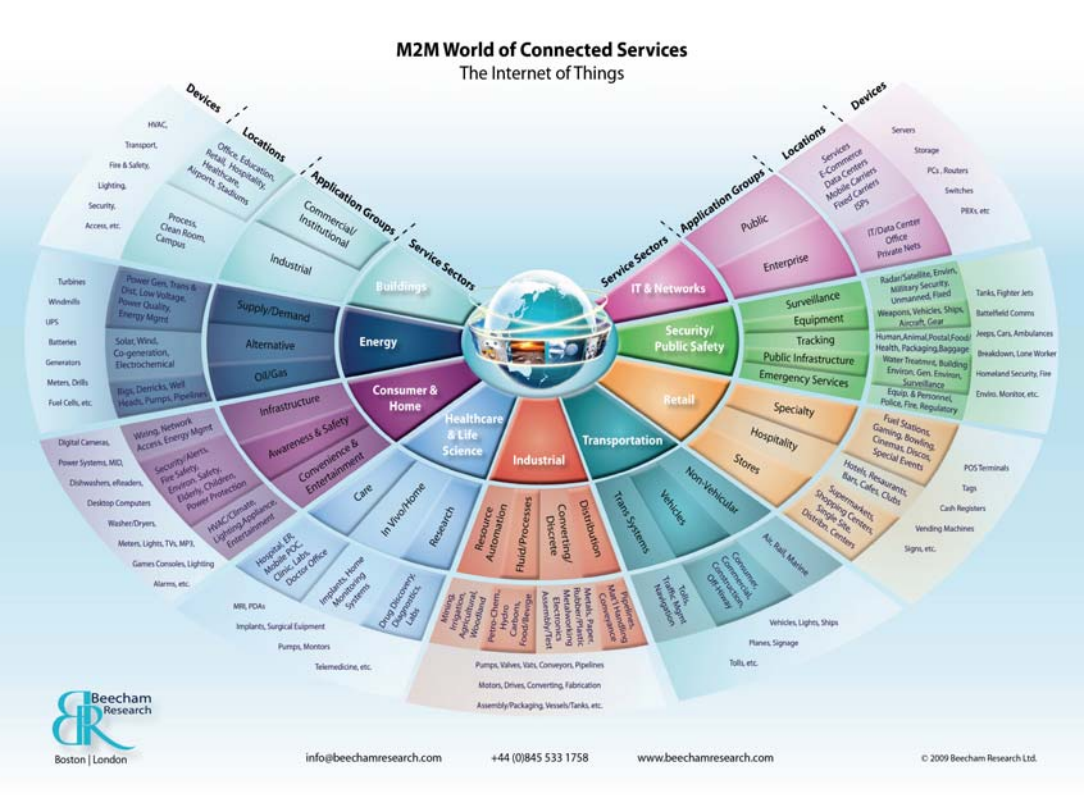
The IoT enables a very broad range of applications – from more efficient agriculture, manufacturing, logistics, counterfeit detection, monitoring of people, stock, vehicles, equipment and infrastructure, to improved healthcare, retailing, traffic management, product development and hydrocarbon exploration. It also enables new business models –

such as car and truck rental clubs, whose members can book and use vehicles parked around their neighbourhood almost on-demand; or "pay-as-you-drive" insurance based on precise driving patterns, behaviour, and risk.

The simplest IoT technology, passive Radio Frequency Identification (RFID) tags, is already widespread in retail, transit ticketing and access control. Near Field Communication (NFC) is now included in newer smartphones, with one prominent application being contactless payments via Visa's payWave and Mastercard's PayPass standards. Specialist sensors and processors in smart phones, watches, bracelets and clothes can collect, process and share data about individuals and their environments.

RFID and NFC only work at close range. M2M systems send information over cellular networks, such as electricity meter readings to energy companies, and car airbag deployment notifications to emergency services, with hundreds of millions of systems being deployed around the world, as shown in figure 2. Both have regulatory implications for licensing and spectrum management – discussed further below.

Figure 2: Machine-to-machine (M2M) services



Source: Beecham Research.

Many M2M devices use standard mobile Subscriber Identity Modules (SIMs) for identification and authentication. Unlike mobile phones, these devices are often located in diverse, unsupervised locations, and subject to wind, rain, large temperature changes, and vibration. To protect the SIM and also prevent theft in such situations, it is often attached permanently and securely to the device.[9]

M2M communications are often periodic and uplink heavy (especially if video is being streamed from cameras, sometimes in high definition), whereas many core and access communications networks are currently configured to support the downlink-heavy communications typical of Internet use.[10]

In the ITU-T model, communications network providers are responsible for:

- Access and integration of resources provided by other providers;
- Support and control of the IoT capabilities infrastructure;
- Offering of IoT capabilities, including network capabilities and resource exposure to other providers.[11]

Depending on the requirements of specific applications, there may be some degree of business integration between device, network, platform and application providers.

Box 2: China's large-scale M2M deployment

China is the world's largest M2M market, with 50 million connections by 2014. China Mobile, China Telecom and China Unicom are all developing large M2M businesses, with support from the Chinese government, which has identified IoT as an "emerging strategic industry" and is investing US$603bn in the M2M ecosystem in the decade to 2020.

The energy (including smart grid) and transportation (including freight tracking) sectors have been early adopters, with increasing demand in the automotive, smart city, healthcare, education and retail sectors. China Unicom connects BMW cars to the BMW ConnectedDrive service, providing embedded SIMs and hosting call and data centres. China Telecom's "Mega Eye" business supports 800,000 video cameras in 20 different industry sectors. The growth of 4G networks will further support applications such as video surveillance and in-car multimedia services.

Hundreds of Chinese cities are deploying smart city technologies, such as intelligent traffic management systems that adjust signals to ease congestion and help drivers find parking spaces, and to monitor pollution and noise sources. Mobile healthcare and education services are being developed to reach patients and schools in remote areas, as well as enhanced emergency response and home health monitoring applications, with Unicom developing smart ambulances that can send patient monitoring data ahead to the destination hospital. China Mobile has developed M2M applications to help farmers to remotely manage greenhouses and irrigation systems, and forest managers to monitor fire hazards.

Source: GSMA, How China is set for global M2M Leadership, June 2014.

3. Development trends and areas of application

The IoT sector has grown sometimes unevenly[12] over the last fifteen years, as hardware developments have made these technologies available at the low cost, size and energy consumption necessary. But many applications have been incremental improvements to existing business processes, developed by the incumbent firms that can afford the investment required. It may require the further growth and entry into new markets of businesses specialising in IoT services, along with further cost reductions, to enable the radical disruption of existing industries that is predicted by many technology companies and consulting firms.[13]

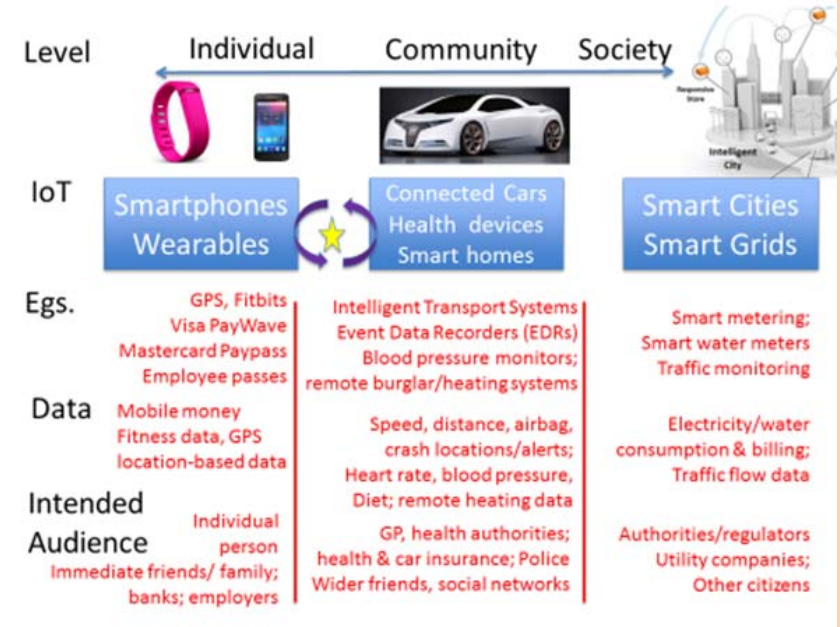
With Near Field Communication, smartphones can act as a universal platform for individuals to interact with IoT objects, removing one of the main cost barriers to growth. Payment, ticketing, vouchers, and customer loyalty applications will become cheaper and easier to manage, and allow much greater sophistication in pricing, marketing, product management and analysis. One company has forecast that around $36.05bn of NFC payments will be made worldwide in 2017, although this figure has been reduced by more than 40% from previous forecasts due to slower growth than expected to date.[14]

So far, IoT technology has been most broadly used in logistics and inventory management. Retailers can track products from the factory, through distribution networks – with real-time updates to orders and routes – to warehouses, into stores, triggering replacement when taken off the shelves, enabling customer self-payment, and replacing theft and shrinkage. Customer flow can be monitored continuously, enabling better retail layout. Shoppers can also take advantage of tags, using smartphones to access online information about products from the manufacturer, retailer, independent reviewers and friends, and even make price comparisons with other retailers. Customers can be given dynamic offers and shown display advertising based on their known preferences or demographics (the latter approximately determined by camera image analysis, and more precisely using signals from wireless devices such as smartphones). The use of data about individuals raises significant questions of privacy regulation, discussed below.

