

Chapter 6

Emerging issues: The Internet of Things

This chapter explores convergence between ICTs and the economy on a grand scale, otherwise known as the Internet of Things (IoT). The term implies the connection of most devices and objects over time to a network of networks. It encompasses developments in machine-to-machine communication, the cloud, big data and sensors, actuators and people. This convergence will lead to machine learning, remote control and eventually autonomous machines and systems. Estimates indicate that potentially 50 billion devices could be connected by 2020, but challenges remain in gathering concrete and accurate data on the widespread use of IoT technology, now and in the future. Adoption will depend to a large extent on the capacity of governments to create an adequate regulatory framework in key areas including telecommunication, privacy and consumer policy.

Policy makers and regulators have taken a keen interest in convergence between fixed and mobile networks, and between telecommunications and broadcasting. They now recognize that the Internet of Things (IoT) represents the next step in convergence between ICTs and the economy on an unprecedented scale. The term IoT implies the connection of most devices and objects over time to the Internet's network of networks. Other terms used to describe this process include the "Internet of Everything", the "Industrial Internet" and "Machine-to-Machine (M2M) communication". The term "Internet of Everything" is increasingly accepted as the most accurate because Internet-connected sensors and actuators¹ will not only link to things, but will also monitor the health, location and activities of people and animals, the state of the natural environment, the quality of food and much else besides.

The Internet of Things has profound implications for all aspects and sectors of the economy, including industrial and commercial processes, consumer and home services, energy, transport systems, health care, infotainment and public services. Embedding devices with limited processor, memory and power resources opens up applications everywhere. For example, data could be gathered in buildings, factories and natural ecosystems with applications in urban planning, manufacturing and environmental monitoring. The end result will be combined with the cloud, big data and machine learning to produce autonomous machines and intelligent systems. This section of the *Digital Economy Outlook* investigates how increasing adoption of the IoT will be facilitated or hampered by differing policy and regulatory approaches. In the area of communication, issues range from management of spectrum and numbering through to practices around SIM cards. Broader issues include privacy, security, and consumer protection and empowerment.

6.1 The Internet of Things: Developments, definition and main elements

Visions of smart, communicating objects are not new and existed well before the Internet became a reality 45 years ago.² By the early 1990s, ideas about pervasive computing and embodied virtuality were well advanced. For example, at Xerox PARC they imagined that "specialised elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence" (see Weiser, 1991). In spite of this, manufacturers of smart consumer products remain uncertain as to which features will most attract consumers and whether demand exists for some devices to be connected at all (Harwell, 2014).

Predictions regarding the significance of the IoT have also met with scepticism, based in part on the rate of take up of Radio Frequency Identification (RFID), which is slower than anticipated a decade ago. The limited use of RFID is largely the result of a lack of standards, a lack of security and the relatively high cost of both RFID readers and tags.³ However, the widespread availability of smartphones with near field communication (NFC) capabilities, which allow communication when the device is in close proximity, may help to overcome this hurdle. The passive RFID tag market is now experiencing significant growth, albeit

a decade later than expected, with the majority of growth based on retailer adoption of RFID for shelf-level stock replenishment (Das and Harrop, 2014). Widespread availability of smartphones implies benefits not only for supply chain management, but also for interactions between retailers and customers in stores, for example. The capabilities of smartphones, from NFC to low-energy Bluetooth, and their pervasive adoption within a very short timeframe, mean that devices to read and interact with the IoT are now available at scale for the first time.

Smartphones have brought the IoT to the consumer and function increasingly as a hub linking other devices to the wider network (Yared, 2013), including a number of consumer electrical appliances (Box 6.1). Firms such as Philips and General Electric produce light bulbs that can be controlled over the Internet, while television, radio, sound speakers and telephones can all be purchased with built-in Internet connectivity. Domestic appliances such as ovens, washing machines and refrigerators increasingly come with built-in Internet connectivity, and in 2013-14 major brands such as General Electric, Philips, Samsung and Whirlpool introduced Internet-connected home appliances to the market in wider ranges and larger quantities, first in North America, and then in Europe and Asia. An increasing amount of sporting goods, ranging from equipment for golf to basketball, can also be linked

Box 6.1. The smartphone as the hub to the Internet of Things

Smartphones play a prominent role in consumer use of the IoT. Internet-connected smart watches, fitness bracelets, running shoes and heart rate monitors are just some of the products consumers can buy and link to the Internet via their smartphone, enabling them to interact with other users or monitor their own fitness levels. Nearly all IoT-connected products come with an interactive smartphone app.

The development of smartphones and tablets has created an entirely new environment for user interfaces. Historically, user interfaces for all kinds of devices and appliances were limited to LED lights and knobs, which limited how devices could be programmed. Not adding too many functions and keeping the interface simple were among the main requirements. The difficulty experienced by many people in programming their video-cassette recorder is a prime example of the challenges involved in developing such interfaces. The smartphone screen interface now allows formerly difficult choices to be made with relative ease. Search and help functions can further support users in ways that were previously impossible. Smartphones not only make possible more flexible user interfaces, they also allow users to customise them.

The development of smartphones has had tremendous implications for the cost of components needed to make IoT devices. The scale of smartphone production is measured in billions of units, which means that sensors such as GPS, magnetometers, barometer gyroscopes and cameras also have to be produced in these quantities. As a result, sensors have become smaller and cheaper, which has promoted their use in other products such as toys, remote-controlled helicopters, home weather stations and many other devices. The same trend is visible in screens and communication chips, where smaller screens of low quality have been replaced by higher quality versions, leading to widespread installation in point-of-sale terminals and other devices. The virtual reality glasses “Oculus Rift”, for example, are built using the highest quality smartphone screens available. High-quality screens are also now being fitted into smart watches, thermostats, vehicles and energy consumption appliances.

to the Internet. The International Tennis Federation has already certified an Internet-connected tennis racquet readily available on the market for competition play (Kelly, 2014). The racquet allows tennis players to analyse their game and work on elements such as perfecting their swing.

The above examples monitor people for recreational purposes, however, the first line of certified health-related monitors are now becoming available on the market. In addition, the IoT is increasingly attracting developers. An increasing number of crowdfunded projects on the Kickstarter website have an IoT component, such as Internet-connected locks, sensor tags and lightbulbs (Table 6.1). The entrepreneurs behind these projects ask the general public to fund development by pre-financing their development and production. Funders do not get equity in the company, but do generally buy the finished product or receive promotional material, depending on the level of funding they provide. Kickstarter, as one of the leading platforms for crowdfunding, can provide an interesting indicator of areas being targeted by innovators.

Table 6.1. **A selection of IoT-related projects from Kickstarter**

| Name | Description | More information | Funding pledged (USD) |
|--|---|--|-----------------------|
| EasyTouch: Turn your world into a touch sensor | EasyTouch is the world's easiest to use capacitive touch sensor. Turn bananas, pencil drawings, water or fabric into a touch button. | www.kickstarter.com/projects/54060271/easytouch-turn-your-world-into-a-touch-sensor?ref=category | 13 023 |
| Ambi Climate: The smart add-on for your air Conditioner | Ambi Climate learns about your habits and home environment. Auto adjusts AC for ideal temperature and energy savings. Remote access via Android/iPhone. | www.kickstarter.com/projects/ambi-labs/ambi-climate-the-smart-add-on-for-your-air-conditi | 94 865 |
| Digitsole: The first interactive insole to heat your feet | Digitsole is the first connected insole on the market controlled via your smartphone – warm your feet, track your distance and calories. | www.kickstarter.com/projects/1308642275/digitsole-the-first-interactive-insole-to-heat-you?play=video_pitch&ref=home_featured | 90 074 |
| Prizm: Turn your speakers into a learning music player | Prizm is a learning device that instantly plays the perfect music on your speakers, based on people in the room and the context. | www.kickstarter.com/projects/prizm/prizm-turn-your-speakers-into-a-learning-music-pla?ref=category | 105 594 |
| Notti: A more beautiful smart light | This beautifully designed app-controlled light provides highly customised visual notifications and other useful info from your phone. | www.kickstarter.com/projects/26398080/notti-a-more-beautiful-smart-light?ref=category | 44 727 |
| PLAYBULB color: Smart Color Light and Wireless Speaker 2-in-1 | PLAYBULB color is a smart colour LED speaker light bulb with the PLAYBULB X free App. Let colour and music fill up your living space. | www.kickstarter.com/projects/mipowusa/playbulb-color-smart-color-light-and-wireless-spea?ref=category | 37 446 |

Source: Kickstarter, 3 November 2014. www.kickstarter.com

Defining the Internet of Things

A definition of the IoT is not a simple matter. A previous OECD report on M2M communication found that the term was associated mainly with applications involving RFID (OECD, 2012a). RFID makes use of so-called tags – tiny chips with antennae that transmit data when they come into contact with an electromagnetic field. These are known as passive communication devices, in contrast to active devices that transmit when they have access to a power source, such as a battery. The term “M2M” was used for:

Devices that are actively communicating using wired and wireless networks, that are not computers in the traditional sense and are using the Internet in some form or another. M2M communication is only one element of smart meters, cities and lighting. It is when it is combined with the logic of cloud services, remote operation and interaction that these types of applications become “smart”. RFID can be another element of a smarter environment that can be used in conjunction with M2M communication and cloud services (OECD, 2012a).

Since 2011, however, the term “M2M” has lost some of its significance and the term “IoT” has gained prominence for a wide variety of developments where “things” are connected to the Internet. The IoT consists of several elements, such as the cloud, big data, machine-to-machine communication, sensors and actuators, covered later in the chapter. As noted earlier, a more accurate term would be the “Internet of Everything”; however, this term has yet to find common currency and may not be widely used in the future.

The IoT in its purest definition would be limited to objects able to communicate via the Internet. This definition, however, has a number of drawbacks: it is limited to things, does not consider effects and does not consider emerging properties. To start with, by definition, everything that is directly connected to the Internet has to be a thing. People cannot communicate via the Internet except through the mediation of a thing. As such the Internet of *things* would be a misnomer, because all Internet connections occur between things. Many definitions, however, explicitly exclude person-operated/controlled devices, such as smartphones, tablets and other computers. For example, a washing machine that communicates with a smartphone app is not considered to be part of the IoT because it is operated by a person. This can have practical implications. In Brazil, for example, M2M communication between devices is excluded from certain taxes if the communication occurs without human intervention for the purpose of monitoring, measuring and controlling the device.⁴ Given that smartphones and tablets function as the main operating devices for much of the IoT, this definition could prove too narrow. For example, health-monitoring devices such as sports heart rate meters and step counters could fall outside the definition, because they may require a smartphone as a platform in order to function.⁵

Defining the IoT becomes even more challenging when taking into account impact. For example, sensors can be used to ascertain whether a car is parked on a parking spot, but modern vehicles with on-board parking cameras and sensors can also determine the location and size of an empty parking spot just by driving by. This information allows the creation of a real-time overview of city parking spaces, without the need for road-embedded sensors. For users, the parking spots appear to be linked to the Internet. But can a parking spot can be defined as a thing?

When multiple sensors are integrated into systems such as a vehicle, it may prove difficult to state accurately the exact number of things connected to the Internet. Some calculations consider sensors and actuators as individual things, however a vehicle may contain between 30 to 200 different sensors. Should the vehicle be seen as the thing or individual sensors? Furthermore, emergent properties develop from combining different sensors and actuators. In other words, sensors may be repurposed or extended in functionality over time. A smart thermostat may have a motion sensor, which can be repurposed/extended to also act as a light switch or as an element in a burglar alarm. A homeowner may not have bought a burglar alarm, but the combination of sensors, actuators and software in the home could result in the creation of an alarm system.

The other element of the definition – when something is part of the Internet – is equally difficult. According to some definitions, an Internet-connected thing must be capable of operating in an IP communications stack. This would exclude devices such as RFID tags, Bluetooth-enabled devices and connected light bulbs, which can only connect to the Internet through a gateway that acts as a mediator between the device and the Internet. For this report, such devices are considered part of the IoT. Therefore, if a light bulb does

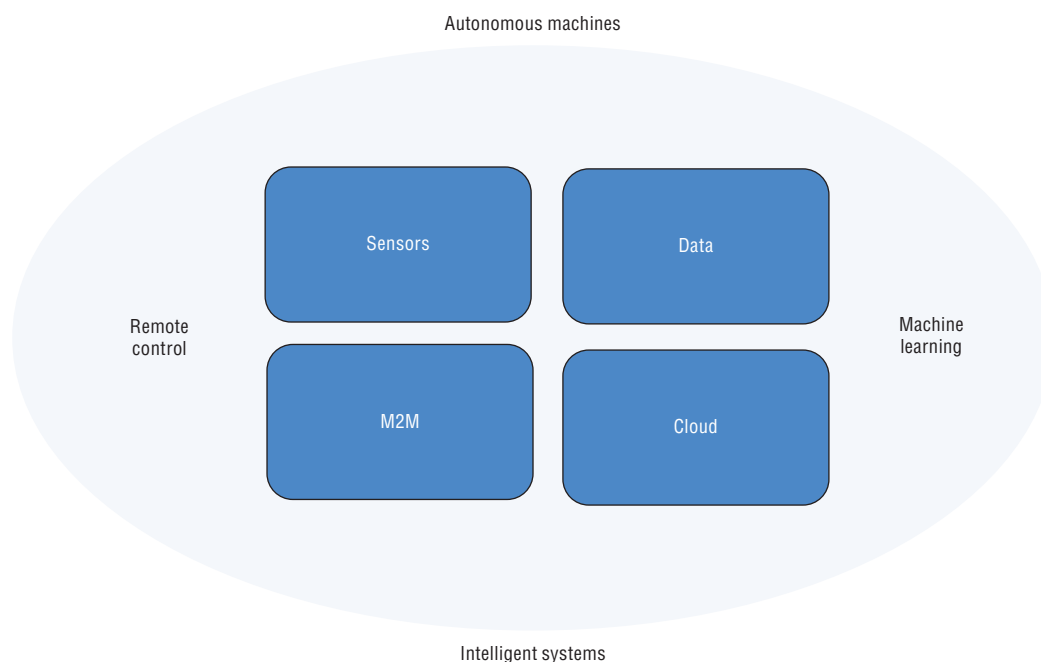
not support the IP protocol but can be addressed via an Internet-connected gateway, it is considered to be Internet connected. The same is true for RFID tags, fitness monitoring bracelets or connected shoes.

This chapter therefore defines the IoT in broad terms including all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, often considered to be part of the “traditional Internet”. However, these devices are integral to operating, reading and analysing the state of IoT devices and frequently constitute the “heart and brains” of the system. As such, it would not be correct to exclude them.

The main enablers of the Internet of Things

The evolution of the IoT is underpinned by four main trends in ICT development – big data, the cloud, M2M communication and sensors (Figure 6.1). The combination of cloud computing and big data analytics leads to improved machine learning applications, operating at a new level of artificial intelligence. This combination also leads to further developments in machine learning and remote control. The latter still requires human interaction, but the machine takes care of all main operational functions with human interaction limited to specific actions. Remote-controlled machines and systems combined with machine learning will ultimately lead to autonomous machines and intelligent systems, in particular robotic machines.

Figure 6.1. **Main enablers of the Internet of Things**



A previous OECD report analysed the contribution of sensors and actuators to “Green Growth” (OECD, 2010: 227-256). It stated that sensors can measure multiple physical properties and may include electronic sensors, biosensors and chemical sensors. These sensors can be regarded as “the interface between the physical world and the world of electrical devices, such as computers” (Wilson, 2008). Conversely, actuators function by

converting an electrical signal into a physical phenomenon. Examples include displays for speedometers and thermostats (the data for which is measured by sensors), as well as those that control the motion of machines.

Early sensor and actuator systems such as vehicle engines measured, processed, acted upon and discarded data. Today, generated data are increasingly communicated to other machines and central computers and stored for further correlation and analysis. The data may be communicated via a variety of means – wired and wireless, short or long range, low or high power, low or high bandwidth. Two OECD reports, *Machine-to-Machine communications: connecting billions of devices* (2012a) and *The building blocks for smart networks* (2013a), discuss many of these options.

Communication between sensors controlled by central processing units has allowed machines to become more aware of their surroundings and has stimulated the development of new actuators that execute an increasing range of functions. As a result, remote operation has become possible in ways that were previously unfeasible, where the machine undertakes the majority of tasks and human interaction is limited. In mining, for example, one remote operator can now manage multiple ore transporters.

Big data, data analytics and cloud computing

Collecting, compiling, linking and analysing very large data flows in real time requires powerful, new analytical techniques and data-sharing models to handle the size and complexity of the necessary data-processing operations. The availability of new techniques and the associated shift in organisation of these operations signal a change towards a data-driven or data-centric socio-economic model commonly discussed under the umbrella term “big data” (Box 6.2). In such a data-driven world, data are a core asset which constitute a vital resource for innovation, new industries and applications, and competitive advantage. The rapid decline in the cost of analytics, including computing power and data storage, as well as the continued expansion of broadband has brought such data increasingly within reach. Storage costs, for example, have decreased to the point where data can generally be kept for long periods of time, if not indefinitely.

Big data is particularly well suited to solutions that favour massively parallel processing (MPP). The data are sliced into smaller units and processed, and the various results are later combined. This is different from traditional computing, where faster processors and memory deliver the required speed increases. Systems that support MPP are essentially large numbers of servers, linked by a common network and a software stack that treats the servers as a common pool for processing and storage. Cloud computing is defined “as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort” (OECD, 2013b).

Sensors, M2M communication and cloud computing generate a vast amount of data, the statistical analysis of which is of enormous value to science, business and consumers. However, big data, M2M and cloud computing also underpin a whole new era of machine learning, otherwise known as artificial intelligence. Previously considered a failed dream of the early age of computing, artificial intelligence has made a comeback through the inclusion of Bayesian statistical analysis. This uses probability distributions based on prior experiences, instead of a priori models, with new tools, better described by the term “machine learning”.⁶

Box 6.2. The difficulty of defining “big data” beyond volume, velocity and variety

A clear definition of “big data” remains elusive. Initially, the term referred to data sets for which volume became an issue in terms of data management and processing. However, the emphasis on volume alone can be misleading, whether measured in gigabytes, petabytes (millions of gigabytes) or exabytes (billions of gigabytes). In some cases, volume is less relevant than the number of readings, the way the data are used and the resulting complexity. For example, managing a day’s worth of data from thousands of sensors in almost real time poses a greater challenge than managing a video collection of equivalent size in bytes. This distinction is captured by the “3Vs” definition of big data, which highlights three main characteristics:

- The **volume** of data as covered by most definitions today (see Loukides, 2010; MGI, 2011; and also McGuire et al., 2012, cited in OECD, 2013c);
- The **variety** of data, which refers to mostly unstructured data sets from sources as diverse as web logs, social media, mobile communications, sensors and financial transactions. Variety also goes hand in hand with the capability to link these diverse data sets;
- The **velocity** or speed at which data are generated, accessed, processed and analysed. Real-time monitoring and real-time “nowcasting” are often listed as benefits that accompany the velocity of “big data”.

However, the 3Vs and other similar definitions describe technical properties that depend on the evolving state of the art in data storage and processing, and as such are in continuous flux. Furthermore, these definitions imply that the sole element in big data is data. While this is true for volume, both variety and velocity are based primarily on data analytics – the capacity to process and analyse unstructured diverse data in (close to) real-time. Furthermore, the term “big data” does not indicate how the data are used, the types of innovation they can precipitate, or how they relate to other concepts such as “open data”, “linked data”, “data mashups” and so on. For these reasons, the OECD KBC2: DATA project has chosen to focus not on the concept “big data”, but rather on “data-driven innovation”, which is based on the *use of data and analytics to innovate for growth and well-being*.

Source: OECD, 2013c.

The combination of machine learning and remote-controlled machines, such as vehicles, can result in autonomous machines and intelligent systems, able to operate without a human controller. Instead, the machines are controlled either internally or remotely through a computer located elsewhere. The machines and the intelligent system they form part of use a combination of big data analysis, cloud computing, M2M communication, and sensors and actuators, to operate and learn.

Traditionally, robots are used mostly in industries where their speed, precision, dexterity and ability to work in hazardous conditions are valued. However, these capabilities required very precisely defined environments and setting up a robotic plant can take months, if not years, to plan all robotic movements down to the millimetre. This situation is now evolving due to the combination of sensors, machine learning and cloud computing. The IoT allows robots to become more flexible and enables them to learn. Current examples of such developments include fully robotic warehouses that only require people to oversee the robots and load and unload trucks.

The move towards intelligent systems that are not limited to controlled environments, such as factories, but interact with non-technological environments, is still some way off, but is already visible in the area of transport. Many industry experts believe that practical application of these systems will follow quickly, once the technical obstacles are overcome. It remains unclear whether autonomous vehicles will eventually be a common sight on the roads, but industry estimates place implementation at about a decade away. The main benefits foreseen for autonomous vehicles are hard to evaluate at the current time, but a number of advantages present themselves:

- **Utilisation.** Most vehicles are not presently used for the majority of their lifetime. Autonomous vehicles might increase the utilisation of vehicles, for example, through subscription models.
- **Energy efficiency.** Significant energy is used and lost during acceleration and deceleration. Machines would be able to better balance acceleration and deceleration. In addition, autonomous vehicles would be lighter, according to some predictions, due to lower requirements for on-board safety components.
- **Safety.** With millisecond reaction times and communication between vehicles, autonomous vehicles might deal better with sudden changes in situations with greater awareness of dangerous situations ahead.
- **Empowerment.** Industry and academics believe that autonomous vehicles will cost less to own and operate and require less or no skill from the occupant (Lee, 2015).⁷ This could provide an alternative to public transport for a larger group of people (e.g. elderly people or those with physical disabilities).

Much of the IoT concentrates in cities and many IoT applications will be useful for urban life, governance, planning, and the management of urban infrastructures and services. For example, intelligent transport systems or smart homes and electricity grids will enable those living in or around cities to save time, energy and money. City governments will have access to increasing amounts of data to plan and invest more wisely and to manage transport, energy, waste and water systems more efficiently. Cities will also foster and benefit from interaction between connected things, machines and systems in areas that have hitherto functioned largely in isolation. For example, synergies could be achieved by connecting water, energy, transport and waste systems with a view to promoting resource reuse and eliminating excess capacity and redundancies in each system. However, interoperability across devices, machines and systems will be essential to optimise the potential of the IoT to transform cities, and technologies, standards, protocols and rules will need to be harmonised across sectors.

6.2 Technical developments in the Internet of Things

The Internet of Things relies upon connectivity with devices and sensors. The different types of connectivity can be described based on the geographic dispersion and geographic mobility they support (Figure 6.2). The higher the geographic dispersion and mobility the application demands, the greater the energy use needed to sustain the application, and the larger the antenna required (if the device is wireless). Energy use and antenna size in turn define the *form factor* (i.e. the size, configuration or physical arrangement of a computer hardware object) and device applications. The smallest sensors and actuators are those that either harvest electromagnetic energy through their wireless circuitry, such as RFID tags, or are connected with a wire to a power source and communications network. Developments

in battery technology unfortunately are linear compared to the exponential advancements in integrated circuits, where increasingly smaller sizes and advances in capabilities are traded off against greater energy use.

Figure 6.2. **Machine-to-machine applications and technologies by dispersion and mobility**

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

Short range and home networks

Both wired and wireless networks are essential for the IoT. Wired networks provide capacity, but are inflexible in their location. Wireless networks allow for flexibility in location and motion, but are often limited by bandwidth and energy. Wired networks use standard networking technologies such as Ethernet (for in-company and fibre networks), GPON (for fibre networks), DSL (for public telephony networks) and Docsis (for cable networks). Although some standards exist for Power-line communication, and Power over Ethernet is commonly used in businesses for VoIP phones and other equipment, there has been little development in wired protocols for the IoT. Existing standards are often applicable for situations where a wired connection can be used.⁸

The least mature and, therefore, the most rapidly changing area is short-range wireless standards in the home and factory (lower left corner of Figure 6.2). Technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Zigbee, 6LowPan, Bluetooth and Wi-Fi, in order of complexity, have all been advanced as global standards, and each has its own niche. RFID technology is a one-way communication protocol that allows small chips (tags) to broadcast their location. In 2003, when Walmart announced that it would require its top suppliers to use RFID for all pallets and cases, it appeared that RFID was set for a big future in retailing. Many analysts predicted that every milk carton would soon carry an RFID tag and a refrigerator would be able to scan and provide an inventory of its contents. Some analysts predicted that within a decade 100 billion tags would be used each year. This has not become a reality, in part because the price of tags has not decreased sufficiently, but also because radio frequencies do not easily penetrate packaging made from tin foil or products that consist (partially) of liquids. Therefore, RFIDs have found only limited use in high-volume, low-margin and fast-moving consumables.

By 2014, the RFID market had matured with RFID tags used increasingly in clothing and apparel stores. The benefit of RFID here lies in the ability to scan a stack of clothing and know whether particular sizes are still available or need to be replenished from storage. This reduces the time spent by customers waiting for employees to locate particular sizes in a stack. In addition, RFID is used in aerospace and manufacturing to track the location of

parts and tools, and to ascertain whether the correct part has been used and its exact age. In health care, RFID is used to track goods, medicine and patients, as well as hand-washing hygiene by staff. The use of RFID-controlled soap dispensers has increased the use of soap in hospitals and decreased the amount of infections. In transport, single-use or multi-day tickets are embedded with RFID tags. RFIDs are also used in livestock identification to comply with government requirements regarding the traceability of animals throughout their lives. One analyst company estimates that 5.8 billion tags were sold in 2013 and predicted a rise to 6.9 billion in 2014 (Das and Harrop, 2014).

NFC is a two-way technology developed for interaction, for example, when making payments or entering a facility. Operation requires two NFC-equipped devices to be in very close proximity to each other. NFC is integrated into swipe cards for building access and public transport (e.g. the Parisian *Navigo*, London's *Oyster* card and Japan's *Suica* card). Its use is currently being expanded to contactless payments, with more and more banks introducing credit and debit cards with NFC. With the introduction of Apple's iPhone 6, all major smartphone platforms now support NFC. At the same time, some public transport cards, such as Seoul's *T-card* and Japan's *Suica* card, can be used for payments of groceries, snacks, taxis and other purchases.

The main challenges of NFC concern standardisation. Most systems that use NFC are so-called closed-loop systems. This means that only cards issued by the organisation can be used for the types of transactions it authorises. This limits usage. For example, a public transport authority will only accept transport cards it has issued, but not cards from neighbouring regions or bank cards (the Parisian *Navigo* system cannot be used outside central France). An open-loop system allows customers to use cards issued by other organisations, such as other public transport authorities, banks and mobile phone vendors. The main obstacle to standardisation is willingness among organisations to open access to what they see as their customers. It is difficult to introduce a system that works only when a customer uses bank Q, public transport organisation X and smartphone brand Y provided by mobile operator Z. Such an overlap covers only a small demographic. Many early NFC trials failed because they were limited to one bank and one mobile operator.

Interest in open-loop systems is now increasing. Starting from September 2014, Transport for London began supporting payments through smartphones via "Cash on Tap" from EE and Vodafone Smartpass. The use of a prepaid debit or credit card means that only the co-operation of the bank/credit card company is needed.⁹ The Transport for London system has proven popular with 5% of trips being paid through the open-loop card system within the first week of launch. One problem with open-loop systems, however, is the potential for "card clash", which can occur when multiple cards may be used to perform actions such as transport payments. If a user's wallet touches a gate, the system may deduct payment from each card it detects.

Smartphones have also brought NFC technology to other applications. For example, pairing a smartphone with a wireless speaker can be achieved by tapping the phone on the speaker. This functionality is integrated into many Android phones and most Bluetooth wireless speakers and headphones, and is now expanding to keyboards, printers, televisions and other devices. It allows the user to pair devices without needing to know or understand the underlying wireless technologies (Wi-Fi/Bluetooth), and to establish authentication without knowing the keys for the devices. NFC stickers allow users to enable their phones to change configuration automatically when the sticker is tapped, for example, when the phone is docked in a vehicle.

Bluetooth was initially designed as a wireless personal area network (WPA) to connect peripheral devices, such as headsets and keyboards, at short range to mobile phones and computers. Over 90% of phones, tablets and laptops have Bluetooth capabilities, and some vehicles. Compared to NFC it is a higher bandwidth longer range technology, working up to 10-20 metres in a star topology with a central controller, where all devices connect to each other.¹⁰ The latest version is Bluetooth 4.0; however ongoing development for Bluetooth 4.1 is expected to introduce mesh-networking and IPv6. This would allow devices to connect directly to each other and via IPv6 to the Internet, instead of via a central controller. This would make Bluetooth a direct competitor to IEEE 802.15.4-based networks (discussed below).

Bluetooth 4.0 has expanded its IoT capabilities through support for low-energy profiles. This has sparked innovation around a number of low-energy sensors and tags, such as Apple's iBeacon and competing standards. A number of uses have been identified in the home, including sensors that combine temperature, movement, position and other capabilities. These can be used to locate objects such as car keys, but also to signal whether a (liquor or gun) cupboard or window has been opened. Bluetooth has also found uses outside the home, for example, in shops and malls. In the airports of Amsterdam and Miami, Bluetooth beacons guide smartphone owners to the correct gate via a dedicated app. SITA (an organisation specializing in IT and communications solutions for airports) maintains an open index which allows airports to register their beacons and app-makers to interact and develop services.¹¹ In a few years it may be commonplace for airlines to use beacons to locate passengers and for travellers to find their plane using tags. Beacons with relevant information can be placed at any location, such as a bus stop, and accessed via a smartphone. On a similar note, Microsoft has designed a headset that conveys information vocally for use by the visually impaired among other users.

IEEE 802.15.4 (Low Rate Wireless Personal Area Network) is a networking standard that distinguishes itself by supporting both star topology and mesh topology networking for low power applications. It is designed to use very little power enabling it to work for years in battery-operated situations, even when a device is in sleep mode. It is limited to 250 Kbit/s, which makes it ideal for IoT applications in the home and industrial settings. IEEE 802.15.4 specifies how devices broadcast and connect, but not some of their higher-level interactions which are necessary to allow devices to interact in a meaningful way.¹² A number of other standards both open and proprietary are built on top of IEEE 802.15.4, including WirelessHart, MiWi, ISA100.11A, Zigbee and Thread, each of which addresses different usage cases. IEEE 802.15.4, however, does not work well with a standard IP stack, which has prompted the Internet Engineering Task Force (IETF) to develop the 6LoWPan standard to enable native IPv6.¹³ The difficulty lies in the packet size, which for IEEE 802.15.4 is too small to hold a standard IP packet, and the energy consumption associated with the Internet's always-on assumption. Unlike Bluetooth, however, 802.15.4 is rarely supported on mobile phones, tablets and laptops, and therefore needs a dedicated gateway to function.