Manufacturers can embed sensors throughout their production processes, enabling much more precise control and hence increased efficiency and quality, while significantly lowering waste, energy use, the risk of accidents and product damage.[15] Similar techniques can be used through the whole lifecycle of equipment, vehicles, and the built environment, allowing for just-in-time repairs that minimise downtime and cost. And farmers can use IoT systems to carefully monitor soil and crop condition, precisely adjusting planting and pesticide use to maximize yield and minimise environmental impact, and enabling better food traceability.[16]

Businesses will likely be the biggest users of IoT technologies, with one analysis estimating that by 2019 enterprises will be using 40% – 9.1 billion – of deployed devices, with the highest-spending industry sectors being manufacturing, transportation and warehousing, and information.[17] Another analysis predicts that by 2020 there will be 2.1bn machine-to-machine device connections, with two-thirds of these in utilities industries, one-fifth in security applications, and smaller numbers in the automotive and transport sector, healthcare, government, retail and financial services. Applications will spread from developed to emerging economies, from limited commercial markets to a broad spread of consumer applications.[18]

Figure 2: Popular IoT uses



Source: ITU

Figure 2 and Table 1 show the areas where IoT usage is currently receiving the most attention from key ICT stakeholders, identifying possible developments. At the macro-level, two of the areas of greatest IoT development and investment are smart cities – where infrastructure and building systems will improve the efficiency and sustainability of a whole range of urban activities – and smart power and water grids. Closer to the individual, "connected vehicles" with hundreds of separate sensors will be safer, more reliable, and able to participate in sophisticated congestion management systems. And population health and wellbeing – a challenge to governments around the world as populations grow older, with a corresponding increase in age-related chronic conditions – could be significantly enhanced with IoT-based systems used by individuals, carers, primary care doctors and hospitals.

Table 1: Overview of some key areas of applications to-date

Areas of applications	Drivers	Examples	Possible development
Smart cities	Continued urban growth, presenting quality-of-life issues. By 2023, there are likely to be 30 cities with a population of over 20 million. Over half of these will be in India, China, Russia and Latin America.[19] Large public and private-sector investments, such as Saudi Arabia's US$70bn four "economic cities" project;[20] South Africa's US$7.4 billion smart city in	Monitoring and maintaining critical infrastructure such as roads, bridges, tunnels, railways, ports, communications, water and power.[23] Doha, São Paulo, and Beijing have used water pipe and pump monitoring sensors to reduce leaks by 40-50%.[24] Networked traffic signals dynamically manage traffic	Continued deployment of sensors and metering system will enable greater city coverage and new applications, as will greater availability of communications capacity; distributed, intelligent network analytics; and platforms for small/medium-sized businesses and software developer

	Modderfontein;[21] Masdar in Abu Dhabi; Accra in Ghana; Yachay in Ecuador; plans for over 100 smart cities in India; and an US$8bn smart city technology investment fund in China.[22]	movement across a city in response to measured and predicted changes in congestion and accidents. Congestion charging systems reduce vehicle commuting time by 10-20%.[25]	interaction.[26]
Smart meters and grids	Environmental sustainability – increase energy efficiency, reduce power consumption, especially at times of peak demand. Enable consumers to better understand and reduce energy usage, and switch to suppliers offering tariffs closer to their needs. Integrate variable renewable and home energy sources into grid. Fraud and theft can be remotely detected and meters disabled.	1.1 billion smart meters estimated to be installed by 2022;[27] 80 million in Japan, hundreds of millions in EU, and 150 million in India.[28] Smart water meters can enable leak detection. Installations in the US, Malta, India and Canada found an average reduction of water usage of 5-10%.[29]	Could save 33% of the total cost of constructing a grid using traditional methods.[30] Reduce downtime and waste through better load balancing and voltage regulation, and faster detection and diagnosis of faults.
Connected vehicles	Faster and more targeted emergency response to accidents. Enable drivers to monitor their car condition and driving habits, enabling them to improve vehicle reliability and fuel efficiency, as well as keep track of journeys. Pay-as-you-drive insurance. Stolen cars can be remotely tracked and disabled. Autonomous driving.	Worldwide, the top 14 car manufacturers, which account for 80% of the global market, all have connected vehicle strategies.[31] EU is close to agreeing requirement for all new cars and small trucks sold to feature an "eCall" system from April 2018.[32]	90% of consumer cars sold in the US by 2020 estimated to have an Internet connection, an increase of over 80% since 2013.[33] Cars share congestion and road problem data, enabling other cars to avoid congestion and notify repair and emergency services of problems. More efficient insurance markets, particularly for under-served groups such as young adults.
Healthcare	Improve efficiency and care in existing healthcare settings. Enable much greater use of remote telehealth provision, with greater patient comfort and lower cost. Let individuals monitor own health, improving wellbeing by better managing conditions such as stress, encouraging exercise and healthy eating, diagnosing medical conditions more quickly, and encouraging compliance with treatment regimes.	Patients with chronic conditions such as diabetes can monitor and report warning signs, using devices such as connected insulin pumps and blood-pressure cuffs. Annual cost of chronic conditions could reach US$15.5 trillion by 2025, with remote monitoring reducing this by 10-20%.[34]	"Quantified self" systems measure heart rate, breathing, temperature, sleep and brainwaves, and apps help users record diet and alcohol intake – increasingly, linked to user's smartphone.[35] Patients can share data to reassure carers and relatives, share advice in online patient forums, and volunteer information to medical researchers

4. Challenges and opportunities

The public and private sector are continuing to fund significant levels of IoT research and development, in areas such as modularity, reliability, flexibility, robustness and scalability.[36] But the basic capabilities needed for many applications are already well understood,[37] and becoming available through smartphones and other standard platforms. These devices will also address some of the cost issues that have held back growth in the past, although cost and reliability remain issues for large-scale systems, as does connectivity.

IoT technical standards have evolved from a variety of different applications and stakeholders, who have different aims and requirements, and more work is needed to integrate different standards frameworks.

A significant opportunity is the greater use of open data, platforms, and Application Programming Interfaces (APIs), which can enable a higher level of innovation in IoT systems.

Table 2 provides an overview of the various challenges and opportunities discussed in this section. It further identifies best practices and possible way forward.

Table 2: Overview of challenges and opportunities

What?	Why?	What is done today/best practice	Possible way forward
Cost and reliability	Most tags and readers not yet cheap enough to be ubiquitous. Limited consumer use of QR codes, and perceived negative impact on aesthetics. Costs can be too high for adoption by SMEs. Very high reliability requirements in large-scale systems with thousands of tags and devices. Power sources are challenging for cheap but long-life sensors. Large investments needed to take full advantage of "smart city" systems.	Ongoing development and deployment of cheaper, more efficient and reliable hardware and protocols. Innovation centres in countries to stimulate market entry and competition. Public-private partnerships and cooperation between municipalities, businesses and contractors to reduce costs and share resources.	Standardised functions in smartphones to interact with tags and sensors, including via web browsers. Great attention to aesthetics of tags, such as dotless visual codes.[38] Further R&D in areas such as energy scavenging, low energy protocols and algorithms, and high-reliability systems.
Connectivity	Application-specific networks and components can increase costs and reduce the opportunity to improve security and reliability. Mobile data networks still adapting to support large M2M systems.	Data from disparate systems integrated at data hubs, including cloud services. Many mobile networks have M2M business units and networks, with specialised business processes including charging and system integration to support large systems. Increased 4G deployment gives high throughput, low latency option for M2M.	Additional IoT support in next-generation cellular networks. R&D of more common middleware and APIs, and further standardisation of protocols for resource-constrained systems.

Standards (from the ITU and other organisations)	Technical standards have evolved for different applications and stakeholders, so harder to make them coherent. Smaller national markets may lack scale to support development of local IoT solutions, unless they are built on international standards. Specific software often needed per-system, increasing user load. Premature standardisation can constrain innovation; but partial or late standardisation can create industry coordination problems and fragmented technology options.	ITU has Global Standards Initiative to develop IoT standards and provide "umbrella" for other standards organisations. Wider-focus IoT and application-specific standards groups and frameworks.	Further cooperation between key standards bodies such as ITU, IEEE, IETF, IoT-specific standards organisations, and industry groups such as GSMA. Governments can encourage further standardisation through standards body participation (already prioritised in China, Korea and India), R&D funding and procurement policies. Development of common user interface mechanisms, especially via web browsers.
Open data and APIs	IoT data is often held in "silos" that are difficult to integrate without time-consuming data discovery and licensing. IoT platforms can be industry and vendor-specific, limiting opportunities for SMEs and startups to participate.	City and country initiatives to provide for the sharing of information by individuals and organizations under non-proprietary, open source licences.	Further work to encourage cataloguing of and contributions to open datasets. National and local government authorities are in a key position to do this, and could collaborate through Open Government Partnership.