Zigbee is the most well-known standard to make use of IEEE 802.15.4. However, a number of incompatible implementations of Zigbee exist on the market, which has slowed adoption. Zigbee can be found in light bulbs by GE and Philips and Comcast's new set-top box. Most variants of Zigbee do not support IP-based networking natively, although some do. One reason for lack of native support for IP is the power requirements. For example, Zigbee Green Power allows the use of Zigbee networking in devices that have no permanent power source, such as a battery or other electrical connection. Instead, these devices can harvest energy from motion, such as by pressing a light switch.

In 2014, Google Nest, Samsung, ARM and a number of other companies announced “Thread”, a standard for in and around the home, launched as an alternative to Zigbee. Thread makes use of 802.15.4 and comes with native 6LowPan support. While incompatible with Zigbee, it is designed in such a way that the same chips and radios can be used. Whether it will be successful remains to be seen.

A number of alternative proprietary technologies to IEEE 802.15.4-based technologies exist, such as ANT, Peanut and Z-Wave. Of these, Z-Wave is the most widely implemented. GE, for example, offers a wide range of Z-Wave-based products. As proprietary technologies, they are controlled by a company or group of companies, unlike open standards which allow everyone to make use of the standard (under certain conditions). A limited number of vendors provide the chips and radios, although more vendors may be building packages around the technology.

Wi-Fi (IEEE 802.11x) is the final networking protocol in this quadrant that deserves attention. It forms the basis for a great many IoT devices in and around a home, with almost every ISP supplying its customers with a modem/switch with Wi-Fi on board. Despite using unlicensed spectrum, Wi-Fi has become the preferred way for many consumers to connect to the Internet. It was optimised for use by computers in local area networks and as a result can attain speeds of up to 1 Gbit/s, instead of prioritising energy efficiency, as does IEEE 802.15.4.¹⁴ This makes Wi-Fi the technology of choice for higher bandwidth and low latency applications, such as voice and video applications. As a result, Wi-Fi requires more energy and does not support battery-operated technologies well. Wi-Fi is therefore used to connect all kinds of devices that are (regularly) connected to the mains supply.

Short-range networking technologies are the most contentious area for networking the IoT, as the conflicting requirements of technologies make it hard to predict a winner. Where a technology needs to work for years on a single charge, IEEE 802.15.4 or Bluetooth-based technologies win out. Where high speeds are needed, Wi-Fi is a likely choice. However, no matter what technology is chosen, a trade-off needs to be made. A possible solution is for some manufacturers to put multiple networking technologies in some of their chipsets aimed at IoT solutions. This might increase the costs of the chipsets, but also increase the flexibility with which they can be deployed, and potentially avoid lock-in.

Long-range and mobile networks

For geographically dispersed networks wired options are only viable in locations where wired connectivity is already present, or for certain organisations such as those managing roads and railroads as part of an overall infrastructure. For others, the costs associated with the civil works necessary often make wiring remote locations too expensive. For this reason the use of mobile wireless networks is essential to the IoT for geographically dispersed IoT applications. Whether used to control traffic lights or remotely monitoring pumps or vehicles, the only cost-effective way to connect them is through wireless networks.

2G/3G/4G networks, as developed by the 3GPP2, are the primary networks for the deployment of the IoT:

- 2G (GSM) networks offer worldwide coverage, both indoors and outdoors, and as such are considered future proof. Some mobile operators plan to retire their 2G networks (e.g. AT&T in 2017), but their coverage is often superior to that of 3G and 4G networks and the installed GSM base is so large, particularly in Europe, that retirement will prove challenging.

- 3G (UMTS/HSDPA) is considered by some in the industry to be less useful because it makes use primarily of the 2 100 Mhz band, which does not offer good indoor coverage. Nevertheless, some countries use 3G in other bands and some M2M modules support 3G.
- 4G networks are increasingly prized because of their potential for use in a wide range of frequencies, including below 1 GHz, and their high throughput and low latency. 4G networks can also work in bands that currently support 2G and 3G. 4G IoT modules are still considered expensive, although prices are decreasing. Analysts predict that by 2022, 70% of M2M modules for M2M applications will use 4G. However, this would still leave 30% of the market based on 2G modules. Given the 10 to 20-year lifespan of M2M, this effectively means that 2G networks would need to remain operational well after 2030 (Connected World, 2014).
- There are, however, drawbacks to using 2G/3G/4G networks for large-scale IoT roll outs. The primary obstacle is SIM card lock-in. It is difficult if not impossible to switch mobile operators during the lifetime of the device, as any change in operator requires the physical replacement of the SIM card, which locks the device to a single operator. This hinders competition. In addition, it creates difficulties in achieving coverage, because even in dense cities no one network can claim full (indoor) coverage. If competitors' networks cover a location, then large-scale users may opt to use multiple networks at the same time. Moreover, mobile networks are not static and change their operating characteristics based on demands from network load and operations such as maintenance. Research in Norway has shown that up to 20% of devices are offline for at least 10 minutes a day, even in dense cities, without counting major network failures (Kvalbein, 2012).¹⁵ In addition, some sites may face congestion during busy hours. This may not be a problem for smart electricity meters, which can reschedule data shipments, but it does pose a problem for recharging an electric vehicle, traffic lights and payment terminals that require direct interaction. Some have suggested that additional quality-of-service mechanisms are necessary to deal with the best-effort nature of the Internet, in order to support critical IoT applications such as autonomous vehicles or eHealth. However, others argue that the inherent unreliability of the underlying network and the inability of higher networking protocols, such as IP, to effect change, calls for a more fundamental approach. This would involve making applications more resilient and allowing the fast switching of the underlying network using operator-independent SIM cards. In addition, international mobile roaming, though well supported, is expensive and no mobile network operator or alliance of operators has a wide enough footprint to offer good coverage and rates for some customer requirements.

One option is for governments to change regulations to allow private companies (not public telecommunication networks) to hold the numbers necessary for use in mobile networks, such as IMSIs for SIM cards, telephone numbers and mobile network codes. This would make the market for 2G/3G/4G connectivity competitive without long-term lock-in to a single network. Instead, customers could choose one or more networks per territory, based on their needs. They might even opt to use alternative networks, such as Wi-Fi networks, and employ their SIM card as an authentication mechanism. In the Netherlands, the government has changed the existing regulations in part at the request of its energy sector for the roll-out of smart meters. Enexis, a regulated utility managing an energy network, is the first private virtual network operator in the country to use its own SIM cards.¹⁶ It chose this solution to avoid lock-in and ensure flexibility in the future.

The governments of Belgium and Germany are also consulting on a possible rule change. The European Conference of Postal and Telecommunications Administrations (CEPT/ECC) working group on naming and numbering concluded in a report on IMSI numbers for SIM cards that:

CEPT countries should review the assignment criteria for E.212 Mobile Network Codes (MNCs) and consider introducing more flexibility regarding the assignment of MNCs for:

- a. Traditional market players such as MVNOs, MVNEs and Resellers; and
- b. Emerging business models such as M2M service providers and SMS Service Providers (ECC, 2014).

Some governments are of the opinion that changes to the relevant ITU recommendations are necessary to grant private networks access to IMSI numbers and related numbers. In 2015, the ITU Study Group 2 will discuss proposed changes to the relevant regulation.

As a result of potential lock-in with mobile networks and the challenges in achieving coverage, large-scale suppliers and users of the IoT have been looking at alternative networking options. It is instructive to examine various solutions used for automatic meter reading/smart grids. Telefonica together with Connode from Sweden won a 15-year contract to supply smart metering solutions in the United Kingdom, using a combination of 802.15.4 IPv6-based mesh networking and cellular connectivity. The mesh networking allows smart meters to use other smart meters to reach a hub that has cellular connectivity. If coverage is lost on one node, another node can act as a hub. In the Netherlands, Alliander (a regulated utility managing an energy network) purchased a CDMA450 license from an existing licensee to offer network services to its own operating companies for smart grid purposes, but also to third parties. CDMA450 offers better coverage than higher frequency networks and is used by some companies to deploy wireless telephony in rural areas. The technology has limited capacity for voice calls; however, CDMA450 or LTE450 may deliver data communication with better coverage than existing wireless technologies. In other countries, energy companies have opted to use power-line communication, which can take up to a day to relay messages. While too slow for real-time services, this option often proves reliable and falls under the control of the energy company. In some cases, metering companies have opted for a short-range drive-by system, where the meter is not permanently connected but communicates when a meter company vehicle passes nearby.

In the United Kingdom, a company called Neul (recently purchased by Huawei) advocates the use of whitespace spectrum – unused frequencies in the television bands. Its technology works on spectrum between 470 Mhz to 790 Mhz. In France, Sigfox aims to use unlicensed industrial, scientific and medical (ISM) bands (868 Mhz in Europe and 902 Mhz in the United States) with Ultra Narrow Band networks. A device can send up to 140 messages per day of 12 bytes payload. Although currently available in only a few countries, it received USD 115 million in funding in 2015 to expand locations. Another French company, Semtech, is promoting LoRa for long-range (up to 15 km) communication at low bit-rates with IoT devices.

These developments underline the need on the part of many users for communication over a widely dispersed area with large coverage. Alternative solutions to 2G/3G/4G are being developed, however only a few can make use of globally standardised spectrum bands and the available spectrum bandwidths are narrow, limiting their use.

IPv6 and the Internet of Things

IPv6 and the IoT are often perceived to be strongly aligned, to the extent that they are mutually reliant. The IoT needs the massively expanded protocol address space that only IPv6 can provide, while IPv6 needs to provide a substantive foundation to justify the additional expenditures associated with widespread deployment of this new protocol. Some argue that use of IPv6 would also alleviate shortages in telephone numbers and IMSI numbers. However, these are still necessary to identify a device in a mobile network over which IPv6 is run.¹⁷

However, the evidence to date on device deployments does not provide a compelling justification. Existing deployment of sensor networks, mobile devices and other forms of microware all use the IPv4 network. This is viewed as a pragmatic choice dictated by availability. While estimates vary, the consensus indicates that between 8 billion and 10 billion devices were connected to the Internet in 2012. At that time the Internet comprised about 2.5 billion addresses, indicating that the majority of these devices were located behind conventional Network Address Translation (NAT) units that allow one IPv4 address to be shared across multiple devices simultaneously.

This raises the question of whether the IoT requires IPv6 as an essential precondition, or whether an ever-expanding population of micro devices can continue to be deployed on the present address-sharing framework on IPv4, or a mix of IPv4 and IPv6 with translation between parts of the same network. This question also relates to the nature of the embedded device and the way in which it communicates within its external environment.

“Polled model” devices collect and retain data in local memory, then pass the data back to a controller when polled. In this data collection model the device is the target of connection requests and generally needs its own uniquely assigned public IP address. Given the large volume of devices contemplated in the IoT, the polled model would require the greater volume of addresses supplied by IPv6, and could not be sustained on IPv4.

An alternate sensor-reporting model is the “report to base” model, in which the device collects data and periodically initiates a connection to its controller to pass the data back. This second model functions adequately in an environment of IPv4 and NATs, as the device initiates connection requests and is assigned the use of a public address only for the duration of the connection. At the same time, this model essentially “hides” the sensor device from the external Internet, as the NAT function effectively prevents external agents from initiating any form of communication with the device.

Much of the work to date in sensor networks and similar application environments for embedded automated devices uses this “report to base” model of connection, which permits the devices to be located behind NATs and use the existing IPv4 network. Such devices do not add to the impetus for broad IPv6 deployment. However, when continuous sensor models (e.g. video streams or continuous environmental sensors) are considered, as well as forms of “just in time” opportunistic data collection, then the ability to poll sensors as and when needed becomes a significant asset and NATs become an impediment. In this case, using IPv6 is generally thought to be a necessary precondition. However, not using a NAT will expose unattended micro devices to the Internet. This has attendant issues relating to security and abuse, including the risk of such addressable devices being co-opted into various forms of high-volume distributed Denial of Service (DOS) attacks. The question of whether the larger address space of IPv6 effectively prevents the

opportunistic discovery of sensor devices, or whether operational prudence requires that such exposed sensors be equipped with robust security and continual monitoring and maintenance, is at present an open issue for the sensor industry.

Predictions and measurements of the size of the Internet of Things

There have been numerous predictions about the size of the IoT in the near future. The most widely cited is that of Ericsson, which stated in 2010 that there would be 50 billion connected devices by 2020. Prior to this, Intel estimated in 2009 that 5 billion devices were already connected to the Internet and predicted that this number would rise to 15 billion by 2015 (GigaOm, 2014). Cisco's Visual Networking Index 2014 also predicted 15 billion devices connected, although for 2018, while in 2013 the Cisco Internet Business Group estimated 50 billion connected things by 2020.¹⁸ These numbers could be judged to be excessive, and the timing could also be off by a few years. However, when the OECD evaluated the underlying calculations for the number of devices, they appeared sound. The main determining factors are the roll-out of fixed and mobile broadband and the decreasing cost of devices.

In 2012, the OECD produced its own estimates of the size of IoT usage in people's residences, with a view to verifying some of these claims. Today, in OECD countries, an average family of four with two teenagers has ten Internet connected devices in and around their home. Estimates indicate that this figure could rise to 50 by 2022 (Table 6.2). As a result, the number of connected devices in OECD countries would increase from over 1 billion today to 14 billion by 2022.¹⁹ This calculation only covers homes in OECD countries and does not evaluate growth in the number of connected devices outside OECD countries or in industry, business, agriculture and public spaces. It is not an unreasonable assumption that the market for the IoT outside of OECD countries is at least as big as for OECD countries.

Measuring the actual size of the IoT is harder, however. A device connected via Bluetooth or Zigbee, such as a light bulb, fitness bracelet or other device, may not show up on the network. These work via gateway devices, such as smartphones and dedicated home gateways, and the gateway devices themselves may operate behind firewalls, proxies and home routers that perform network address translation. In practice, this means that it is hard to look beyond the router into the home or to look across the mobile network and the smartphone to connected devices. However, the OECD and regulators have found a number of ways to measure the growth of the IoT.

One way of measuring the IoT is to look at the number of SIM cards and phone numbers allocated to M2M communication devices on mobile networks (Figure 6.3). Increasingly, governments require mobile operators to report the number of M2M devices on their networks. Some countries have gone further mandating that any device not used for telephony has to be assigned a (longer) M2M number rather than a traditional telephone number.²⁰ Current data show brisk market growth in SIM cards and phone numbers in many countries. Most countries report double digit growth between 2012 and 2013, although most lack data for 2011, so it is hard to analyse trends. Some operators are also reporting on the number of connected devices. AT&T in the United States, for example, reports that it connected 1.3 million devices on its mobile network in the second quarter of 2014, of which 500 000 were vehicles.