4.1 Cost and reliability

For IoT to become a truly ubiquitous technology, the cost of tags, sensors and communications systems needs to fall to a level where they are a very small fraction of the total cost of the objects they are attached to, with readers also easily available. And even the cheapest (printed) tags, Quick Response (QR) codes, have not yet had a high response in consumer-targeted marketing campaigns. This is partly because specific software can be needed to read the codes, which is beyond the initial motivation of some users to install, and users need to position phone cameras so the code is in focus and can be accurately read.[39] In response, companies are developing more aesthetically attractive codes that can include images, such as the "dotless visual codes" being used by Chinese e-commerce giant Alibaba to combat counterfeits.[40]

High reliability levels also become important in large-scale systems that can include thousands of sensors, devices and readers. Trials of the most important RFID standard, EPC Global, by retailers such as Walmart and Tesco, found some difficulties in detecting tags due to product orientation and the blocking effect of nearby materials.[41]

Powered tags relying on batteries must minimise energy consumption, which is encouraging further research into and development of energy scavenging, low energy protocols and algorithms.[42] An example is Bluetooth Low Energy (BLE), which is supported by new smartphones. BLE tags advertise their presence by sending out a message every second, and can operate for up to one year using a lithium coin cell battery. They currently cost under $US5, which is likely to drop further.[43] Another example is EnOcean, which is an ultra-low power wireless standard that supports energy harvesting wireless technology for smart buildings. Such sensors can be powered entirely using motion, light or temperature differences.[44]

Due to the immature and fragmented markets for many IoT services, which increase development and operational costs, a Korean government review found limited application of IoT e-government pilot projects, and a low rate of introduction of IoT services in small and medium-sized enterprises (SMEs). To encourage new businesses to develop and use IoT applications, a number of governments (including Korea, China, India and the UK) are supporting the development of IoT business incubators and innovation centres, which include platforms and testbeds for startups and SMEs. These can increase market entry and hence increase competition and reduce cost.[45]

The most ambitious smart city projects, such as India's 100 smart sustainable cities project, are spending hundreds of millions of dollars to build more liveable and sustainable communities.[46] Creating city-wide infrastructure for smart cities needs a strong commitment from local governments and other authorities, as well as large investments and strong partnerships between municipalities, businesses and contractors. Laying new fibre-optic cables to increase the communications bandwidth available for smart city applications, for example, can be done more cheaply if contractors can take advantage of shared infrastructure (such as road trenches and utility tunnels) coordinated by a local authority.

This can be particularly effective when a smart city is built on a greenfield site. The ITU-T focus group on smart sustainable cities has developed focus group specifications for multi-service infrastructure in such new-development areas. It gives the example of the new Indian city Lavasa, where a single company has been appointed to establish, maintain, and grant rights to assets such as dark fibre, rights of way, duct space, and towers, on a lease/rent/sale basis to telecom services.[47] In existing cities, deployment of systems is much more likely to be on an incremental basis.

4.2 Connectivity

For IoT system designers, there is a choice between centralised, cloud-based functionality and more distributed applications, where some data is stored and processed on or near to sensors. Centralised systems allow a small number of powerful computers to manage large numbers of cheap devices – although those devices must have a network interface that can connect to the Internet or mobile phone networks.

This configuration has advantages when large amounts of sensor data must be brought together for processing. In a more distributed system, devices can send data to smartphones or other nearby computing devices over a local radio protocol such as Bluetooth, which process data before in some cases sharing it further across a global network. This increases system responsiveness to a local user, and can provide more privacy protection to data about people – which is especially valuable for sensitive information such as health data.[48]

Some radio protocols (such as Ultra-Narrow Band) can provide longer-range coverage, which can be useful for smart city applications such as streetlight management, video surveillance and environmental monitoring. Using application-specific networks can increase costs and reduce the opportunity to improve security and reliability compared to multi-purpose networks.[49] Where mobile phone network coverage is available, 2G and 3G networks can be used by most IoT applications. The increasing coverage of 4G cellular networks provides a high-throughput and low-latency option for higher-value IoT applications such as video surveillance.

The development of 5G cellular networks, expected to be deployed in the early 2020s, will provide a number of benefits for IoT applications, especially high-bandwidth ones such as video sharing. It will bring significant improvements in wireless communications, using smart radios and spectrum sharing with 1,000 times higher spectral efficiency. It will support cooperative relays and femtocells, enabling low-power sensors to communicate further while reducing the possibility of interference between communicating devices. It will include specific features to support device-to-device communication (such as traffic offloading), and explicit support for IoT/M2M systems.[50]

Industry association GSMA identifies sub-1ms latency and >1 Gbps bandwidth as defining features of 5G, noting that many of the other goals can be met gradually using existing protocols, and that autonomous driving, augmented and virtual reality systems and tactile Internet interfaces are the main technologies today that would require such low latency and high throughput. These could be used in gaming, telemedicine and manufacturing.[51]

5G will also likely support Software Defined Networking, allowing operators to run production and test networks above physical networks, and separate IP control and data planes, increasing security, and reducing expenditures. And it could provide support for running cloud computing in core networks, hence moving analytics closer to IoT edge devices.[52] SDN and femtocells are already being deployed in some 4G networks.

Where a company such as a smart meter operator is managing thousands or millions of M2M devices via mobile data networks, they have very different requirements from a typical mobile telephone customer. They need comprehensive network status information, to determine whether a non-communicating device or its network connection is faulty. They want a single subscription for the system, not on a per-device basis. And in many cases, the intended device lifetime will be much longer than individuals typically own a mobile phone – perhaps a decade or more. Replacing a device or even communications module within it will require either an expensive service visit, or a complicated process for customers that may cause faults. Not all mobile network operators can yet cope with these requirements, although many have set up specific business units to address them.[53]

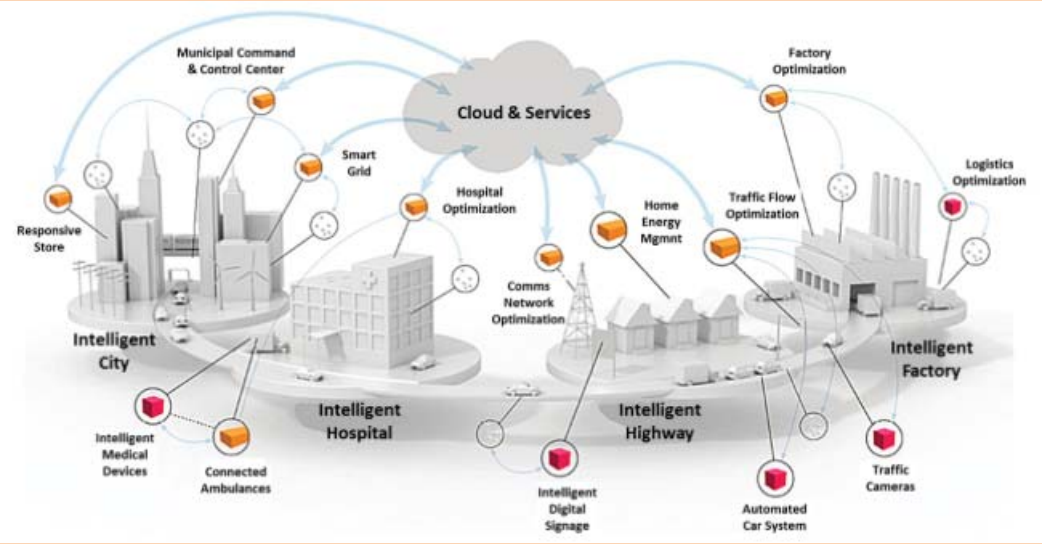
IoT systems are built on fixed and wireless communications standards, but it can still be difficult to connect together systems in different industry sectors or reuse system components. The great heterogeneity in Application Programming Interfaces and middleware (software components) makes it difficult to write applications that will run on different systems – therefore users often have to rely on a single set of applications for a single set of IoT components. More standardisation would enable more innovation, and enable information to flow between industry verticals like consumer electronics and the automotive industry. There is a need for interoperability (an issue covered further in another GSR discussion paper), connectivity, access control, service discovery, and privacy services, built on IoT-optimised protocols where necessary.[54] Greater configurability allows components to be used in a wider variety of systems, but can increase complexity and price.

Because IoT applications have strongly heterogeneous requirements, there is a need to fit different communications protocols to different applications – for example, using IoT-specific protocols such as the Constrained Access Protocol CoAP in resource-constrained systems. Most applications will be built around the Internet Protocol, except on very constrained devices. M2M devices can connect directly to other machines, but frequently there are gateways connecting IoT devices, which provide added value services such as

protocol conversion, filtering, caching; and back-end hubs – which can run on smartphones, gateways, or for global scale in the cloud.[55]

Even if integration of infrastructure and networks can prove challenging between organisations – whether public or private sector – data from disparate systems can still be integrated at data hubs, including cloud services.[56] Companies are building system frameworks to connect together disparate applications and networks via cloud services. One example is shown in Figure 3:

Figure 3: Intel's Intelligent Systems Framework



Source: Intel Corporation, Simplifying the Internet of Things: Intel® Intelligent Systems Framework, 2012.

Much of the value from IoT systems will come from integration of separate, proprietary silos, especially for large organisations with a broad range of partners – in the same way that development of shared technologies for personal computers, like operating systems and processors, enabled much greater levels of distributed innovation and consumer choice in the 1980s. Improved data sharing will also allow the development of specialised data analysis providers, who can increase the value of that data.[57] This does however depend on consumer trust in the security and privacy protection of the data (discussed further below).

4.3 Standards

To date, Internet of Things technical standards have evolved from a variety of different applications and stakeholders, who have different aims and requirements.[58] A universal and uniform network of "things" is unlikely to develop in the medium term. Smart meters are unlikely to communicate directly with heart rate monitors, or recipe planners; some networks will use public infrastructure, others will be entirely private; some applications have high bandwidth and interactivity requirements (such as video surveillance) while others may focus on transferring short bursts of information (such as smart meters). But with effective standards, these networks can be bridged.