Table 6.2. Number of devices per household

| 2012 | 2017 | 2022 |
|--|---------------------------------|------------------------------------|
| 2 smartphones | 4 smartphones | 4 smartphones |
| 2 laptops/computers | 2 laptops | 2 laptops |
| 1 tablet | 2 tablets | 2 tablets |
| 1 DSL/Cable/Fibre/Wi-Fi modem | 1 connected television | 3 connected televisions |
| 1 printer/scanner | 2 connected set-top boxes | 3 connected set-top boxes |
| 1 game console | 1 network-attached storage | 2 e-Readers |
| | 2 eReaders | 1 printer/scanner |
| | 1 printer/scanner | 1 smart meter |
| | 1 game console | 3 connected stereo systems |
| | 1 smart meter | 1 digital camera |
| | 2 connected stereo systems | 1 energy consumption display |
| | 1 energy consumption display | 2 connected cars |
| | 1 Internet-connected car | 7 smart light bulbs |
| | 1 pair of connected sport shoes | 3 connected sport devices |
| | 1 pay-as-you-drive device | 5 Internet-connected power sockets |
| | | 1 weight scale |
| | | 1 eHealth device |
| | | 2 pay-as-you-drive devices |
| | | 1 intelligent thermostat |
| | | 1 network-attached storage |
| | | 4 home automation sensors |
| Devices that are likely, but not in general use | | |
| e-Readers | weight scale | alarm system |
| sportsgear | smart light bulb | In-house cameras |
| Network-attached storage | ehealth monitor | connected locks |
| connected navigation device | digital camera | |
| Set-top box | | |
| smart meter | | |

Some caution is necessary in interpreting the data, as these numbers are allocated to mobile operators of particular countries, however the devices may be used outside the country. This issue is notable in European countries where multinational corporations may purchase connectivity from one operator to cover all or part of Europe. An example is Sweden, where Telenor Connexion has a large M2M business, with a large proportion of the numbers used outside of Sweden. In addition some mobile operators will assign a number from a small country, such as Luxembourg or Malta, so that the device can, in principle, roam on all networks in other European countries. These countries will be overcounted, whereas other countries will see an undercount for the number of devices.

Across the OECD, regulators report that there are at least 83 million M2M numbers in use. There are 12 countries for which data are not available. Even if no growth between 2012 and 2013 was assumed for countries for which no data for 2012 were available, then the growth in number of M2M connections at 21%, or 12 million devices, can still be viewed as robust. These data do not capture all M2M devices connected through mobile networks, as an unknown number of users connect using consumer subscriptions. While the United States leads in absolute number of devices connected, Sweden leads on the basis of number of devices connected per capita. However, not all these devices may be located in Sweden (Figure 6.4).

Figure 6.3. Number of M2M SIM cards per country

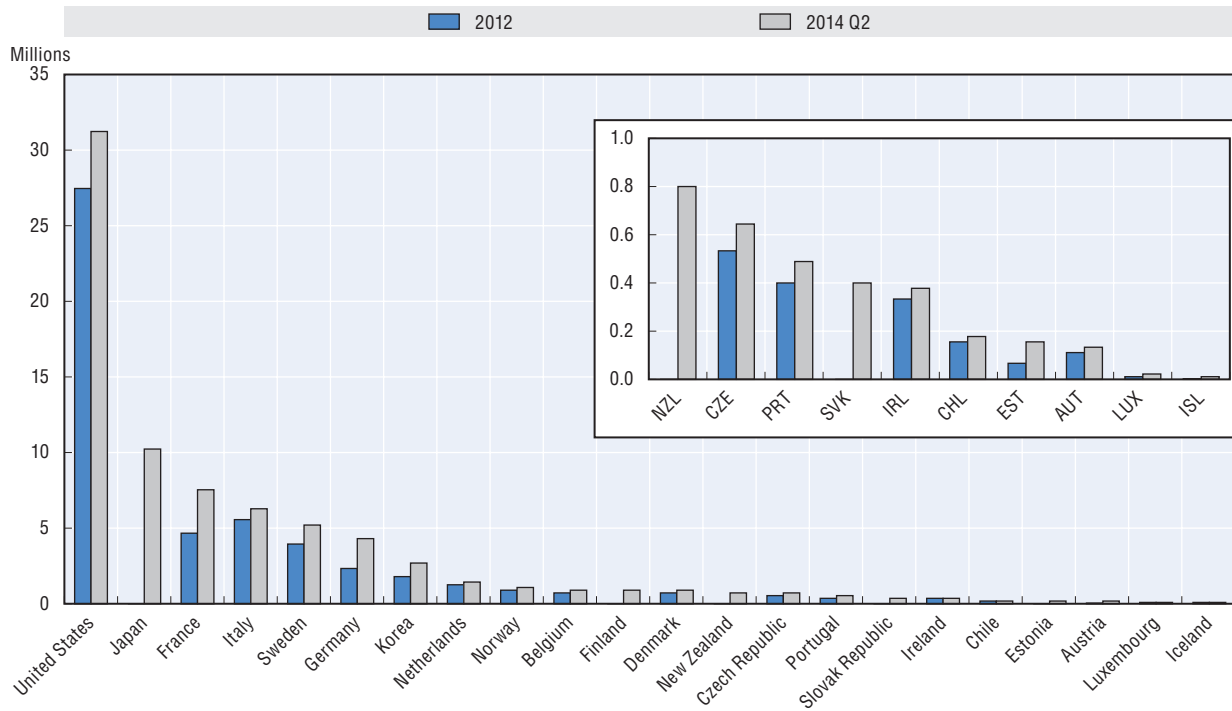
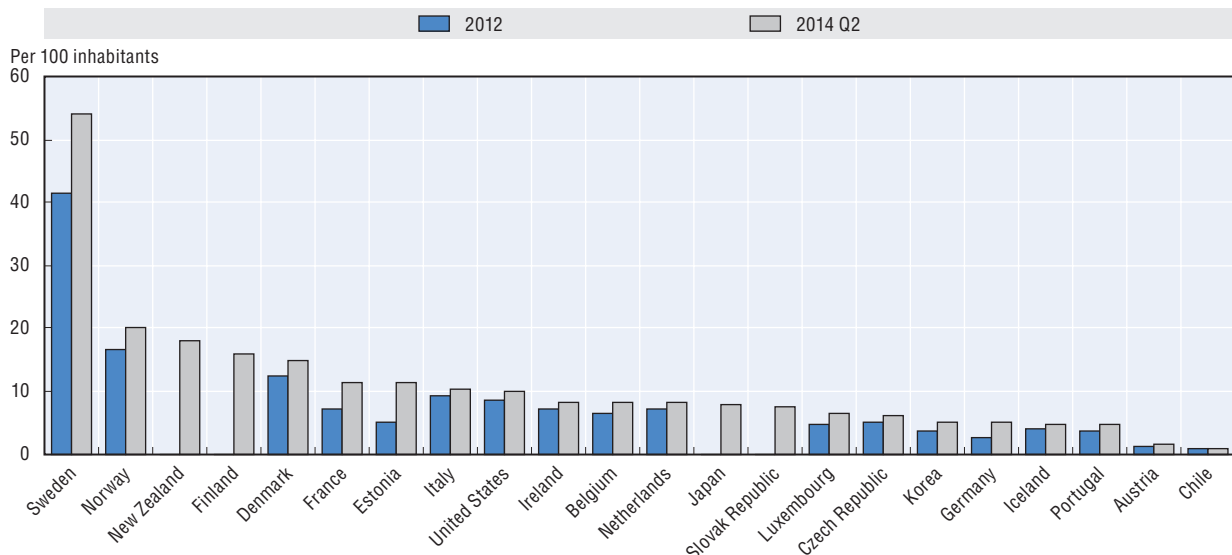
StatLink <http://dx.doi.org/10.1787/888933225289>

Figure 6.4. Number of M2M/embedded mobile cellular subscriptions, per 100 inhabitants

StatLink <http://dx.doi.org/10.1787/888933225295>

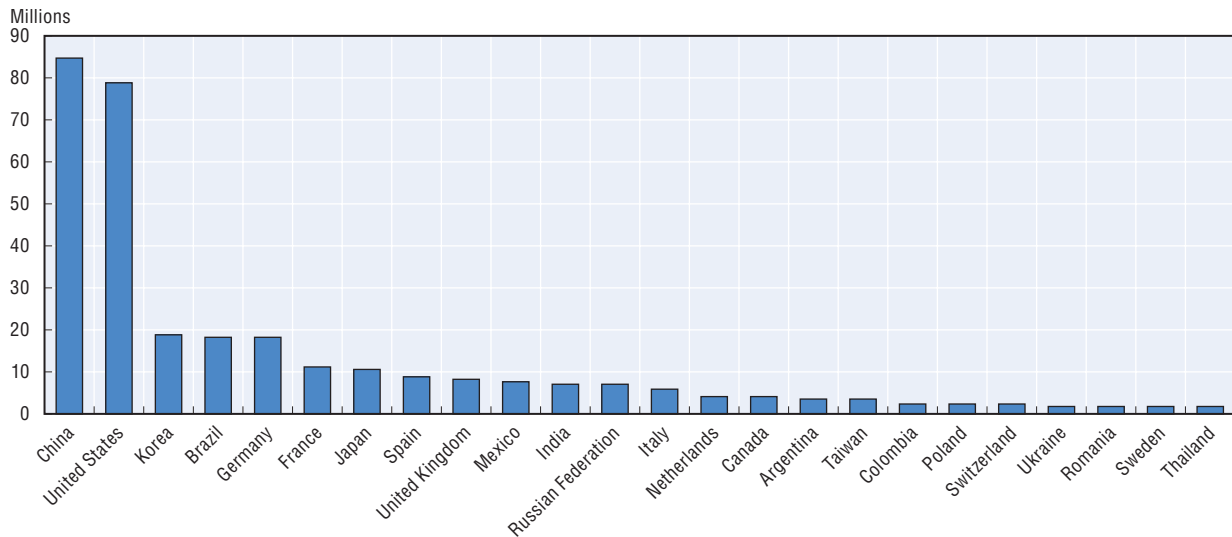
An alternative way of measuring the size of the IoT is to scan IP addresses for the types of devices connected to the Internet. Data from companies such as Shodan can be used for this exercise. Devices themselves often provide data on the brand and type of

device, or this can be inferred from the type of response they give. Although this approach is promising, the lack of a classification for devices producing the raw data hinders its use as a means to measure the size of the IoT. Security researchers have created profiles for specific devices, such as SCADA systems that control factories and energy plants, but as yet there is no general classification of devices. A more encompassing framework that will allow analysis of data received through scanning the Internet is likely to be created in the near future.

Even if all IPv4 addresses are scanned there are some limitations to the data. Not every device connected to the Internet will respond to every request to identify itself. System administrators may limit the types of requests a device will respond to and a large number of devices are located behind home and business DSL routers, cable modems and corporate firewalls that use Network Address Translation (NAT), which may not respond to random requests. In the case of Carrier Grade NATs used in mobiles, it is often impossible to reach individual devices.²¹ If networks switch to IPv6 this might become even harder, as it is impossible to scan all IPv6 addresses in a meaningful manner. While it may take a few hours to a day to scan all 4 billion IPv4 addresses, the IPv6 space is 4 billion times 4 billion times 4 billion times larger. Registration of IP addresses to countries can also be problematic. If the data from regional Internet registries (RIRs) are used some countries may be over-represented. For example, the network of Liberty Global, which spans multiple countries in Europe, is considered an Austrian network according to some IP location mappings. This is because the address space was registered by RIPE NCC to the Austrian branch of Liberty Global, but the space is used across all European subsidiaries of Liberty Global.

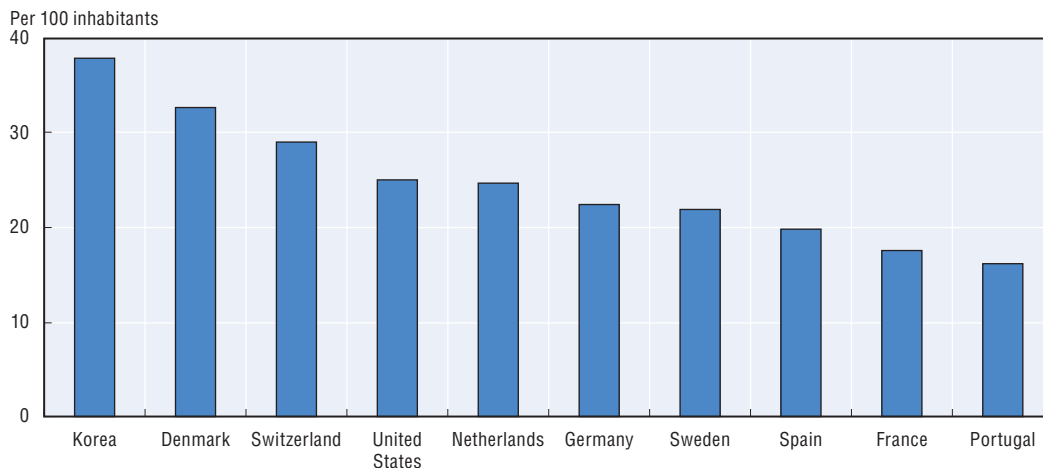
Even with these limitations the data provide an approximate overview of device locations on the Internet. Shodan finds 363 million devices online (Figure 6.5) with some 84 million registered to China and 78 million to the United States. Korea, Brazil and Germany follow with 18 million connected devices, and Japan, Spain, the United Kingdom and Mexico make up the rest of the top 10 with 8 million to 10 million devices. Efforts to rank devices per capita are hindered by data limitations, but an experimental top 10 is provided (Figure 6.6). For example, Luxembourg does not rank high in terms of this approach because some operators use Carrier Grade NAT for their FTTH implementation, effectively shielding all devices behind the NAT.

Other approaches could be based on the number of Bluetooth, Ethernet, IEEE 802.15.4, Wi-Fi and 2G/3G/4G chips shipped. Estimates for shipments can be obtained from industry analysts, although the methodologies may not be transparent. Difficulties can arise, however, in combining the data as some devices will have multiple chips and chipsets on board. The Wi-Fi-alliance states that in 2013 an estimated 2 billion Wi-Fi-enabled devices were shipped. Over 2 billion Bluetooth chipsets were shipped in 2013, with smartphones making up 61% of that market. It is likely that there is an almost complete overlap between smartphones, laptops and tablets that integrate both Wi-Fi and Bluetooth, but it is unclear whether sales figures distinguish correctly between the two if Bluetooth and Wi-Fi form part of the same chipset. With sales of laptops, tablets and smartphones close to 1.5 billion units, this would indicate that up to 1 billion other wireless connected devices were sold. Data for sales of 802.15.4 chips are unfortunately not available.


Figure 6.5. **Devices online, top 25 countries**

Sources: Based on Shodan, www.shodanhq.com.

StatLink  <http://dx.doi.org/10.1787/888933225304>

Figure 6.6. **Devices online per 100 inhabitants, top OECD countries**

Sources: Based on Shodan, www.shodanhq.com.

StatLink  <http://dx.doi.org/10.1787/888933225312>

6.3 Fostering public policy goals with the Internet of Things

A number of governments have introduced regulations that rely on data from the IoT. For example, remotely monitoring traffic lights and dykes allows governments to optimise traffic flow and better understand flooding risks. The IoT also allows governments to achieve policy goals in new ways. For example, some governments now use GPS and mobile communication to calculate road pricing based on time of day and distance travelled, with a view to reducing congestion. This represents a shift from conventional road-pricing systems, which relied on a toll booth or digital moat around a city to charge all incoming traffic a flat congestion charge.

eHealth

Analysts and governments have high expectations of eHealth devices that will allow remote monitoring of patients at home or work. However, only a few certified devices are available on the market. This appears to be due not to a lack of research or government commitment, but rather to difficulties in implementation. One example is created by the use of portable eHealth equipment in conjunction with near real-time data streaming to a central server. Users of portable Electro Cardiogram (ECG) equipment have reported an increase in anxiety as a result of calls from carers resulting from anomalous readings, possibly caused by a user moving out of range, compounded by an inability to distinguish between an emergency call and a service call.²² Regulators also have to certify the equipment and the associated applications. In the case of a radiology application, regulators also needed to verify the quality of the iPad screen to ensure it can display the images at the correct quality and luminescence. Such problems are not easily rectified by a simple change in policy. Instead they require the consistent evaluation of each new application with a view to minimising the risks to users, while maximising the benefits.

Transport

Road toll systems in most OECD countries are based on RFID technology, activated when a user drives through a toll-gate. The drawback of this system is its inflexibility. It works only on main highways and equipping new roads with the system can be expensive as this necessitates a redesign of the road. GPS-based systems that use wireless networks to communicate can function on any road and do not require physical infrastructure. However, implementation has proven more challenging than expected in countries that have tried. The reasons for this include a failure to reach agreement among stakeholders and issues relating to technology and price.²³ Germany and Hungary have GPS-based tolls in operation for trucks above 12 tonnes and 3.5 tonnes respectively. Belgium will use the same system as Germany for trucks as of 2016. Germany uses an integrated system where the on-board unit and back-office systems are provided by one company, Toll-Collect. Hungary's system is more modular and relies on a number of manufacturers and service providers for the on-board unit. These companies can also provide fleet-management (location, fuel consumption) solutions to hauliers, which has allowed the Hungarian system to act as a platform for additional services to the industry.

The European Commission has proposed eCall in all vehicles sold in the European Union. This initiative is designed to bring rapid assistance to motorists involved in a collision anywhere in the European Union. The EC proposals for legislative acts foresaw full implementation and seamless functioning of eCall throughout Europe by end-2015. However, the adoption procedure for these legislative acts by the European Parliament and the Council is still ongoing, so the deadlines for implementation will most likely be delayed to end-2017 or early 2018. In Brazil, a similar system (Denatran/SIMRAV) will become mandatory and is targeted for release during 2015. This system is designed to prevent vehicle theft, but will also enable other services. Manufacturers of vehicles also expect the eCall system to become a platform for other on-board services.

Online on-board services using inbuilt mobile communications are currently more popular in North America, where examples such as OnStar of General Motors, Bluelink of Hyundai and BMW Assist, provide emergency services, theft protection and similar services. Most manufacturers choose a hybrid system that incorporates a mobile communications unit on-board for emergency services, but uses the driver's mobile phone

for other services. It is also possible to connect to the vehicle using a smartphone and read its location, tyre pressure and other mechanical properties, or heat up the vehicle prior to departure. Accurate numbers across the North American market are difficult to obtain for all manufacturers. This type of service is becoming a standard feature on new vehicles and AT&T reports connecting to 2 million vehicles per year. OnStar has over 6 million users in Canada, China and the United States, while BMW Assist has over 1 million users.

The IoT can also be used to connect data about road usage with vehicles and traffic lights. Several navigation providers, such as Garmin, Google and TomTom, make use of data from governments and mobile networks on the speed of vehicles in certain locations to provide their customers with real-time traffic updates. Transport for London has gone one step further and connected data on road usage with real-time control of traffic lights in the city. The collected data are fed to a machine-learning algorithm, which aims to optimise traffic flow. The system known as SCOOT is said to deliver on average a 12% improvement in traffic flow. It is likely that other large cities will aim to introduce similar systems to improve in-city traffic flows.

Energy

Smart grids are another area where countries expect the IoT to benefit their economies. Smart grids will allow two-way communication between the home/business and the energy grid. This will increase consumer awareness of their energy consumption, which policy makers expect to result in reduced energy consumption, but will also deliver energy back to the grid, which could promote the use of renewable energy sources such as solar and wind power. Accordingly, the European Commission required all European Union member states to conduct a cost-benefit analysis of smart meters, with countries implementing smart meters in 80% of positively assessed locations by 2020. In 16 European Union member states the cost-benefit analysis was positive and smart meter roll-out will commence. In seven countries the analysis was negative or inconclusive, but in some of these, such as Germany, roll-out will commence for certain groups of customers (EC, 2014).

In the United Kingdom, consumers with smart meters will be offered an in-home display (IHD) which will let them see how much energy they are consuming and its associated cost. In addition, the communications hub in the meter will allow users to connect third-party devices and services to the meter and develop services around it.²⁴ The smart meter is expected to function as a platform on which the IoT can be built. Expected benefits include:

- near real-time information on energy use, expressed in pounds and pence
- the ability to manage energy use, save costs and reduce greenhouse gas emissions and other harmful gases and particles
- an end to estimated billing with customers charged only for the energy they actually use, helping them to budget better
- smoother and faster switching between suppliers to obtain better deals
- supplier access to accurate data for billing, removing the need to manually read meters.

The energy crisis in Japan, resulting from the 2011 Tōhoku earthquake and tsunami, prompted the Tokyo energy company Tepco to accelerate its plans for smart metering. The company intends to roll-out a network by 2018 to cover 80% of its customers. The innovative network will be based on IPv6 over wireless mesh networking, cellular network and power-line communication. It will transmit meter data every 30 minutes – much more

frequently than most existing systems. In addition, it will act as a two-way system that supports push messaging demand response and energy management capabilities, all the way to individual devices in the home. To ensure security Tepco have adopted an end-to-end security model. The result should be a system that can support the future of electric vehicles, solar cells and building energy management systems (St. John, 2014).

In the United States, a federal stimulus programme designed to counter the global economic crisis aimed to promote the roll-out of smart grids to promote energy efficiency. As a result, two-way communicating smart meters were installed in 50 million households (43% of the total) by September 2014 (IEI, 2014). Over 8 million customers can participate in a variety of “smart pricing” programmes, which reward participants for voluntarily reducing energy consumption when demand for electricity and prices are expected to be particularly high. In some cases, customers make use of connected thermostats and other devices to automatically change their usage in line with smart pricing programmes.

Cities

In addition to the above examples for transport and electricity, city governments increasingly use the IoT to pursue policy goals. For example, the city of Boston has developed a mobile app, StreetBump, that sends data from the smartphones of citizens driving through Boston. Making use of the accelerometer (motion detector) and GPS, StreetBump identifies potholes and bumps and communicates their location. Other examples include Barcelona’s app 2.0 incidències, which reports on commuter rail service interruptions or delays in the metropolitan area of Barcelona, or San Francisco’s Cycle Track app that informs transport planners about bicycle trips in the city and thus on the actual use of existing bike lanes and the need for new ones. Several cities are currently looking into upgrading public rubbish cans to communicate how full they are, which would allow trash collectors to optimise their routes and stops. The increasing amount of real-time, fine-grained IoT data enables more targeted and cost-effective infrastructure maintenance, service improvements and investment decisions in cities.

Public policies that promote or affect use of the Internet of Things

The potential benefits of the IoT feature in a growing number of public policies, either as a means to achieve goals or an area targeted for research. There is no consistent approach among governments to the IoT, but some examples can be provided.

The European Union has made the IoT an essential part of its Digital Agenda for Europe 2020, which focuses on applications, research and innovation, and the policy environment. The European Union has been particularly active in promoting research and innovation:

*The Internet of Things European Research Cluster groups together the IoT projects funded by the European research framework programmes, as well as national IoT initiatives. The requirements of IoT will also be fed into the research on empowering network technologies, like 5G Mobiles. The Future Internet public private partnership will develop building blocks useful for IoT applications, while Cloud Computing will provide objects with service and storage resources. On the application side, initiatives like Sensing Enterprise and Factory of the Future help companies use the technology to innovate, while experimental facilities like FIRE are available for large-scale testing.*²⁵

In February 2014, the Korean government published its plan for building the IoT with the aim of launching a hyper-connected “digital revolution” to address policy goals. One of the aims was to promote IoT-driven economic development, existing examples of which

include Songdo Smart City and smart eel farms (Box 6.3). The plan aims to commercialise 5G mobile communication by 2020 with Gigabit Internet achieving 90% of national coverage by 2017. In addition, a total of 1 GHz of spectrum will be freed by 2023 and IPv6 infrastructure further expanded into the subscriber network by 2017. The plan also emphasises the development of low-power, long-distance and non-licensed band communication technologies for connecting objects in remote areas (Ministry of Science, ICT and Planning, 2014).

Box 6.3. IoT advances in Korea

Smart farm projects

In January 2014, SK Telecom introduced an IoT technology-based eel farm management system. Farmers can monitor their fish tanks in real time through smart devices including smartphones. In general, each eel farm has 20 to 60 water tanks breeding about 10 000 eels, which are worth over USD 100 000 per tank. Eel farming is a high value-added business, but the farming requires farmers to frequently monitor a variety of indicators as even minor environmental changes are fatal to eels. Under the IoT-based fish farming management system, three sensors are installed on each fish tank to measure water temperature, quality and oxygen level. The farmer can operate the sensors and machinery remotely when intervention is needed.

Songdo Smart City

“Songdo” city is a new city built on a peninsula off the coast of Seoul, which will become home to 200 000 people. The whole city is wired with fibre optics to connect the different systems that keep Songdo city running. Telepresence is installed in homes, offices, hospitals and shopping centres to allow people to make video calls wherever they want. Sensors are embedded in streets and buildings to monitor everything from temperature to road conditions. These sensors also monitor fire and safety in many towers. The wireless sensor networks used in Songdo are designed specifically to create smart cities. The aim is to build a distributed network of intelligent sensor nodes that can measure a variety of parameters for more efficient management of the city. Data are delivered wirelessly and in real time to citizens and the appropriate authorities. Citizens can monitor the pollution concentration in each street of the city. The authorities can also optimise irrigation of parks or lighting throughout the city. Water leaks can be easily detected and vehicle traffic can be monitored in order to modify street lights. Systems that detect and transmit the location of available parking spots will reduce traffic congestion and pollution, and save time and fuel.

When rolling out IoT services nationwide, conflicts with existing regulation and regulatory uncertainty may act as bottlenecks. For example, existing medical regulations may hamper innovative services by requiring the presence of a doctor on both ends of a tele-medicine consultation. Such regulations undermine a key advantage of tele-medicine – the ability to consult a medical practitioner when factors such as distance would make this otherwise impossible. With this in mind, the Korean government has established a “telecommunication strategy council” which will aim to improve general regulations. It will also establish an IoT testbed as a regulation-free zone and aim to improve the legal system.

The German government has launched innovation clusters directly tied to the IoT. For example, the “Cool Silicon” innovation cluster in the south of Germany aims to develop low-energy and energy self-sufficient processors and sensors. Another innovation cluster called

“IT’s OWL”, located in central Germany, focuses on creating intelligent and autonomous industries through the use of robots. Also in Germany, Microtec Sudwest aims to develop new sensors, microsystems and flexible, bendable chips. A fourth cluster focuses on software for new industries. Each of the research clusters is tied to a large number of businesses, universities and research centres in the region that combine to deliver the output.

Other countries have acknowledged the future of the IoT in their policies, and its underlying and accompanying developments in the cloud, big data, sensors and actuators and the aims of autonomous machines and systems. Some have started to assess whether current policies are still in alignment with the perceived future (Box 6.4). Ofcom in the United Kingdom, for example, has started a consultation on the implications of IoT for spectrum and numbering policy (Ofcom, 2014). The Netherlands, the first country to liberalise access to IMSI numbers for SIM cards, is consulting on further policies regarding signalling point codes needed for routing traffic in mobile networks.²⁶ Liberalising access to IMSI numbers has enabled Enexis, a Dutch energy network, to deploy 500 000 SIM cards (not tied to a mobile operator) to its smart meters. The Belgian government has indicated its support for this approach (BIPT, 2014). Some countries are of the opinion, however, that a change of the ITU E.212 recommendation is required – something that is being discussed in 2015.

Governments will also have to re-evaluate a large number of policies. These include policies surrounding naming and numbering, particularly with regard to numbers used in mobile networks, where further liberalisation and access for private networks could bring great economic benefits. Numbering policies surrounding IPv4 and IPv6 do not appear to need fundamental changes, as these numbers are already available to all interested parties, although the number of available IPv4 addresses is limited.

Policies surrounding the use of “national” numbers on an international scale will also need discussion. For example, does it matter when “national” numbers are used outside the national territory? Conversely, does it matter when a device with a foreign IMSI number or foreign E.164 (telephone) number is used within a territory? Although this practice is common for IP addresses, which have no strict link to a country, these questions are now being asked by national telecommunication regulators. There are already cases where governments and incumbent operators have declined to allow “foreign” devices roam in their country permanently, despite the payment of all applicable charges and taxes.

Spectrum is necessary for the IoT, although it is unclear how much. Globally harmonised ranges would be best, but may be unattainable. In and around people’s residences and businesses, unlicensed bands have proven to be of great value. Lack of competitive offers that fit their circumstances has pushed some large-scale IoT users to try to obtain access to their own dedicated spectrum or to find alternatives. Others have sought to create dedicated bands for IoT communication, sometimes with service providers that have monopoly power.

Standardisation has proved difficult. Because the IoT encompasses everything from the technical level upwards, it also affects business processes and even political decisions. As such, there is no single standard and as a result standards are fragmented. Large manufacturers often back multiple competing standards at each level, thereby failing to ensure consumer confidence by choosing one particular standard. There is a chance that countries and economic sectors will decide to use different and competing sectors, thus creating a situation of inoperability and fragmentation. However, it is equally possible that flexible frameworks will develop where devices can interoperate with multiple standards at the same time.

Box 6.4. IoT policy in the United States

At the Federal Communications Commission, the Technological Advisory Council (a group of academic and industry experts appointed by the FCC Chairman) is studying issues surrounding how the IoT will effect communications networks in the next 10 to 20 years. In December 2014, the IoT Working Group made the following recommendations to the TAC:

- The FCC should programmatically monitor consumer IoT network traffic impact on WLAN and WWAN with a focus on new high bandwidth consuming applications.
- The FCC should focus on availability of unlicensed spectrum suitable to a range of PAN/WLAN services without making spectrum allocations unique to IoT, and ensure there is enough short-range spectrum to meet growth in PAN/WLAN requirements and sufficient network capacity upstream from IoT devices and proxies.
- The FCC should define its role within the context of an overall cybersecurity framework, dedicating resources and participating in IoT security activities with other government stakeholders.
- The FCC (in collaboration with other agencies) should conduct a consumer awareness campaign related to IoT security and privacy.
- The FCC should conduct internal periodic scenario exercises to determine appropriate response to widespread consumer events related to the IoT.

In February 2014, the United States National Institute for Standards and Technology (NIST) released a “Framework for Improving Critical Infrastructure Cybersecurity,” which provides a structure that organisations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programmes. Designers of ICT systems (including those with IoT components) in any country can utilise this framework to enhance their systems security. In August, NIST convened its first meeting of the Cyber-physical Systems Public Working Group to develop and implement a cybersecurity framework for IoT with the goal of establishing an integrated and interoperable system across all economic/industry sectors. NIST plans to produce a draft “reference architecture” by early 2015.