Greater technical standardisation can both reduce the barriers to entry to IoT markets and increase economies of scale – the latter helping suppliers to compete internationally. Without this, national markets may face the issues identified in a Korean government review, where large businesses are developing IoT platforms, but lack leadership in the global market, which in turn makes it difficult for local SMEs to enter the market – and leaves them dependent on global suppliers.[59] However, the diversity of IoT systems and users means that there is a limited constituency actively pushing for standardisation.[60] Many of these users – for example in the healthcare sector – do not have a great deal of experience in communications standards bodies. Standards need to be carefully designed so they do not constrain innovation in still-young IoT markets. However, partial or too-late standardisation can complicate innovation due to industry coordination problems and fragmented technology options.[61]

In an effort to deal with these issues, the ITU-T has created a Global Standards Initiative on Internet of Things (IoT-GSI) to "promote… a unified approach in ITU-T for development of technical standards (Recommendations) enabling the Internet of Things on a global scale," and to "act as an umbrella for IoT standards development worldwide." This works with specific ITU-T IoT groups (a Joint Coordination Activity, and Focus Group on a machine-to-machine service layer), and the main ITU-T Study Groups (especially Study Groups 2, 3, 5, 9, 11, 13, 16 and 17).[62]

Other international communications standards bodies have ongoing IoT-related activities. The Institute of Electrical and Electronics Engineers (IEEE) considers IoT-related issues in a range of its communications standards, particularly 802.11 (Wi-Fi), 802.15 (Wireless Personal Area Networks), and 802.16 (broadband wireless), 802.3 (Ethernet), and 1901.2 (power line networks), as well as considering applications relating to the smart grid, energy, industrial, agriculture and mining sectors. It has created a draft standard (P2314) on an architectural framework for the IoT. The leading Internet communications standards body, the Internet Engineering Task Force (IETF), has considered IoT issues in its 6Tish (IPv6 access and meshing over deterministic (scheduled) MAC), IPv6 (Internet Protocol version 6), 6LoWPAN (IPv6 over Low power WPAN), RPL (Routing Over Low power and Lossy networks), MPL (Multicast Protocol for Low power and Lossy Networks), and CoAP (Constrained Application Protocol) working groups.[63]

There are a number of IoT-specific standardisation groups. The OneM2M group brings together manufacturers, service providers, end-users, and regional standards bodies from North America, Europe and East Asia.[64] It has developed a suite of standards for M2M and other IoT applications, including a set of security solutions.[65] Another IoT-specific group is the Industrial Internet Consortium, which includes some of the largest companies developing IoT technologies, such as AT&T, Inc., Cisco Systems Inc., General Electric, IBM, and Intel. The consortium is developing use cases, reference architectures and frameworks, and aims to influence global standards processes.[66] A third example is the AllSeen Alliance, a consortium that is developing the open source AllJoyn software and services framework. Members include consumer electronics companies such as Canon, Electrolux, LG, Panasonic and Sharp, as well as technology companies such as Microsoft and Qualcomm.[67] And the mobile industry association GSMA works with its members to drive M2M standardisation.

There are also IoT application-specific standards frameworks, such as the M/490 Smart Grid reference architecture, which can be reused in other IoT domains. This was created

following a specific mandate from the European Commission to European standards organisations, principally ETSI, CEN and CENELEC. These standards bodies are able to create standards that can be referred to by EU Regulations and Directives – one example of a mechanism by which policymakers can incentivise the creation and use of specific technical standards.[68] Another is for governments to support the development of standards and products implementing them using research and development funding, and prioritising the use of such products in government-funded programmes. Without such incentives, it can sometimes be in the interests of large companies to attempt to create their own proprietary *de facto* standards as barriers to entry to competitors.[69]

Many IoT systems will require very limited human interaction – for example, an on/off switch, or a bus stop notifying passengers of the time until the next bus arrival. Requiring a separate smartphone app or other type of software to interact with such systems will be an unnecessary burden for users. One suggestion for standardising the user interface to these systems is that they locally broadcast a Uniform Resource Indicator (URI), which is currently most commonly used to identify web pages. Other smart devices in range can then list and interact with such devices, via a web browser or more specialised software.[70]

4.4 Open platforms, data and APIs

A mechanism for encouraging much greater analysis and integration of IoT data is for individuals and organisations to share information under non-proprietary, open source licences. This makes it available for new applications without the need for time-consuming data discovery and licence negotiation.

One example is Amsterdam's Open Data programme, which has catalogued 438 datasets about the city.[71] Partners contributed to and analysed these datasets – including by designing a sensor to enable individuals to monitor and share pollution, noise and light intensity data from their neighbourhood. Amsterdam is also one of eight cities participating in a CityService Development Kit (CitySDK) project,[72] which lets programmers write software that can access data and shared IoT services via open Application Programming Interfaces (APIs) – such as services to improve transportation, help report problems to the city council, and guide tourists around places of interest.[73]

As part of the Amsterdam initiative, a number of "Living Labs" have been set up in communities to experiment with smart city initiatives, identifying successful ideas so they can be implemented across the city. An example is in IJburg, which has "projects like free Wi-Fi and a new Fiber network, personalized television and transportation services, and a co-working space allow residents to experiment and test city projects to improve healthcare, environment, and energy programs in the city."[74]

Another example of the use of open source approaches is in the Korean government's IoT master plan. The government will collaborate with the private sector to develop an open IoT platform, and all ministries will be encouraged to collaborate with businesses across the entire country. This will stimulate an open IoT ecosystem, which is intended to improve interoperability, reduce costs through economies of scale and scope, and enable flexible responses to environmental changes. A test-bed for small and medium-sized enterprises will reduce development costs and time-to-market, and support collaboration between businesses in different areas. The ecosystem will support startups to turn ideas into

businesses, using tools including open source hardware (circuit diagrams, board plans, and specifications required for hardware development) and software, and DIY open labs.

5. Policy and regulatory implications and best practices

The deployment of IoT systems, and their potential impact on individuals and businesses, raises regulatory issues – some familiar to telecoms regulators, such as licensing, spectrum management, standards and competition, and others where a lead is often taken by other regulators, such as data protection, privacy and security.

A 2013 European Commission consultation exercise found a diversity of views on whether IoT-specific regulation is necessary. Industry respondents argued that state intervention would be unwise in this still-young sector, and that general rules such as the EU's forthcoming Data Protection Regulation will suffice. Privacy advocacy groups and academics responded that IoT-specific regulation is needed to build public confidence, as well as to ensure a competitive market.[75] Meanwhile, an FTC staff report suggested that IoT-specific legislation would be "premature". It instead encouraged self-regulatory programs for IoT industry sectors to improve privacy and security practices – while also reiterating the FTC's previous call for "strong, flexible, and technology-neutral federal legislation" to strengthen its ability to enforce wider data security standards and require consumer notification following a security breach, and for broad-based privacy legislation.[76]

This section reviews actions taken by regulatory agencies that will enable the development and adoption of IoT systems in a way that maximizes their societal benefit (see Table 3).

Table 3: Overview of policy and regulatory measures taken

What?	Why?	What is done today/best practice
Licensing and spectrum management	Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands.	Monitor availability of spectrum for short and long-range IoT communications and backhaul network capacity, and encourage 4G deployment and use of small-cell technology.
Switching and roaming	Standard mobile telephony network SIMs and accounts unsuitable for large M2M users, mobile devices, and fixed devices in areas of poor reception.	Mobile network operators develop M2M-specific business units with appropriate billing and management. Further development and deployment of embedded, remotely provisioned SIMs in M2M systems.
Addressing and numbering	Very large address space needed for globally addressable things.	Deployment of IPv6 by ISPs, public and private sector organisations. Use of IMSI for M2M applications.
Competition	Some market configurations of IoT services could strengthen position of large firms and increase potential for consumer lock-in. Limited user access to raw IoT data reduces ability to switch providers (and to understand privacy implications).	Ensure competition regulators have capability to monitor IoT markets for abuses of dominant positions. Provide institutional mechanism for ongoing review of laws and regulations for impact on IoT competitiveness.
Privacy and security	Security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles. Many IoT companies have little Internet	Ensuring security and privacy from outset of IoT system design process. Development of co-regulation by all stakeholders to protect security and privacy. Further development of privacy and

	security expertise. IoT device resource and connectivity constraints make security and vulnerability patching more difficult. Smart city vulnerabilities can be hard to fix but present significant safety issues (e.g. in traffic lights). Innocuous sensor data can be linked together to create detailed individual profiles, and used to infer sensitive personal information, such as medical disorders. This may lead to discrimination in employment, financial and healthcare services.	consumer protection rules to ensure security testing of IoT systems that process sensitive personal data.

Box 2 describes one notable example, India's programme to develop 100 smart cities and highlights a number of policy and regulatory issues raised by the Telecom regulator, TRAI.

Box 2: India's smart cities programme

India is continuing its rapid pace of urbanization, and expects its urban areas to contribute almost 75% of GDP within 15 years. To improve efficiency, employment opportunities and quality of life, the government has embarked on a programme to create 100 smart sustainable cities (SSCs), consisting of 80% public-private partnership and 20% public-funded basic infrastructure.

"Smart" services will include transport, building planning, water supply, solid waste management, sewerage and sanitation, electricity, Wi-Fi connectivity, health care and education, with a total investment of USS113bn over 20 years. They will be built around an Internet Protocol core network, broadband access network, building sensing and analytical capabilities, and provide e-services to citizens. Shared infrastructure will include Wi-Fi in all public places; and small cell deployment for high speed/capacity links.

TRAI, India's telecoms regulator, has identified a number of policy and regulatory issues raised by SSCs. These include how to encourage sharing of common assets and resources; ensuring spectrum availability for reasonable quality of service, and avoiding electromagnetic frequency issues with large-scale wireless sensor deployment; identifying and developing open standards, especially to enable operability between sectors; data security; a numbering and addressing plan, including customer addresses for M2M devices; and security and lawful interception for M2M devices.

Source: Telecom Regulatory Authority of India, Smart Sustainable Cities - Policy and Regulatory Issues for India, 2015.