In November 2014, the National Security Telecommunications Advisory Committee (NSTAC, a group of representatives from large information and communications corporations that reports to the President) released a draft report on IoT, urging the US government to take actions to secure the IoT. The report identifies risks associated with the IoT with a focus on critical infrastructure, concluding that, “there is a small and rapidly closing window to grasp the opportunities of the IoT in a way that maximizes security and minimizes risk. If the nation fails to do so, it will be coping with the consequences for generations”. The report further states that, “there are only three years – and certainly no more than five – to influence how the IoT is adopted”. While the report highlights the benefits of the IoT, it warns that “the rapid and massive connection of these devices also brings with it risks, including new attack vectors, new vulnerabilities and perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction”.

The NSTAC report made several recommendations for the Obama Administration to work on. The Department of Commerce, specifically NIST, was tasked to develop a definition of the IoT for departments and agencies to use during assessments related to the IoT. NSTAC recommended that the White House Office of Management and Budget (OMB) require all federal departments and agencies to conduct an internal assessment of IoT capabilities that currently or could potentially support national security and emergency preparedness (NS/EP) functions. Furthermore, it stated that OMB should direct federal departments and agencies to develop contingency plans to identify and manage security issues created by current and future IoT deployments within the United States Government. These plans should anticipate an environment that cannot be fully secured because of the dynamic nature of the IoT and the potential threat. NSTAC recommended that the President create an inter-agency task force to coordinate with existing organisational bodies to foster balanced perspectives between security, economic benefits and potential risks. Participants should include, at a minimum, the Departments of Commerce, Homeland Security and Defense, and set milestones for the completion of a set of activities relevant to NS/EP.

As the IoT is pervasive, it will touch much of government policy. Policy makers should not just identify the potential benefits from IoT, they should also identify where the data and functionality offered by IoT could be leveraged and combined with other data elsewhere. The above-mentioned Hungarian case of creating an open system for road tolls, where data are also available to hauliers for their logistical processes, constitutes such an example.

Building the Internet of trust

In order to ensure that the IoT works to the benefit of people, some have argued that it should be thought of as the “Internet of Trust”, as trust will be fundamental to enhancing user experience and addressing key legal challenges such as user privacy. Another pertinent factor is that while the “IoT is global .. the law is not” (Cappgemini, 2014). The OECD has typically considered security, privacy and consumer protection as key elements for building trust in new technologies such as the IoT (OECD, 2015). This means prioritising security for devices connected to the IoT against cyber-attacks and ensuring the confidentiality and integrity of data communicated between devices. As already mentioned, this will require a shift in mindset from a traditional to a risk-based security approach (OECD, 2015).

Addressing the protection of personal data is more complicated. Broadly speaking, the privacy challenges raised by the IoT are not new. However, the enormous increase in the collection and use of data, its new and unanticipated uses, and the increased complexity and all-pervasive nature of the IoT present new challenges to traditional principles such as data minimisation, notification and consent. This complexity will make it more difficult for individuals to control and police data collection, especially when they are not actively involved or aware that it is occurring (OECD, 2015).

Individual preferences with respect to the use of personal data are nuanced and contextual, and are influenced by factors such as trust in service providers, perceived value exchange and other attitudinal, demographic and cultural factors. Acceptable practice is therefore subjective and may evolve (WEF, 2014). Data-use policies that treat all data equally and have universal application are neither appropriate nor sufficiently flexible. However, the difficulty of building context-related nuances with appropriate safeguards into regulations should be recognised.

One possible way forward is to learn from the experience of security risk management. Risk management could be adopted as an approach to privacy protection in a context-dependent environment that is rapidly evolving. This could be achieved in particular through the development of privacy management programmes to implement accountability (OECD, 2013a). This would take into account data sources and quality, as well as the sensitivity of the intended uses with a view to mitigating the risks of misuse. Such an approach would need to consider the wide range of harms and benefits, and be simple enough to be applied routinely and consistently. Privacy-enhancing technologies also have a role to play in reducing the identifiability of individuals, and in improving traceability and accountability.

The third element in building trust is consumer protection and empowerment, whose basic tenets revolve around adequate information disclosure, fair commercial practices including quality of service, and dispute resolution and redress. In increasingly complex environments involving a number of devices and parties, it will become more difficult for

consumers to know where a problem lies when it arises, and who is responsible for its resolution. Take, for example, the case of devices with firmware and software supporting an app for health monitoring. If the app ceases to work following a software update, who is responsible? Assuming the user can identify the issue, who should they turn to for assistance? Furthermore, for how long should such hardware or software be expected to function?

How well existing consumer protection frameworks address these challenges (or will be adapted to do so) is yet to be determined – a point recently discussed by the Committee on Consumer Policy in the context of its revision of the OECD's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce*.²⁷ Some consumer organisations such as Consumer Action in the United States have already spoken at conferences on the subject of consumer protection frameworks in light of the IoT.

Managing security risks

Management of digital security risks has long been an issue in communication networks, and the commercialisation of the Internet has seen security concerns grow in scope and scale. Critical infrastructure increasingly depends on ICTs and communication networks, and guarding against accidental or malicious interference is becoming ever more important. End-to-end security is paramount for the IoT and must be built into networks and devices. Moreover, effective management of security risks will be essential.

Take, for example, a smart metering system with a network of electricity meters that measure consumer usage and send data to an electricity company's servers. There are numerous ways that such a system could be compromised: a fake meter could transmit false data, a genuine meter could be tampered with to send incorrect data, data from a meter could be intercepted and modified by a network eavesdropper, and malicious users could install a fake server or compromise a genuine one to issue malicious commands or upload malicious firmware to meters on the network (Rubens, 2014).

Successfully hacking approaches such as this could have potentially devastating consequences. In 2012, the US Federal Bureau of Investigation reported that several smart meter hacks had occurred over the previous few years, costing hundreds of millions of dollars a year (KrebsOnSecurity, 2012). One commentator has identified three likely forms of attack (Baudoin, 2014):

- Eavesdropping on data or commands could reveal confidential information about the operation of the infrastructure.
- Injecting fake measurements could disrupt control processes and cause them to react inappropriately or dangerously, or could be used to mask physical attacks.
- Incorrect commands could be used to trigger unplanned events or to deliberately send physical resources (water, oil, electricity, etc.) to unplanned destinations.

The United States Federal Trade Commission (FTC) has also taken enforcement action. In 2013, the FTC charged TRENDNet, a maker of video cameras designed to allow consumers to monitor their homes remotely, with lax security practices that exposed the private lives of hundreds of consumers to public viewing on the Internet. In its complaint, the FTC alleged that, from at least April 2010, TRENDnet failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement. Under the terms of its settlement with the FTC, TRENDnet is prohibited from misrepresenting the

security of its cameras or the security, privacy, confidentiality or integrity of the information that its cameras or other devices transmit. In addition, TRENDnet is required to establish a comprehensive information security programme designed to address security risks that could result in unauthorised access to or use of the company's devices, and to protect the security, confidentiality and integrity of information that is stored, captured, accessed or transmitted by its devices. The settlement also requires TRENDnet to notify customers about the security issues with the cameras and the availability of the software update to correct them, and to provide customers with free technical support for two years to assist them in updating or uninstalling their cameras (US FTC, 2014).

The OECD is currently undertaking a review of its 2002 *Guidelines for the Security of Information Systems and Networks*, in line with the changing context (OECD, 2012b):

- The threat landscape has evolved in scale and in kind. Since 2002, cyber criminality has considerably increased and the exploitation of vulnerabilities in information systems provides an opportunity for economic, social and political disruptions of all kinds (“hacktivism”).
- The perimeter of information systems is increasingly blurred. In a hyper connected world – where every process, device and infrastructure is in some way interconnected – it is becoming difficult to define the perimeter of information systems or corporate networks.
- IT and the Internet have evolved from being useful to individuals and organisations to being essential to society.
- Cybersecurity policy making is at a turning point. Responding to cybersecurity challenges has become a national policy priority in many countries.

A risk-based approach recognises that guaranteeing end-to-end security in the IoT is impossible and that it is up to everyone, including consumers, to assess the likelihood of problems occurring and the potential impact, and to take responsibility for their actions. The key message is that you cannot secure your digital environment and that you cannot expect “suppliers” to do everything for you. It therefore becomes a matter of assessing and managing the risk. Governments have a particular role to play in educating consumers and citizens in this regard. However, this is quite a sophisticated and subtle message and making intelligent decisions may be beyond the capability of many consumers. Perhaps a new class of trusted intermediaries will emerge to manage interactions with the IoT on consumers' behalf.

Governments also have a role to play in fostering the development of a common set of standards, which would become a benchmark for the required level of security expected from a device. The goal is not to guarantee absolute levels of security. Instead it is necessary to instil confidence and trust among consumers that, in the event the security of their device is breached (especially as new vulnerabilities emerge), the problem will be addressed. Cross-country adhesion to a similar set of standards would avoid creating trade barriers by requiring different standards.

Privacy

Data protection and privacy are key concerns associated with the IoT. However, ever since the invention of the telephone and the camera, the adoption of new technology has challenged privacy. With billions of connected devices in the IoT transmitting and receiving

huge amount of data, much of it sensitive personal data, a key question is: “To what extent is it necessary to rethink approaches to data protection and privacy?” According to US FTC Commissioner Brill, “We should all be concerned that questions about privacy will keep consumers away from the IoT because they do not trust it” (Brill, 2014).

A key privacy issue relates to consent, particularly regarding possible onward use of data outside the initial terms of an agreement. Will consumers in the IoT retain control of their data or will they be unwitting participants in a system that neither respects nor needs their consent? This fear is compounded by the enormous number of organisations that might be able to use personal data and benefit from the nascent potential of data analytics.

Devices connected to the IoT will send and receive frequent, sometimes continuous, data streams. If collection of this data were to rely on traditional notification and consent, people would be prompted hundreds or thousands of times a day. In addition to the inconvenience to individuals it might slow the IoT to a grinding halt (Wolf and Polonetsky, 2013). Adhering to a traditional approach of notification and consent to protect privacy might lead consumers to just give up or to turn down requests as a default option. Providing effective information disclosure to consumers as a basis for privacy protection is already a challenging issue. The IoT will compound the difficulties.

Some have argued that the scale and complexity of the IoT signals the death of privacy (Rauhofer, 2008). Others respond that there is nothing fundamentally new about the IoT in terms of its implications for privacy (Pasiewicz, 2008). Nevertheless, there are several emerging approaches, such as the proactive “baking in” of privacy to the IoT at the design stage.²⁸ Some think that the IoT will stimulate the emergence of trusted intermediaries (or infomediaries), such as OpenPDS, who will manage the use of data on the behalf of consumers (Co.Exist, 2014). Others believe that these approaches will be insufficient to resolve the challenges and argue that data ownership should be rethought completely. Tim Berners-Lee, the inventor of the World Wide Web, for example, believes that the data people create about themselves should be owned by each individual, not by large companies that harvest data (Hearn, 2014; see also *Edge*, 2012).

Instead of focusing on the collection and communication of information, Wolf and Polonetsky, co-chairs of the think tank Future of Privacy Forum, argue that it is more important to focus on how personal data is used (Box 6.5). Whether a use model would provide more effective protection in practice is disputed, and remains a topic of ongoing discussion and debate among experts (OECD, 2014).

Box 6.5. A use-focused privacy paradigm for the Internet of Things

- “Use anonymised data when practical.”
- “Respect the context in which personally identifiable information is collected.”
- “Be transparent about data use.”
- “Automate accountability mechanisms.”
- “Develop Codes of Conduct.”
- “Provide individuals with reasonable access to personally identifiable information.”

Source: Wolf and Polonetsky, 2013.

Consumer protection and empowerment

As mentioned above, the key consumer issues subject to considerable policy attention in the e-commerce environment (e.g. privacy protection, the need for adequate information disclosures, fair commercial practices, and dispute resolution and redress) are likely to be amplified in an IoT context, where multiple parties engage in a complex set of transactions with consumers.

As regards disclosure, a charter developed by the Alzheimer's Society (2014), provides people with dementia and their carers with a list of questions to consider prior to purchasing or accessing technology used to deal with the consequences of this illness (Box 6.6).

Box 6.6. What to consider when purchasing IoT equipment related to dementia

Questions for professionals working in dementia

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

Questions for individuals, families and carers

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

Source: Based on Alzheimer's Society (2014).

While not all the questions in Box 6.6 may be appropriate for every IoT product, they provide an interesting overview of the type of information passed on to consumers at an early stage, so as to engage in an IoT transaction in an informed manner. Such information should help consumers to:

- access and use devices and related services in an easy manner and at all times
- determine the level of interoperability of the IoT devices
- identify who to turn to when problems with such devices arise.

One of the major drivers of consumer adoption of the IoT is likely to be the desire to make life simpler. But even one device such as a smart heating controller can be quite complex to programme and manage, and anyone with several devices may need guidance on ways to access and use them. A related issue is the need to ensure that consumers can access and use their devices and associated services within the IoT network, on any Internet connection, in an effective and uninterrupted manner. This will help to address situations where access to devices is prevented when part of the network goes offline. Likewise, the lifetime of IoT devices will need to be explored. This will mean examining conditions for updating software and the continued functioning of devices in an IoT network. In recognition of the need for enhanced consumer understanding of IoT device functionality and limitations, and for trusted compliance processes that will operate along the IoT supply chain, the United Kingdom Information Economy Council has developed a voluntary consumer-focused framework of recommendations. This aims to help address consumer expectations and to provide consumers with adequate disclosures about their rights and obligations in an IoT ecosystem (BT, 2014).

Ensuring a greater level of interoperability for connected devices and providing consumers with adequate information will be key to building a trusted and reliable IoT ecosystem. Exploring ways to overcome software update management challenges will also be essential to maintain interoperability between older and newer consumer IoT devices. In the area of payments, this will involve addressing problems associated with the range of diverse NFC systems in operation, as pointed out in a study of NFC in public transport (Liebenau et al., 2011). Proprietors of those systems currently have no incentive to make their payment cards interoperable with other systems, however convenient this might be for consumers.

However, the complex structure of the IoT market may not only obscure which provider is responsible for a particular problem in the value chain, but also which authority can help consumers and be involved in the policy decision-making and enforcement process. In the NFC area, regulatory responsibilities for both the development of NFC-related rules and their enforcement are quite fragmented in some countries. One example of this is Australia (Box 6.7), although it is likely other countries have similar structures.

The ongoing development of separate responses to emerging technology developments risks an overall loss of regulatory coherence, with consequences for industry participants in terms of increased compliance costs. For consumers, increased complexity and regulatory fragmentation can make it more difficult to manage their communications experience. A single regulatory framework, or at least a joint approach, for addressing the changing dimensions of IoT activities would offer a more coherent arrangement for both businesses and consumers engaging in such activities.

Undoubtedly, much of the unease that surrounds the IoT stems from a lack of consumer understanding and awareness. A recent survey found that although mass adoption of connected technology is likely in the long term, the majority of consumers (87%) had not even heard of the term “The Internet of Things” (Aqurity Group, 2014). The study concluded that the highest barrier to mass adoption of the IoT was not so much price or concerns about privacy, but a lack of both awareness and value perception of the new ecosystem among consumers. This strongly suggests that improving customer experience in this area, and educating consumers about the key functional characteristics

(e.g. connectivity, interactivity, telepresence, intelligence, convenience and security) and benefits (e.g. personalised offers and cost savings) of connected technologies, should be a high priority in building consumer trust and stimulating demand for the IoT (YaPing et al., 2014). Moreover, in situations where a household will have tens or even hundreds of connected devices, overall systems for managing these devices will become essential. As IoT apps proliferate, and in the face of the growing potential complexity of the market, integrated consumer interfaces will be essential to ensure that the desired simplicity of the IoT is maintained.

Box 6.7. NFC regulation in Australia

The Australian Communications and Media Authority (ACMA) requires industry to develop codes and standards to ensure that consumer protection is maintained in the telecommunications industry, and in a range of different areas, including privacy, maintenance of service standards and appropriate redress measures.

The ACMA, in its role as spectrum regulator, is responsible for planning and managing radio frequency spectrum as a public resource. Growth in the take-up and use of NFC-enabled services will also need to be accommodated in future spectrum demand planning and the management of spectrum interference.

The ACMA further provides consumer protection by requiring active devices, such as readers at a cash register or a mobile phone with an NFC chip, to meet relevant electromagnetic compatibility and emissions standards.

The Australian Securities and Investments Commission (ASIC) administers the e-Payments Code and related measures under the Corporations Act 2001. These regulate electronic payments, including internet/online payments and mobile banking.

The Australian Competition and Consumer Commission (ACCC), along with state and territory fair-trading agencies, enforce Australian consumer legislation, and provide consumer with guarantees for faulty NFC transactions in cases where consumers were incorrectly charged by a merchant or the contactless payment terminal was not operating properly.

The Attorney-General's Department, supported by the Office of the Australian Information Commissioner (OAIC), administers the Privacy Act 1988, which outlines National Privacy Principles (NPPs). Organisations that facilitate NFC transactions need to comply with the Privacy Act regarding the information they hold.

Source: ACMA (2013).

6.4 Autonomous machines and public policy

The IoT will affect remote-controlled machines, machine learning and autonomous machines. The economic implications and the implications on sectoral regulations could be a topic for future research. Some of the main implications are related to employment and to the growth of autonomous machines. Furthermore, current regulations especially in transport assume human control of vehicles, which is not the case with remote-controlled and autonomous vehicles. At present, there is therefore an absence of regulation that explicitly allows the use of remote-controlled and autonomous machines and/or regulates their use.

Policy implications of autonomous machines on employment and growth

A question that arises around the IoT is its implications for employment. Brynjolffson and McAfee (2011) mention in their book *Race against the Machine* a possible future, where machine learning allows robots to replace humans in many “lower skilled” jobs. Their book aimed to bring technology into the discussion on unemployment and the global financial recession. The “End of Work”, as this hypothesis is known, after a book by Jeremy Rifkin, has been proposed by many economists, but has received only minor attention as technological changes have generally been accompanied by increases in employment in other parts of the economy, such as the services economy and the IT industry. To many economists, the proposition is therefore also known as the Luddite fallacy (Economist, 2011). John Maynard Keynes used a different term as early as 1930, stating:

We are being afflicted with a new disease of which some readers may not yet have heard the name, but of which they will hear a great deal in the years to come—namely, technological unemployment. This means unemployment due to our discovery of means of economising the use of labour outrunning the pace at which we can find new uses for labour. But this is only a temporary phase of maladjustment (Keynes, 1930).

Economist Alex Tabarrok’s summary of the concept states that “[i]f the Luddite fallacy were true, we would all be out of work because productivity has been increasing for two centuries” (Tabarrok, 2003). Robert Gordon states:

In setting out the case for pessimism, I have been accused by some of a failure of imagination. New inventions always introduce new modes of growth, and history provides many examples of doubters who questioned future benefits. But I am not forecasting an end to innovation, just a decline in the usefulness of future inventions in comparison with the great inventions of the past (Gordon, 2012).

This last statement evokes a general pessimism regarding the extent to which much new technology can add to the growth of the economy.

While there are different views on the implications of technological change for employment, the IoT promises to increase their scale and reach. Brynjolffson and McAfee point to the introduction of mechanisation at the start of the twentieth century, which led to an almost complete replacement of the use of horses in only two decades. In many ways, the world is today at the dawn of machine learning, similar to its position in 1994 with respect to the Internet. Practical commercial examples are now available, but much is still to be learned. Technology has moved quickly and the integration of low-cost electronics, large-scale processing power and ubiquitous networking has made possible new generations of autonomous and semi-autonomous machines. These machines are moving into every part of the economy and are displacing work in various sectors. This could theoretically lead to workerless factories. Even if it causes only temporary friction problems in the economy, as Keynes once suggested, it is a development that policy makers need to consider. Machine learning is as much about the competitiveness of the economy as it is about labour policy.

The competitiveness of the market of an economy is dependent upon having the most efficient tools and processes. It is, therefore, likely that countries that invest more in the development of machine learning and autonomous systems will benefit to a greater extent from them. Whether this will lead to economic growth and/or influence jobs is food for debate among economists. What is likely, however, is that if robotic warehouses perform as well as argued by those responsible for their implementation, then jobs in the warehouse sector will decrease and companies will compete to build more efficient warehouses. This

will lead to greater efficiency, which in turn lead will lead to greater purchasing power for consumers. It could also lead to job loss and friction problems in the economy that cost society economic growth. That the market is moving in this direction is exemplified by Wehkamp.nl, a Dutch online retailer, which announced in October 2013 that it would build the world's largest robotic distribution centre to replace its traditional warehouse. This centre will permit order-to-package times of 30 minutes and same-day delivery, which customers will likely appreciate.²⁹ Robots will manage the warehouse, pick goods, and move to and from picking stations, where employees will pick and pack the goods.

In the area of manufacturing, robots will likely replace many labour intensive tasks that are presently too difficult or too expensive to execute by robot. For policy makers keen to repatriate manufacturing to their countries from low-cost labour countries, the resultant effect might not produce the number of jobs traditionally associated with the sector. For the least developed economies, the traditional development path from assembly of low-cost clothing and goods, via low-cost electronics, to high tech will be cut off because the assembly of higher value goods will be performed in developed countries by robots.

Many other "routine" jobs may also disappear in the coming years. If autonomous vehicles are a success, then autonomous taxis, buses and trucks would be likely candidates. Some jobs that in the past absorbed unskilled or low-skilled workers may no longer exist. Jobs will still be associated with providing these functions; however, many of them will require higher skills, for example, repair and programming of robotic functions. Having a skilled labour force is therefore crucial. On the other hand, there are also cost savings associated with autonomous machines, which may allow re-employment of people in other parts of the economy.

Autonomous machines, whether in transport or manufacturing, are dependent upon reliable infrastructures. Autonomous technologies can only provide their full benefits when countries have dependable transport, energy and communications networks. The vision of an entirely robotic production process can only exist if each element fits well with the next, because despite its increased flexibility, machine learning will not have the ability to deal with adversity. For example, a human factory worker may be able to reorganise some of the work in the event of an electricity failure. Similarly, failing communications systems may be detrimental to the functioning of autonomous taxis, which might not be able to find new passengers, but a human driver will still be able to identify a waiting passenger. Therefore, a well-functioning infrastructure will be essential.

Policy implications of autonomous machines for regulation

Autonomous and remote-controlled machines are used mainly in controlled environments at present. However, they will form a major part of the IoT. Regulation in controlled environments consists mostly of adequate health and safety measures, which often translates into a switch that turns the robot off when an employee enters the operations area. This will change with the newest generation of autonomous machines, where humans and machines will interact and co-operate. The legal context of these machines will as a result change, dramatically.

A number of countries and companies are actively testing driverless cars on public roads. Google in the United States is the best-known example, but every major car manufacturer has a prototype programme that deals with autonomous vehicles. For the near future, companies are focusing on near-autonomous vehicles. The first applications can be found in driver assisted systems, some of which are already available, for example,

to allow autonomous driving in low-speed traffic jam environments or to allow automatic parking. These applications will expand over time to allow automatic cruising on highways. Some automobile manufacturers, however, expect to bring near or fully autonomous vehicles on the market between 2017 and 2020.

The legality of use of automated vehicles, be they airborne or on the road, is much more complex. Existing international treaties, as well as national and local regulations, were not written with autonomous or remote-controlled vehicles in mind. International treaties to which the majority of OECD countries are signatories include the 1949 Geneva Convention on Road Traffic and the 1968 Vienna Convention on Road Traffic. These require a driver to be present. Some countries disagree on the definition of “driver” and on whether an automated function would fit the treaty definition.

Stanford University’s Cyber Law Center assumes that as long as a human operator can take over control, the treaties do not prohibit automated vehicles (Smith, 2012). “Possibly the condition is also satisfied if that vehicle operates within the bounds of human judgment. These interpretations may not require a human to be physically present” (Smith, 2012). It is therefore important that the definitions be clarified or modified for autonomous vehicles to become a possibility in all signatory countries.

In the United States, some states including California, Florida and Nevada have now enacted legislation that allows the use of autonomous vehicles. These laws do not resolve all legal issues surrounding their use, but they do explicitly recognise the existence of autonomous vehicles and authorise their use in the state. According to the analysis of Stanford University, areas that will require attention include: vehicle standards, general tort liability, insurance, data collection, transportation planning and environmental impact assessment.

The United Kingdom held a consultation in 2014, with a first trial to be conducted in 2015 in Greenwich. The government plans to publish a Code of Practice in early 2015 for those who want to test driverless vehicles on the roads of the United Kingdom. Officials have said that they want “a light touch/non-regulatory approach” to testing self-driving cars in order to get such automobiles on the road faster. “A Code of Practice will be quicker to establish, more flexible and less onerous for those wishing to engage in testing than the regulatory approach being followed in other countries” (Mlot, 2015). In the Netherlands, the government has stated that it wants to become a testbed for the use of autonomous vehicles and has approved their use on the road. In Korea, however, despite research at national research institutes, the Road Traffic Act requires a driver to be present in the vehicle.

(Light) unmanned remote-piloted aircraft systems (RPAS), also known as Unmanned Aerial Vehicles (UAV) or drones, are allowed in some OECD countries. In Japan, for example, remote-controlled helicopters are used to spray 40% of the rice crop. A roadmap for RPAS prepared for the European Commission states that the Czech Republic, France, Ireland, Italy, Sweden, Switzerland and the United Kingdom currently have national rules and regulations in place. National regulations are also being prepared in Belgium, Denmark, the Netherlands, Norway and Spain (EC, 2013). In Korea, RPAS above 150 kilograms are forbidden, whereas those under 150 kilograms need to file 18 documents seven days prior to a flight. Only RPAS under 12 kilograms are exempt from these rules. In the United States, the FAA is working to produce regulations. However, at this moment commercial use of RPAS is restricted. Autonomous piloted aircraft systems are not yet part of the regulatory roadmap because the International Civil Aviation Authority is currently limiting itself to RPAS. RPAS are also used in many military applications and, as a result, are listed on the

export control list of Wassenaar Arrangement countries, to which many OECD countries adhere (category 9.A.12). This means that farmers in Australia cannot buy remote-controlled helicopters from Japan, but have to hire them as a service from the manufacturer, complete with a pilot. Future work could examine possible regulation of this sector in greater detail.

That regulation is necessary was demonstrated by an incident in Sweden, where all traffic to and from Stockholm's Bromma airport was halted because of a commercial, but unauthorised drone flight in the airport's control zone over central Stockholm.³⁰ The airport remained closed for an hour until the drone operator was located. In the United Kingdom, the pilot of an Airbus 320 on approach for a landing at Heathrow airport reported a drone passing 7 metres over the left wing. The Airbus was at that time 213 metres above the ground. An investigation was held, but the operator of the drone was not found. These are not the only episodes known to involve RPAS, but they serve as an indication of the seriousness of possible future incidents.

Notes

1. Merriam-Webster defines an actuator as "a mechanical device for moving or controlling something". While a sensor can be used to ascertain the state of a system, an actuator can be used to change that state.
2. For a list of milestones in the evolution of the blending of the physical with the digital, see Gil Press (2014).
3. For information on the cost of RFID readers, see: www.rfidjournal.com/site/faqs#Anchor-If-36680.
4. Decree 8234 of 2 May 2014, found at <http://leisonline.blogspot.fr/2014/05/decreto-n-8234-de-2-de-maio-de-2014.html#!/2014/05/decreto-n-8234-de-2-de-maio-de-2014.html> (accessed 15 April 2015).
5. For a further discussion of definitions of the Internet of things see Evans (2011). For a more academic evaluation of definitions, see Atzori, Iera and Morabito (2010).
6. This is not a fully accurate depiction of the changes machine learning is undergoing as a result of advances in Bayesian analysis and might be too negative of prior work in the field of machine learning. However, a discussion of the nuances involved would be too technical for the present report.
7. Similar predictions have been made by researchers and engineers of vehicle manufacturers in conversations with OECD staff.
8. Power-line communication carries data on a conductor that is also used simultaneously for AC electric power transmission or electric power distribution, while Power over Ethernet (PoE) passes electrical power along with data on ethernet cabling.
9. Transport for London, "What is a Contactless Payment card?", www.tfl.gov.uk/fares-and-payments/contactless/what-is-contactless?intcmp=8610 (accessed 15 April 2015).
10. A star network is a computer network topology which consists of one central switch, hub or computer, which acts as a conduit to transmit messages.
11. SITA's website is here: www.sita.aero/about-us.
12. 802.15.4 is a layer 2 protocol, which defines modulation, power output, frequencies used and a number of other elements necessary to make communication possible. Zigbee, Thread and 6LowPan are layer 3 and higher protocols that define how the network will organise itself, how addressing is done, how routing becomes possible and data is packaged. An 802.15.4 wireless device that uses one layer 3 protocol can make itself heard, but is not understood by devices that use a different layer 3 protocol.
13. The term "native" is used when the infrastructure supports IPv6 from the bottom up and each device receives an IPv6 address. Non-native use describes when there are translation mechanisms to move from IPv6 to another underlying protocol.
14. See http://en.wikipedia.org/wiki/IEEE_802.15.4.
15. Time periods can be brief lasting only seconds, or longer lasting minutes.