5.1 Licensing and spectrum management

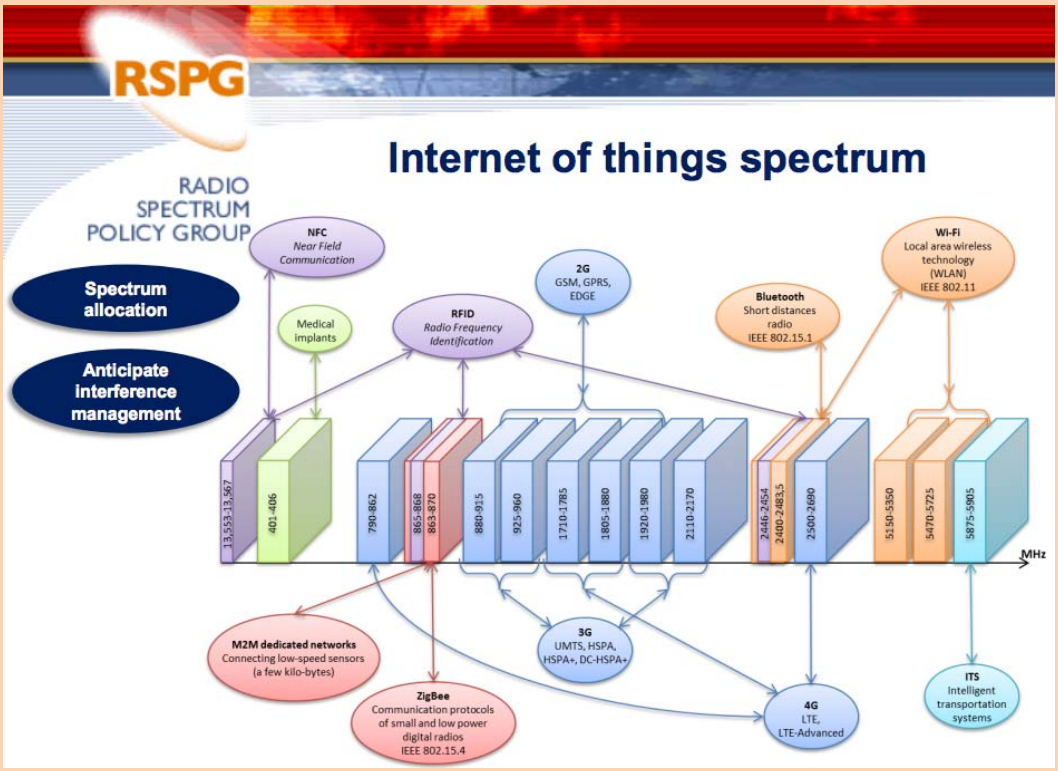
Licensing and spectrum management is an important issue for ensuring availability and capacity for IoT communications. IoT devices communicate using a range of different protocols, based on their connectivity requirements and resource constraints. These include short-range radio protocols such as ZigBee, Bluetooth and Wi-Fi; mobile phone data networks; and in more specialised applications such as traffic infrastructure, longer-range radio protocols such as Ultra-Narrow Band (UNB).

To communicate to remote networks, IoT devices may send data via a gateway with a wired (PSTN, Ethernet, power line or DSL) or wireless (2G, 3G, 4G/LTE or UNB) connection to the global Internet or telephony network – or directly over one of these mediums.[77] For

consumers, the gateway will often be a smartphone or home wireless router. Businesses will frequently make use of their existing corporate data networks.

Devices communicating over kilometres need access to the 300 MHz to 3GHz spectrum area, while centimetre or millimetre contactless transactions may use near field communications at 13 MHz or EHF bands (as shown in figure 4). Some IoT applications may also make use of AM/FM bands in the VHF range. Telecommunications companies are experimenting with white space spectrum to make more use of often-unused spectrum bands, while a US presidential commission has recommended the development of shared-space technology that enables government, licensed commercial users, and unlicensed users to cooperatively make use of a large amount of spectrum.[78]

Figure 4: IoT spectrum



Source: Radio Spectrum Policy Group.

The US Federal Communications Commission (FCC)'s expert IoT working group predicts IoT will add significant load to existing services such as Wi-Fi and 4G mobile networks. Regulators will need to give continuing attention to the availability of spectrum for short-range IoT communications, and the capacity of backhaul networks that connect IoT gateways to the Internet, as well as encouraging the roll-out of small cell technology such as 4G. If these conditions are met, the working group does not expect that new spectrum will need to be explicitly allocated to IoT communications.[79]

The FCC is also reviewing the use of spectrum above 25 GHz for 5G networks, and possibly the IoT.[80] The Korean government plans to secure additional frequency of at least 1GHz by

2023 and ensure 5G is commercialised by 2020 in response to the "exponential growth" it expects in IoT traffic.[81]

Studies for the European Commission have suggested that a licence exempt model is most effective for IoT development, since it avoids the need for contractual negotiations before devices are manufactured and used, allowing the production of large numbers of cheap devices.[82] Most current systems use unlicensed frequencies in the Industrial, Scientific and Medical (ISM) bands, including sub-kHz for video surveillance and access control, the Medical Implant Communications Service (MICS) in the 400 MHz band, and 900 MHz for the EPC RFID standard. The generic Bluetooth, ZigBee and Wi-Fi standards also work in unlicensed spectrum.[83]

One example of a specific long-distance IoT-focused communications system, SIGFOX, uses the most popular European ISM band (the ETSI and CEPT-defined 868MHz) and the FCC-defined 902MHz band in the USA.[84] A Korean government review found an increasing demand for unlicensed, low-power, long distance communications to connect devices in remote areas.[85]

5.2 Switching and roaming

Firms operating large networks of M2M devices via mobile telephony networks, with a fixed SIM in each device, may not find it easy to switch network at the end of a contract, or if a device roams into a different network area or for some time period could get better service from a different provider. This roaming capability is important for devices that move between countries, and also for fixed location devices that may be used in an area of short or long periods of service unavailability – often indoors.[86]

Some technical standardisation work has been done to enable such services, with some of Apple's latest iPads including SIMs that make it easier for users to switch between mobile networks, and leading SIM supplier Gemalto supplying reprogrammable SIMs for smart watches. The first steps have been taken in this direction in the Netherlands, which in 2014 allowed SIMs to be issued by organisations other than mobile network operators, such as utilities and car companies.[87] The GSMA has developed standards for remote M2M device management, which are being supported by mobile operators including China Unicom and Telefónica.[88]

Greater flexibility and competition would be possible if large IoT operators were able to act similarly to mobile virtual network operators – not least because they could then have wholesale access to mobile networks.[89] The German network regulator *Bundesnetzagentur* consulted on the market for IMSIs in late 2014.[90] An OECD analyst estimated that if German carmakers were able to issue their own SIMs and rent spare capacity on mobile networks, they could save US$2.5 billion per year through lower prices and more flexible contracts.[91] The Belgian communications regulator BIPT is also consulting on the national number plan.[92]

The European Conference of Postal and Telecommunications Administrations (CEPT) Electronic Communications Committee has recommended that SIMs whose IMSI can be remotely updated should be implemented as soon as possible, and that CEPT countries consider great flexibility in assigning Mobile Network Codes (MNCs) to IoT service providers. It has also encouraged the ITU-T to consider updating Recommendation E.212 to explicitly

allow this flexibility, as well as to plan for the future use of MNCs to support a broader range of services.[93] These changes have been under consideration in ITU-T Study Group 2.

5.3 Addressing and numbering

IoT devices may have a globally unique and routable communications address (requiring a very large protocol address space, such as that of IPv6); an address assigned by a gateway that allows limited inter-network connectivity; or make use of local networks only, to share data with and receive instructions from a nearby controller, such as a personal computer, smartphone, or specialised management device – in which case a globally-unique address is not required.

Enabling peer-to-peer connections between devices can increase the reliability of communications, compared to requiring a large and complex global network, and matches the common use case of an individual discovering and interacting with nearby devices. But where devices must be globally reachable – most likely, via the Internet – a large address space is required to individually identify each one.

The number of unallocated addresses for the current version of the Internet Protocol (IPv4) is extremely limited, but the new version (IPv6) being rolled out by ISPs around the world has enough addresses for almost any conceivable number of devices.[94] The transition from IPv4 to IPv6 has taken longer than expected, and policy makers may need to continue with programmes to encourage the transition in the medium term. The US government, for example, set up a Federal IPv6 Task Force to move all federal agencies from IPv4 to IPv6, with one aim being to encourage the private sector to do the same. Many other countries have also set up IPv6 Task Forces to encourage national transitions.

For any IoT identification scheme, there will be trade-offs between performance, scalability, interoperability, efficiency, privacy preservation, ease of authentication, reliability, flexibility, extensibility, and mobility support. As well as IPv6 addresses, the other main identification standards being developed are from ISO and GS1, as well as ITU-T Recommendation E.212 for the use of the International Mobile Subscriber Identifier (IMSI) for machine-to-machine communications.[95] The latter has the advantage of a well-developed authentication, payment and global roaming framework, operated by mobile telephony providers, with hardware security based on SIMs.

5.4 Competition

IoT technologies will likely have a range of impacts on the competitiveness of different markets. In the short term, firms adopting IoT systems will have better information on their business processes, enabling an increase in efficiency and more flexible responses to supply, processing and demand shocks. This could strengthen the market position of larger firms that have greater access to capital (to build their own IoT infrastructure) or brand loyalty (to increase sales volume to cover the price of third-party IoT services). For products with network effects (the purchase of a product increases its value to existing purchasers – for example, telephone service, where a new customer can call and be called by all existing customers), greater sales volumes can increase the likelihood of consumers being locked in to existing suppliers[96] – especially if the supplier uses non-standard interfaces and sells complementary services.