16. Energy network operators in the Netherlands manage the physical connections to the electricity and gas grid network. They are structurally separated network operators, who cannot generate electricity, sell retail services to end users or operate the national high voltage distribution grid.
17. The OECD has published a number of reports on IPv6. For an overview, see: www.oecd.org/sti/ieconomy/telecomandinternetreports.htm#Internet.
18. Cisco Visual Networking Index 2014 states: “The number of devices connected to IP networks will be nearly twice as high as the global population in 2018. There will be nearly three networked devices per capita by 2018, up from nearly two networked devices per capita in 2013. Accelerated in part by the increase in devices and the capabilities of those devices, IP traffic per capita will reach 17 GB per capita by 2018, up from 7 GB per capita in 2013” (Cisco, 2014). The UN estimates the world population to be 7.5 billion in 2018. The estimate from Cisco Internet Business Group is found in Evans (2011).
19. The calculation adjusts the initial estimate for a family of four to an average household size.
20. Mobile networks currently still require each SIM card to be assigned at least one e.164 telephone number. This may change in the future, but so many systems now expect a phone number for billing and management purposes, that moving to other types of numbers may take considerable time.
21. Carrier Grade Network Translation is the term used when the Network Address Translation (NAT) is performed at the core of the network instead of at the edge. Millions of devices may simultaneously share the same pool of addresses, requiring a much higher throughput and reliability than NAT in a home DSL router. Carrier Grade NAT is the only way to perform NAT in a mobile wireless network, because the network translation cannot easily be handled by devices at the edge.
22. Online posts regarding such concerns can be found at: www.medhelp.org/posts/Heart-Rhythm/Why-does-cardionet-event-monitor-record-when-nothing-is-wrong/show/1393291 and www.medhelp.org/posts/Heart-Rhythm/30--day-Cardionet-Monitor-going-off-by-itself/show/1089961.
23. Several countries have examined GPS-based road pricing, but so far have not moved forward. A lack of support from rule makers or complex demands, for example, by allowing pre-booking of slots and so forth, can create delays in their introduction. See, for example: <http://roadpricing.blogspot.nl/2011/08/uk-concludes-gps-based-distance-road.html>, http://en.wikipedia.org/wiki/Road_pricing and www.nce.co.uk/news/transport/government-collapse-scuppers-dutch-road-pricing-plans/5216811.article.
24. A leaflet entitled “The Smart Metering System”, published by the UK Department of Energy and Climate Change, can be found at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/336057/smart_metering_leaflet.pdf.
25. See <http://ec.europa.eu/digital-agenda/en/internet-things>.
26. See *Besluit van de Minister van Economische Zaken van 3 maart 2014, nr. ETM/TM/14024019, houdende wijziging van het Nummerplan voor identiteitsnummers ten behoeve van internationale mobiliteit (IMSI-nummers) in verband met het gebruik van IMSI-nummers door besloten netwerken* (in Dutch), <https://zoek.officielebekendmakingen.nl/stcrt-2014-6781.html>.
27. See www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm.
28. For more information, see the “7 Foundational Principles” on the Privacy by Design website, www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/.
29. A clip of the announcement and the new distribution centre can be seen at www.youtube.com/watch?v=Q5eie0IgccY (in Dutch).
30. For the Heathrow incident the official Air Proximity report (no. 2014117) can be found at www.airproxboard.org.uk/docs/423/2014117.pdf. The Swedish incident was described in the press, for example, at Aircoc (2014).

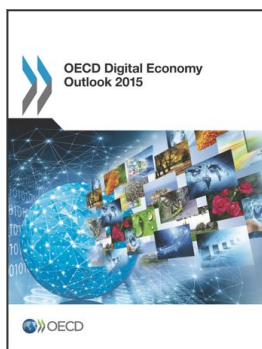
References

- ACMA (2013), *Near-field communications. Emerging Issues In Media and Communications*, Occasional Paper, No. 2. Australia Communications and Media Authority, Canberra, <http://165.191.2.87/~media/Regulatory%20Frameworks%20and%20International%20Coordination/Information/pdf/Near%20field%20communications%20Emerging%20issues%20in%20media%20and%20communications%20Occasional%20paper%202.pdf>.

- Airsoc (2014), "Airspace around Stockholm-Bromma briefly closed following drone sighting", Airsoc webpage, <http://airsoc.com/articles/view/id/5480fa8d31394477768b456a/airspace-around-stockholm-bromma-briefly-closed-following-drone-sighting> (accessed 15 April 2015).
- Alzheimer's Society (2014), *DementiaFriendly Technology: A Charter That Helps Every Person With Dementia Benefit From Technology That Meets Their Needs*, Alzheimer's Society, London, www.telecare.org.uk/sites/default/files/file-directory/Publications/Dementia%20Friendly%20Technology%20Charter.pdf.
- Aquity Group (2014), *The Internet of Things: The Future of Consumer Adoption*, www.aquitygroup.com/news-and-ideas/thought-leadership/article/detail/aquity-group-2014-internet-of-things-study (accessed 15 April 2015).
- Atzori, L., I. Antonio and G. Morabito (2010), "The Internet of Things: A survey", *Computer Networks*, Vol. 54/15, pp. 2787-2805, www.sciencedirect.com/science/article/pii/S1389128610001568.
- Baudoin, C. (2014), "The Internet of things: Automation heaven or security hell?", *Cutter Consortium website*, www.cutter.com/content/bia/fulltext/updates/2014/biau1403.html (accessed 15 April 2015).
- BIPT (2014), *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 (Consultation at the request of the board of BIPT of 25 November 2014 in relation to the policy review on the management of the numbering plan)*, Belgisch Instituut voor Postdiensten en Telecommunicatie, Brussels, www.bipt.be/public/files/nl/21394/Consult_review_KB_Nummering_NL.pdf.
- Brill, J. (2014), "The Internet of Things: Building trust to maximize consumer benefits", speech at The Internet of Things: Roundtable with FTC Commissioner Brill, Center for Policy on Emerging Technologies, Washington DC, 26 February 2014, www.ftc.gov/system/files/documents/public-statements/203011/140226cpetspeech.pdf.
- Brynjolfsson, E. and A. McAfee (2011), *Race Against the Machine*, Lexington, MA, Digital Frontier Press.
- BT (2014), *Promoting Investment and Innovation in the Internet of Things*. Ofcom Internet of Things Consultation – BT Response, British Telecom, London, <http://stakeholders.ofcom.org.uk/binaries/consultations/iot/responses/BT.pdf>.
- Capgemini (2014), "Internet of Things = Internet of trust", *Capping IT Off* blog, 19 September 2014, www.capgemini.com/blog/capping-it-off/2014/09/internet-of-things-internet-of-trust.
- Cisco (2014), *Cisco Visual Networking Index: Forecast and Methodology, 2013–2018*, Cisco Systems, Inc., www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html (accessed 15 April 2015).
- Co.Exist (2014), "7 tools that let you control your own data", *CoExist website*, www.fastcoexist.com/3024857/world-changing-ideas/7-tools-that-let-you-control-your-own-data (accessed 15 April 2015).
- Connected World (2014), *Two Views: Is It Too Soon to Move to 4G/LTE?* Aug/Sept 2014, <http://connectedworld.com/two-views-is-it-too-soon-to-move-to-4glte/> (accessed 15 April 2015).
- Das, R. and P. Harrop (2014), *RFID Forecasts, Players and Opportunities 2014-2024*, IDTechEx, www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2014-2024-000368.asp (accessed 15 April 2015).
- EC (2014), *Benchmarking Smart Metering Deployment in the EU-27 with a Focus on Electricity*, EC Report, No. COM(2014) 356 final, European Commission, Brussels, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0356&from=EN>.
- EC (2013), *Roadmap for the Integration of Civil Remotely-Piloted Aircraft Systems into the European Aviation System*, Final Report from the European RPAS Steering Group (ERSG), European Commission, Brussels, http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf.
- ECC (2014), *Evolution in the Use of E.212 Mobile Network Codes*, ECC Report, No. 212, CEPT Electronic Communications Committee, www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP212.PDF.
- Economist* (2011), "Difference engine: Luddite legacy", *The Economist*, 4 November 2011, www.economist.com/blogs/babbage/2011/11/artificial-intelligence (accessed 15 April 2015).
- Edge (2012), "Reinventing society in the wake of big data: a conversation with Alex (Sandy) Pentland", *Edge*, 30 August 2012, <http://edge.org/conversation/reinventing-society-in-the-wake-of-big-data> (accessed 15 April 2015).
- Evans, D. (2011), *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper, CISCO IBSG, www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

- GigaOm (2014), "Ericsson CEO predicts 50 billion Internet connected devices by 2020", GigaOm, 14 April 2014, <https://gigaom.com/2010/04/14/ericsson-sees-the-internet-of-things-by-2020/> (accessed 15 April 2015).
- GigaOm (2009), "Intel inside becomes Intel everywhere", GigaOm, 2 March 2009, <https://gigaom.com/2009/03/02/intel-inside-becomes-intel-everywhere/> (accessed 15 April 2015).
- Gil Press (2014), "A very short history of the Internet Of Things", *Forbes*, 18 June 2014, www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/ (accessed 15 April 2015).
- Gordon, R.J. (2012), "Why innovation won't save us", *Wall Street Journal*, 21 December 2012, <http://online.wsj.com/articles/SB10001424127887324461604578191781756437940> (accessed 15 April 2015).
- Harwell, D. (2014), "Whirlpool's 'Internet of Things' problem: No one really wants a 'smart' washing machine", *The Washington Post*, 28 October 2014, www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/whirlpools-internet-of-things-problem-no-one-really-wants-a-smart-washing-machine/ (accessed 15 April 2015).
- Hearn, A. (2014), "Sir Tim Berners-Lee speaks out on data ownership", *The Guardian*, 8 October 2014, www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership (accessed 15 April 2015).
- IEI (2014), *Utility-scale Smart Meter Deployments: Building Block of the Evolving Power Grid*, Institute for Electric Innovation, The Edison Foundation, Washington DC, www.edisonfoundation.net/iei/Documents/IEI_SmartMeterUpdate_0914.pdf.
- Keynes, J.M. (1963), "Economic possibilities for our grandchildren", *Essays in Persuasion*, W.W.Norton & Co., New York, pp. 358-373, www.econ.yale.edu/smith/econ116a/keynes1.pdf.
- KrebsonSecurity (2012), "FBI: Smart meter hacks likely to spread", *KrebsonSecurity*, 12 April 2012, <http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/> (accessed 15 April 2015).
- Kvalbein, A. (2012), *Measuring Mobile Broadband in Norway*, Simula Research Laboratory, RIPE 64, https://ripe64.ripe.net/presentations/172-Mobile_Broadband_Measurements.pdf.
- Lee, T.B. (2015), "5 reasons self-driving taxis are going to be amazing", *Vox*, 17 March 2015, www.vox.com/2015/3/17/8231401/self-driving-taxis-amazing (accessed 15 April 2015).
- Liebenau, J. et al. (2011), *Near Field Communications: Privacy, Regulation & Business Models*, A white paper of the LSE/Nokia research collaboration, www.lse.ac.uk/management/documents/LSE-White-Paper_-_Near-Field-Communications-Privacy-Regulation-Business-Models.pdf (accessed 15 April 2015).
- Kelly, S.M. (2014), "World's first connected tennis racquet will perfect your swing", *Mashable*, 7 January 2014, <http://mashable.com/2014/01/07/connected-tennis-racquet/> (accessed 15 April 2015).
- Ministry of Science, ICT and Planning (Republic of Korea) (2014), *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, Ministries of the Republic of Korea, Seoul, www.iotkorea.or.kr/2013_kor/uploadFiles/board/KOREA-%20IoT%28Internet%20of%20Things%29%20Master%20Plan%20-%202014.pdf.
- Mlot, S. (2015), "Driverless cars hitting U.K. roads this summer", *PC Magazine*, 11 February 2015, www.pcmag.com/article2/0,2817,2476609,00.asp (accessed 15 April 2015).
- OECD (2015), *Trust in a Data-Driven Economy: Data and Analytics: Prospects for Growth and Well-being*, OECD, Paris.
- OECD (2014), *Summary of the OECD Privacy Expert Roundtable on Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, OECD Publishing, Paris, [www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg\(2014\)3&doclanguage=en](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en) (accessed 15 April 2015).
- OECD (2013a), "Building blocks for smart networks", *OECD Digital Economy Papers*, No. 215, OECD Publishing, Paris. DOI: <http://dx.doi.org/10.1787/5k4dkhvnzv35-en>.
- OECD (2013b), "Cloud computing: The concept, impacts and the role of government policy", *OECD Digital Economy Papers*, No. 240, OECD Publishing, Paris, DOI: <http://dx.doi.org/10.1787/5jxzf4lcc7f5-en>.
- OECD (2013c), "Exploring data-driven innovation as a new source of growth: Mapping the policy issues raised by 'big data'", *OECD Digital Economy Papers*, No. 222, OECD Publishing, Paris, DOI: <http://dx.doi.org/10.1787/5k47zw3fcp43-en>.
- OECD (2012a), "Machine-to-machine communications: Connecting billions of devices", *OECD Digital Economy Papers*, No. 192, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5k9gsh2gp043-en>.

- OECD (2012b), "Terms of Reference for the Review of the OECD Guidelines for the Security of Information Systems and Networks", OECD Digital Economy Papers, No. 210, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5k8zq92zhqhl-en>.
- OECD (2010), *OECD Information Technology Outlook 2010*, OECD Publishing, Paris, http://dx.doi.org/10.1787/it_outlook-2010-en (accessed 15 April 2015).
- Ofcom (2014), *Promoting Investment and Innovation in the Internet of Things*, Ofcom, London, <http://stakeholders.ofcom.org.uk/consultations/iot/> (accessed 15 April 2015).
- Pasiewicz, M. "On people, the death of privacy, and data pollution", interview with Bruce Schneier, Schneier on Security, www.schneier.com/news/archives/2008/03/on_people_the_death.html (accessed 15 April 2015).
- Rauhofer, J. (2008), "Privacy is dead, get over it! Information privacy and the dream of a risk-free society", *Information & Communications Technology Law*, Vol. 17/3, www.tandfonline.com/doi/abs/10.1080/13600830802472990#.VDWAHUvgp5k (accessed 15 April 2015).
- Rubens, P. (2014), "Internet of Things a potential security disaster", *eSecurity Planet*, 4 September 2014, www.esecurityplanet.com/network-security/internet-of-things-a-potential-security-disaster.html (accessed 15 April 2015).
- Smith, B.W. (2012) "Automated vehicles are probably legal in the United States", *The Center for Internet and Society*, <http://cyberlaw.stanford.edu/publications/automated-vehicles-are-probably-legal-united-states> (accessed 15 April 2015).
- St. John, J. (2014), "4 ways Tokyo's smart meter plan breaks new ground", *Greentechgrid*, 19 March 2014, www.greentechmedia.com/articles/read/4-ways-tokyos-smart-meter-plans-break-new-ground (accessed 15 April 2015).
- Tabarrok, A. (2003), "Productivity and unemployment", *Marginal Revolution*, 31 December 2003, http://marginalrevolution.com/marginalrevolution/2003/12/productivity_an.html.
- US FTC (2014), *In the matter of TRENDDnet*. Docket no. C-4426. Decision and Order. United States Federal Trade Commission, Washington DC, www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.
- WEF (2014), *Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems*, World Economic Forum, Geneva, www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.
- Weiser, M. (1991), "The computer for the 21st century", *Scientific American*, Vol. 265/9, pp. 66–75.
- Wilson, J. (2008), *Sensor Technology Handbook*, Newnes/Elsevier, Oxford.
- Wolf, C. and J. Polonetsky (2013), "An Updated Privacy Paradigm for the 'Internet of Things'", *Future of Privacy Forum*, 19 November 2013, www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.
- YaPing, C. et al. (2014), "Influence of characteristics of the Internet of Things on consumer purchase intention", *Social Behavior and Personality*, Vol. 42/2: 321-330.
- Yared, P. (2013), "2013: The Internet of things, delivered via smartphone", *VentureBeat*, 2 January 2013, <http://venturebeat.com/2013/01/02/internet-of-things-via-smartphone/> (accessed 15 April 2015).



From:
OECD Digital Economy Outlook 2015

Access the complete publication at:
<https://doi.org/10.1787/9789264232440-en>

Please cite this chapter as:

OECD (2015), "Emerging issues: The Internet of Things", in *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/9789264232440-8-en>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.