Over time, if IoT technology is adopted in ways that require high capital spending, increase firms' pricing power, or strengthen network effects, then adopters can drive out competitors. Market structure will also be affected if large companies can build their own IoT systems but smaller companies have to subscribe to them, or connect to networks of larger firms. If a "core" of large businesses adopt IoT, this could increase competition between them while reducing competition between core and peripheral firms. This could benefit consumers by turning quality-based competition into price competition. But if firms feel they have to adopt IoT simply because competitors have, this could lead to overinvestment by incumbent firms and reduced entry into those markets by firms not willing to make this investment.[97]

An important aspect affecting competitiveness of IoT systems in the longer term is the extent to which end-users can gain access to the raw data gathered and stored by components. Systems usually extensively process sensor data so that it is more useful when presented to users. While this makes systems more user-friendly, it reduces the ability of users to transfer data to different providers if a better service is offered (as well as to understand what inferences could be drawn about them from the data).[98] It also makes it more difficult for end-users to combine systems from different providers – which could become a competition issue if a provider becomes dominant in one area, and tries to extend that dominance into other areas by blocking interoperability with competitor systems.

One example of regulatory activity to promote competition is Korea, where the government's Telecommunications Strategy Council has been given responsibility to adapt existing laws and regulations to ensure a liberal and competitive industrial environment for IoT. Where the Council finds regulations that hinder ICT convergence, it can request related ministries to improve these regulations. For new products and services, attention will be given to prompt processing and interim licensing.[99]

At this relatively early stage of IoT market development, it is not clear whether it will support "more than a relatively small number of very large players", as is the case with existing Internet markets such as search and advertising. Competition regulators will need to keep under review whether *ex post* investigations of abuse of dominant positions will be sufficient to foster a competitive market and rapid innovation, including the ability of start-ups and individual entrepreneurs to create new products and services.[100]

5.5 Privacy and security

Privacy and security are two significant (and closely related) issues in large-scale IoT deployment. There are already technologies available that address some of the underlying technical issues, particularly in sensors – such as key diversification and reader authentication. But these can have a significant impact on device size, cost, functionality and interoperability.[101]

Without adequate security, intruders can break into IoT systems and networks, accessing potentially sensitive personal information about users, and using vulnerable devices to attack local networks and devices. This is a particular issue when devices are used in private spaces, such as individuals' homes, for example with baby monitors. The operators of IoT systems, and others with authorised access to the data produced, are also in a position to "collect, analyze, and act upon copious amounts of data from within traditionally private spaces."[102]

Electronic attacks could also lead to threats to physical safety, for example if carried out against medical devices like pacemakers and insulin pumps, or car engines and brakes. Information about building occupancy could be used by burglars to target unoccupied premises, while location-tracking data might enable physical attacks against specific individuals.[103]

If compromised IoT devices can connect to systems elsewhere on the Internet, this provides a potential route for further attacks. One security company announced in 2014 it had discovered hundreds of home devices – including smart fridges – sending unsolicited e-mail. While a further analysis found this to be inaccurate, it also warned of recently discovered malicious software targeting Linux-based IoT devices.[104] Another common security and privacy issue is the use of default passwords on devices, which users are not required to change when setting up a device. One website has claimed to find 73,000 webcams accessible over the Internet using a default, known, password.[105]

IoT devices can be harder to secure than personal computers. Many companies building IoT devices do not have previous experience of dealing with Internet security issues in their products. IoT devices are often inexpensive and resource-constrained (notably on power and battery life), which puts strong pressure on security costs and additional hardware or software to deal with threats. Combined with the limited Internet connectivity of some devices, this may make it more difficult to develop and apply regular security patches when vulnerabilities are discovered – and for companies to afford ongoing support.[106] But most IoT devices contain multipurpose computers and can be reprogrammed beyond their intended purpose – with limited mechanisms for users to monitor the device. And they frequently share operating systems, embedded chips and drivers, meaning that a single vulnerability can often be used to attack a wide variety of devices.[107]

In large IoT systems such as smart cities, IoT insecurity can create significant vulnerabilities, and be extremely complex to address given interdependencies and links to older public and private sector systems. One 2014 threat assessment found 200,000 vulnerable traffic control sensors in cities including Washington DC, New York, Seattle, San Francisco, London, Lyon, and Melbourne. The assessment also found such vulnerable technologies being developed and used in critical infrastructure without security testing, and that it can be difficult for third-party security researchers to gain access to devices to carry out their own tests, due to their expense and limits on sales to governments and specific companies.[108]

Companies developing and operating IoT systems will need to conduct security testing, and consider how security vulnerabilities discovered after devices are sold can be fixed during their likely lifetime. Where security flaws cause consumer harm, consumer protection agencies may be able to take action to require those harms be remedied, and better security processes be put in place to reduce the risk of them recurring.[109] EU rules require organisations processing personal data from IoT systems to carry out security assessments, and make use of relevant security certifications and standards.[110] And companies need to ensure that where they use external service providers to manage IoT devices and data, those providers also take reasonable security precautions.

To meet these security and privacy challenges, regulators have suggested that companies developing IoT devices should follow a security and privacy "by design" approach, building security and privacy functionality into the device from the outset of the development process, when it is much more likely to be effective.[111] The 2014 international conference of

privacy regulators declared that this "should no longer be regarded as something peculiar. [It] should become a key selling point of innovative technologies."[112] That said, there is so far little evidence of market demand for privacy-friendly services – partly because of the difficulties for individuals in assessing and weighing up complex privacy risks. And while regulators have been discussing privacy by design for over a decade, the specifics of implementation have so far only been developed to a limited extent.[113]

Companies can undertake Privacy Impact Assessments when designing IoT systems, to consider how different design options have different privacy effects. This can also reduce the risk of the need for expensive delays and redesigns of systems that are found to be non-compliant with privacy rules – as was extensively debated during the development of the Netherlands' smart meter programme.[114]

A significant amount of work has already been done on security and privacy issues by policymakers and regulators in the EU and USA. Under the General Data Protection Regulation being debated in the European Parliament and Council of Ministers, there will be stronger regulatory incentives for companies developing systems that process personal data to protect security and privacy by design. The US Federal Trade Commission (FTC) also suggests companies follow a "defence in depth" approach, considering security measures at several different points in their systems, such as using access control measures and encrypting data even when users are making use of encrypted links to home Wi-Fi routers (which will not protect the data between the router and the company's servers, or if the router is badly configured).[115]

Privacy is a particularly strong regulatory issue in European countries, where it is included in a comprehensive legal framework that includes the Council of Europe's European Convention on Human Rights and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the EU Charter of Fundamental Rights. This framework has been influential in the development of comprehensive privacy laws now in force in over 100 countries around the world.[116]

The EU already has a very detailed legal framework regulating the public and private sector's use of personal data, with a general Data Protection Directive (95/46/EC) relevant to IoT device manufacturers, social media platforms and app developers that access IoT data; and an e-Privacy Directive (2002/58/EC) also relevant to IoT device manufacturers.[117] The European Commission has already sponsored a process to create an RFID privacy code of practice, developed collectively by industry and civil society and approved by the EU's data protection authorities.[118]

These authorities have issued a detailed opinion on the implications of the Internet of Things for privacy protection. They note the IoT produces high-volume flows of personal data that could present challenges to traditional data protection regulation – for example, since individuals will not necessarily be aware when data is shared, or able to review this data before it is sent to other parties, creating a risk of self-exposure and lack of control.[119]

A further privacy issue is the amount of personal information that can be derived from seemingly innocuous sensor data, especially when it is combined with user profiles and data from other sources. As European privacy regulators noted, "Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed."[120] Smart meter data, for example, can

be surprisingly revealing of individuals' day-to-day activities – down to the detail of which programmes are being watched on a television.[121] Researchers have found that smartphone sensor data can be used to infer information about users' personality types, demographics, and health factors such moods, stress levels, smoking habits, exercise levels and physical activity – even the onset of illnesses such as Parkinson's disease and bipolar disorder.[122]

This kind of information has obvious applications, such as in pricing health insurance; but also for other decisions related to employment, credit and housing. This could lead to economic discrimination against individuals classified as poor credit and health risks, and potentially to "new forms of racial, gender, or other discrimination against those in protected classes if Internet of Things data can be used as hidden proxies for such characteristics."[123]

To protect individuals' privacy, the FTC has suggested that notice and consent be required when personal data is collected by IoT applications outside the reasonable expectation of consumers, based on the context of transactions and companies' relationships with consumers. Similarly, the EU data protection authorities have noted that IoT data collected for one purpose may be analysed and matched with other data, leading to a range of secondary purposes – which should be compatible with the original purpose of collection and known to the user (this is known as purpose limitation).

IoT data collection and analysis could particularly affect privacy when it includes data from private spaces like homes and cars, and even make it difficult for individuals to go about their daily life in the largely anonymous way they took for granted.[124] When IoT applications process personal data that can reveal "sensitive" data under EU data protection law – racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life – explicit consent is required from the individual concerned.[125] Under EU law, individuals must be able to withdraw their consent to all or specific data processing at any time, without "any technical or organisational constraints or hindrances" using tools which are "accessible, visible and efficient."[126]

A range of mechanisms could be used to obtain consent, including choices at point of sale or device setup; QR codes or barcodes on a device that could take a user to a website; privacy dashboards, for example in smartphones; and by learning from consumer behaviour, such as through privacy preferences set on other related devices.[127]

Data minimisation remains an important privacy-protective principle for consumer IoT devices, limiting the amount of personal data collected or retained, and hence reducing risks from data breaches and use of the data in ways not expected by consumers. The FTC foresees more flexibility for IoT services in collecting data not initially required to provide a service, while under stricter European rules the EU data protection authorities "cannot share this analysis".[128]

Table 5 below identifies possible measures regulators can consider to foster development of the IoT.

Table 5: Potential regulatory measures

	Potential regulatory measures
Licensing and spectrum management	Further experimentation with use of white space and shared-space technology. Encourage development of LTE-A and 5G networks, and keep need for IoT-specific spectrum under review.
Switching and roaming	Global agreement on updated E.212 standards, making appropriate use of GSMA standards, and provision of Mobile Network Codes to IoT service providers.
Addressing and numbering	Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption.
Competition	Consider measures to increase interoperability through competition and consumer law, and give users a right to easy access to personal data. Support global standardisation and deployment of remotely provisioned SIMs for greater M2M competition.
Privacy and security	R&D on more hardware and software security and privacy mechanisms for resource-constrained IoT systems, particularly targeted towards start-ups and individual entrepreneurs that lack resources to easily develop this functionality. Incentives for companies to develop new mechanisms to improve transparency of IoT personal data use, and for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn. Greater use of Privacy Impact Assessments by organisations building and configuring IoT systems. Development of further guidance from global privacy regulators on application of the principles of data minimisation and purpose limitation in IoT systems. More cooperation between telecoms and other regulators such as privacy/data protection agencies.

6. Conclusions

While it is difficult to make precise forecasts about the global impact of the Internet of Things, analysts seem almost unanimous that it will be extremely significant – with tens of billions of devices deployed, and trillions of dollars of annual impact within the next decade. IoT technologies could make an important contribution to global challenges such as improving public health and quality of life, moderating carbon emissions, and increasing the efficiency of a range of industries across developed and developing economies.

The pace of IoT deployment will partly depending on meeting the challenges currently facing the development of cheaper, more reliable, well-connected systems. Common networks, technical standards, system components, and infrastructure, as well as strong public-private partnerships, can reduce the costs of IoT systems. Open data and platforms can make it easier for new systems to be developed, especially by individual entrepreneurs, start-ups and SMEs. Innovation centres and incubators can further encourage new businesses to enter IoT markets, increasing competiveness. Governments can take further steps to encourage national transitions to IPv6, updating all their own systems and providing incentives to private sector providers to do so, hence ensuring addresses are available for all IoT devices that connect directly to the Internet.

Large-scale IoT systems like smart cities and international logistics chains need very cheap sensors that can last for long periods of time without needing repairs or new power sources, as well as the bandwidth to share data – whether infrequent bursts, or streams of high-

resolution video. M2M systems need continued growth in coverage of 3G and 4G networks, and support for remotely provisioned embedded SIMs for more reliable and competitive communications.

This is the area where telecoms regulators can have the greatest impact, by supporting the continued development and deployment of high-speed cellular networks, and keeping under review the need for IoT-specific spectrum. Decisions on licensing and spectrum management are important to ensure IoT systems can be developed cost-effectively, and have the necessary bandwidth to communicate. By agreeing updated standards (such as the ITU's Recommendation E.212) and providing Mobile Network Codes to M2M service providers, better services could be provided at a significantly lower cost. In the long run, shared-space technology has the potential to offer much greater bandwidth for IoT and other communications services.

The widespread use of common technical standards will be key to a low-cost, interoperable IoT, and can be encouraged by continued cooperation between standards bodies, and government support for standards use and participation. National and local government authorities can stimulate the availability of open IoT datasets, platforms and components. Municipal governments are playing a key role in smart city and open data programmes, and can find it easier to experiment with new technologies and policies suited to local conditions than national governments.

Some countries are taking a relatively hands-off approach to IoT regulation, with the focus of promoting economic growth and innovation. For example, the Korean government has recently planned to reduce IoT (as well as e-commerce and Internet finance) regulation to support a dynamic ecosystem for future growth, while still protecting users, preventing abuse of market dominance and protecting Internet networks, and will decide on which restrictions to maintain through social consensus.[129] Other countries and regions – notably the European Union – are taking a more pro-active approach to protect social values such as privacy as the IoT develops, while still paying strong attention to the need to promote the economic benefits of the technology. Such strategic decisions are political ones that can only be taken by national governments, while sharing evidence and best practice through international forums such as the ITU.

Regulators can play a role in encouraging the development and adoption of the IoT, while promoting efficient markets and the public interest. Competition regulators will need to keep under review whether *ex post* investigations of abuse of dominant positions will be sufficient to foster a competitive market and rapid innovation. Particular attention will be needed from regulators to IoT privacy and security issues, which are key to encouraging public trust in and adoption of the technology. While many telecoms regulators already have responsibility for network security, this is an area where they could do more by cooperating with national privacy and consumer protection regulators to encourage development of a trustworthy IoT.

References

[1] The author is grateful for suggestions and comments on earlier drafts by Rudolf van der Berg, Mailyn Fidler, Simon Forge, Ben Hawes, Gilad Rosner, and ITU staff.

[2] Cisco Systems, *Internet of Things Connections Counter*, at http://blogs.cisco.com/news/cisco-connections-counter

[3] Gartner, *Forecast: The Internet of Things, Worldwide, 2013*, at https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-

[4] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson and A. Marrs. *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, May 2013, p.51.

[5] J. Bradley, J. Loucks, J. Macaulay and A. Noronha, Internet of Everything (IoE) Value Index, *Cisco White Paper*, February 2013, at http://www.cisco.com/web/about/ac79/docs/innov/IoE-Value_Index_White-Paper.pdf

[6] International Telecommunication Union – Telecommunications Standardization Sector, *Overview of the Internet of things*, Recommendation ITU-T Y.2060, June 2012, s.I.1.

[7] ITU-T Recommendation Y.2060, note 6, s.8.4.

[8] GMSA, *Understanding 5G: Perspectives on future technological advancements in mobile*, December 2014, p.10, at https://gsmaintelligence.com/research/2014/12/understanding-5g/451/

[9] GMSA, note 8, pp.7-10.

[10] Sasu Tarkoma, *Evolution of Internet based applications: Internet of Things, 5G and smart devices*, Helsinki public lecture, 3 April 2014, at http://livestream.com/ITstriimIT/Hetky-THkerho--IoT-5G/videos/46998469

[11] ITU-T Recommendation Y.2060, note 6, s.I.1.2.

[12] M. Malone. Did Wal-Mart love RFID to death? *Smart Planet*, 14 February 2012.

[13] J. Esmeijer, A van Veenstra, T. Bakker, A. van Nunen, B. Kotterink and M. Ooms. *New sources of growth: Knowledge-based Capital*, OECD, 2015.

[14] Gartner. *Forecast: Mobile Payment, Worldwide, 2013 Update*, 4 June 2013.

[15] M. Chui, M. Löffler and R. Roberts. The Internet of Things. *McKinsey Quarterly*, March 2010, pp.1-9, at http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things

[16] Esmeijer et al., note 13.

[17] Business Insider Intelligence Estimates, 22 Dec. 2014, at http://uk.businessinsider.com/the-enterprise-internet-of-things-market-2014-12

[18] S. Hilton, *Imagine an M2M world with 2.1 billion connected things…* Analysys Mason, 27 January 2011.

[19] Frost & Sullivan, *Mega Trends: Smart is the New Green*, at http://www.frost.com/prod/servlet/our-services-page.pag?mode=open &sid=230169625

[20] Cisco Internet Business Solutions Group, *Saudi Arabia Invests US$70 Billion in Economic Cities Project*, July 2009, at https://www.cisco.com/web/about/ac79/docs/success/Saudi_Arabian_General_Investment_Authority_SAGIA_Engagement_Snapshot.pdf

[21] NewsCentral Media, PCCW to connect Modderfontein 'smart city', *TechCentral*, 22 April 2014, at http://www.techcentral.co.za/pccw-to-connect-modderfontein-smart-city/47706/

[22] Kieron Monks, Wire the desert: The next generation of smart cities, *CNN*, 18 December 2014, at http://edition.cnn.com/2014/12/18/business/smart-cities-next-generation/

[23] Robert E. Hall, The Vision of a Smart City, *2nd Life Extension Technology Workshop*, Paris, 28 September 2000, p.2, at http://ntl.bts.gov/lib/14000/14800/14834/DE2001773961.pdf

[24] Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.57.

[25] Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.56.

[26] S. Mitchell, N. Villa, M. Stewart-Weeks and A. Lange. *The Internet of Everything for Cities: Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities*, Cisco Systems, 2013.

[27] Navigant Research, *The Installed Base of Smart Meters Will Surpass 1 Billion by 2022*, 11 November 2013, at http://www.navigantresearch.com/newsroom/the-installed-base-of-smart-meters-will-surpass-1-billion-by-2022
[28] Navigant Research, Smart Electric Meters, *Advanced Metering Infrastructure, and Meter Communications: Global Market Analysis and Forecasts*, November 2013, at http://www.navigantresearch.com/research/smart-meters
[29] Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.57.
[30] GB Smart Grid: a race worth winning?: a report on the economic benefits of smart grid, Ernst & Young, 2012, https://www.smartgrid.gov/sites/default/files/doc/files/Smart_Grid_Race_Worth_Winning_Report_on_Economic_Benefits_201209.pdf
[31] Verizon, The Internet of Things 2015, p.6, at http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf
[32] European Parliament Internal Market and Consumer Protection Committee, *MEPs back deal with Council on automatic emergency call system for cars*, 4 December 2014.
[33] FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World*, January 2015, p.1, at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[34] Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.54.
[35] Counting every moment, *The Economist*, 3 March 2012, at http://www.economist.com/node/21548493/
[36] See e.g. the European Commission's Horizon 2020 research programme.
[37] European Commission, *Internet of Things in 2020: Roadmap for the future,* 27 May 2008, p.13.
[38] Davey Alba, Alibaba Reveals a New Kind of QR Code to Fight Counterfeits, *Wired*, 18 May 2015, at http://www.wired.com/2015/05/alibaba-reveals-retro-way-fight-counterfeits-qr-codes/
[39] Roy Want, Bill N. Schilit, and Scott Jenson, Enabling the Internet of Things, *IEEE Computer*, Jan. 2015, p.31.
[40] Alba, note 38.
[41] Want, Schilit, and Jenson, note 39, p.30.
[42] Ovidiu Vermesan and Peter Friess (eds.), *Internet of Things – From Research and Innovation to Market Deployment*, Aalborg: River Publishers, 2014, p.45.
[43] Want, Schilit, and Jenson, note 39, p.32.
[44] EnOcean Alliance, EnOcean Wireless Standard ISO/IEC 14543-3-10: The interoperable wireless standard for home and building automation, at https://www.enocean-alliance.org/en/enocean_standard/
[45] Republic of Korea Ministry of Science, ICT and Future Planning, *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, 8 May 2014, p.6.
[46] Selena Larson, Inside Amsterdam's efforts to become a smart city, *The Kernel*, 4 January 2015, at http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11313/amsterdam-smart-city/
[47] ITU-T Focus Group on Smart Sustainable Cities, Multi-service infrastructure for smart sustainable cities in new-development areas, FG-SSC, May 2015.
[48] Want, Schilit, and Jenson, note 39, p.32.
[49] Mitchell, Villa, Stewart-Weeks and Lange, note 26, p.12.
[50] Tarkoma, note 10.
[51] GMSA, note 9, pp.3-9.
[52] Tarkoma, note 50
[53] OECD, Machine-to-Machine Communications: Connecting Billions of Devices, *OECD Digital Economy Papers*, No. 192, OECD Publishing, 2012, pp.26-27, at http://dx.doi.org/10.1787/5k9gsh2gp043-en
[54] Tarkoma, note 50.
[55] Tarkoma, note 50.
[56] Eric Openshaw, Craig Wigginton, John Hagel, John Seely Brown, Maggie Wooll and Preeta Banarjee, *The Internet of Things Ecosystem: Unlocking the Business Value of Connected Devices*, Deloitte, 2014, p.11, at http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-Iotecosystem.pdf

[57] Openshaw, Wigginton, Hagel, Seely Brown, Wooll and Banarjee, note 56, p.10.
[58] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 95, p.48.
[59] Republic of Korea, note 45, p.4.
[60] Mailyn Fidler, *Ubiquity, Interrupted? A Comparison of European, Chinese, and U.S. Governance of the Internet of Things as an Emerging Technology*, First Annual Conference on Governance of Emerging Technologies, Phoenix, AZ, 2013.
[61] G. Tassey, Standardization in technology-based markets. *Research Policy* 29(4)-29(5), 2000, pp.587-602.
[62] Internet of Things Global Standards Initiative, at http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[63] FCC TAC IoT Working Group, note 79.
[64] T. Wachtel. *10th Meeting of the Internet of Things Expert Group*. Brussels, 14 November 2012.
[65] oneM2M, *oneM2M Security Solutions*, Technical Specification, 1 August 2014, at http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf
[66] Industrial Internet Consortium, *About Us*, at http://www.iiconsortium.org/about-us.htm
[67] AllSeen Alliance, *An Open Source project building the framework for the Internet of Things (IoT)*, May 2015, at https://allseenalliance.org/sites/default/files/resources/intro_to_alliance_5.21.15.pdf
[68] Vermesan and Friess, note 42, pp.151-152.
[69] Want, Schilit, and Jenson, note 39, p.33.
[70] Want, Schilit, and Jenson, note 39, pp.33-34.
[71] http://www.amsterdamopendata.nl/home
[72] http://www.citysdk.eu/about-the-project/
[73] Larson, note 46.
[74] Larson, note 46.
[75] European Commission, *Conclusions of the Internet of Things public consultation*, 28 February 2013.
[76] FTC Staff Report, note 33, pp.vii-viii.
[77] ITU-T Recommendation Y.2060, note 6, s.8.4.
[78] Dan Worth, Microsoft and BT to begin white space spectrum trials, *V3*, 2 October 2013, at http://www.v3.co.uk/v3-uk/news/2298124/microsoft-and-bt-to-begin-white-space-spectrum-trials
[79] US Federal Communications Commission Technological Advisory Council Internet of Things Working Group, Spectrum: Initial Findings, *FCC TAC meeting update*, 10 June 2014, at http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting61014/TACmeetingslides6-10-14.pdf
[80] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 95, p.24.
[81] Republic of Korea Ministries of Science, ICT and Future Planning, note 59, p.11.
[82] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 95, p.24.
[83] Paul Barbagallo, As 'Internet of Things' Evolves, FCC's Spectrum Strategy Will Be Put to the Test, Bloomberg BNA, 19 November 2014, at http://www.bna.com/internet-things-evolves-n17179912070/
[84] http://www.sigfox.com/en/#!/technology
[85] Republic of Korea Ministries of Science, ICT and Future Planning, note 59, p.4.
[86] OECD, note 53, p.20.
[87] The endangered SIM card, *The Economist*, 20 November 2014, at http://www.economist.com/news/business/21633870-moves-reinvent-or-even-abolish-sim-card-could-have-big-consequences-endangered-sim?frsc=dg%7Ca&fsrc=scn/tw_app_ipad
[88] GSMA, *How China is set for global M2M Leadership*, June 2014, at http://www.gsma.com/newsroom/wp-content/uploads/2014/06/china-report.pdf
[89] OECD, note 53, pp.30-31.
[90] Bundesnetzagentur, *Marktbefragung zu einem zukünftigen Nummernplan für Internationale Kennungen für Mobile Teilnehmer (International Mobile Subscriber Identity, IMSI)*, Mitteilung Nr. 819/2014, Amtsblatt Nr. 15/2014, at http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehm

en_Institutionen/Nummerierung/Technische%20Nummern/IMSI/Mitteilung819_2014.pdf?__blob=publicationFile&v=2

[91] The Economist, note 87.

[92] Belgisch Instituut Voor Postdiensten En Telecommunicatie, *Raadpleging Op Vraag Van De Raad Van Het Bipt Van 25 November 2014 Met Betrekking Tot De Herziening Van Het Beleid Inzake Het Beheer Van Het Nummerplan*, at http://www.bipt.be/public/files/nl/21394/Consult_review_KB_Nummering_NL.pdf

[93] CEPT ECC, Evolution in the Use of E.212 Mobile Network Codes, ECC Report 212, 9 April 2014, at http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP212.PDF

[94] Want, Schilit, and Jenson, note 39, p.30.

[95] Helen Rebecca Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Jean Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge and Hans Graux, *Europe's policy options for a dynamic and trustworthy development of the Internet of Things*, RAND Corporation, 2013, pp.50-52, at http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf

[96] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 95, p.23.

[97] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 95, pp.23-25.

[98] Article 29 Working Party, note 117, p.19.

[99] Republic of Korea Ministries of Science, ICT and Future Planning, note 59, p.11.

[100] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 95, p.86.

[101] European Commission, note 75.

[102] Center for Democracy and Technology, *Comments to the Federal Trade Commission after November 2013 Workshop on the "Internet of Things"*, 10 January 2014, p.3, at https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf

[103] FTC Staff Report, note 33, p.12.

[104] Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, Symantec Official blog, 23 January 2014, at http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam#!

[105] Kevin C. Tofel, Got an IP webcam? Here are 73,000 reasons to change from the default password, *GigaOm Research*, 7 November 2014, at https://gigaom.com/2014/11/07/got-an-ip-webcam-here-are-73000-reasons-to-change-from-the-default-password/

[106] FTC Staff Report, note 33, p.13.

[107] Ashkan Soltani, What's the security shelf-life of IoT? *Tech@FTC blog*, 10 February 2015, at https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot

[108] Cesar Cerrudo, *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks*, IOActive Labs White Paper, 2015, at http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf

[109] See for example the US Federal Trade Commission's orders Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014); Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent); and HTC America, Inc., No. C-4406 (July 2, 2013) (consent), discussed in FTC staff report, note 115.

[110] Article 29 Working Party, note 120, p.18.

[111] 36th International Conference of Data Protection and Privacy Commissioners, *Mauritius Declaration on the Internet of Things*, 14 October 2014, p.2, at http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf

[112] 36th International Conference of Data Protection and Privacy Commissioners, note 111, p.2.

[113] See B.J. Koops and R. Levene, Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law, *International Review of Law, Computers & Technology* 28 (2), 2014, pp.159-171; ENISA, *Privacy and Data Protection by Design*, December 2014.

[114] C. Cuijpers & B.J. Koops, Smart metering and privacy in Europe: Lessons from the Dutch case. In S. Gutwirth et al. (Eds.), *European data protection: Coming of age*, Springer, 2012, pp.269- 293.

[115] FTC Staff Report, note 33, p.28.

[116] Graham Greenleaf, Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories, *Journal of Law, Information & Science* (2014) 23(1).

[117] Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 16 September 2014.
[118] Article 29 Working Party. *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.* 11 February 2011.
[119] Article 29 Working Party, note 120, p.6.
[120] Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 16 September 2014, p.8.
[121] FTC Staff Report, note 33, p.17.
[122] Scott R. Peppet, Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent, 93 *Texas L. Rev.* 85 (2014), pp.115-16.
[123] Peppet, note 122, p.93.
[124] Article 29 Working Party, note 117, p.8.
[125] Article 29 Working Party, note 120, p.17.
[126] Article 29 Working Party, note 120, p.20.
[127] FTC Staff Report, note 33, pp.39—42.
[128] Article 29 Working Party, note 120, p.16.
[129] Jack H. Park, Government to Ease Up on Regulations on Financial Technology, Internet of Things, *BusinessKorea*, 12 December 2014, at http://www.businesskorea.co.kr/article/7814/internet-deregulations-government-ease-regulations-financial-technology-internet-things