Briefing

May 2015

European Parliament

The Internet of Things

Opportunities and challenges

SUMMARY

The Internet of Things (IoT) refers to a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers. The data these devices report can be collected and analysed in order to reveal insights and suggest actions that will produce cost savings, increase efficiency or improve products and services. The IoT is growing rapidly, with an estimated 25 billion connected objects throughout the world by 2020, and added value from the IoT of US$1.9 trillion by the same year. The IoT can thus be a key contributor to achieving the EU's Europe 2020 strategy for smart, sustainable and inclusive growth.

However the IoT also poses important challenges to society. Open standards and interoperability may need to be encouraged, in order to widen choices for consumers and ensure competition and innovation. Sufficient radio spectrum must be allocated for future needs. With so many interconnected devices, security is a major concern. A balance needs to be achieved between the rights of citizens to keep personal data private and protected, and to consent to its use in other contexts, and the significant benefits that can accrue to enterprises and society from the analysis of such rich data sources.

The European Union is supporting the development of the IoT through funding for research as well as competitiveness and innovation. While EU institutions have taken a notable interest in the IoT, the balance between too much and too little regulation may need to be carefully managed if the full benefits of the IoT are to be realised.

In this briefing:

EPRS | European Parliamentary Research Service

Author: Ron Davies

Members' Research Service

PE 557.012

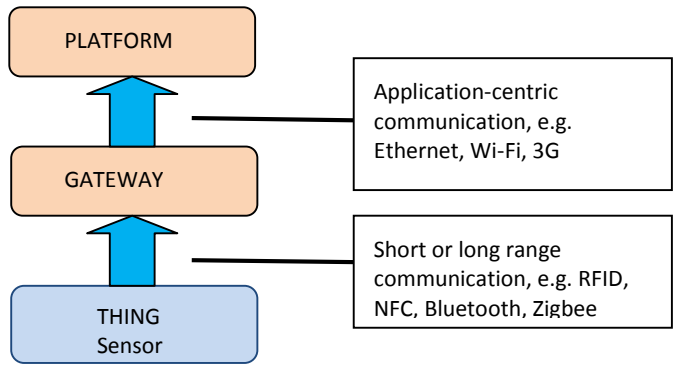
EN

What is the Internet of Things?

The Internet of Things (IoT) has been defined in a number of different ways. Generally speaking, it refers to a global, distributed network (or networks) of physical objects that are capable of sensing or acting on their environment, and able to communicate with each other, other machines or computers. Such 'smart' objects come in a wide range of sizes and capacities, including simple objects with embedded sensors, household appliances, industrial robots, cars, trains, and wearable objects such as watches, bracelets or shirts. Their value lies in the vast quantities of data they can capture and their capacity for communication, supporting real-time control or data analysis that reveals new insights and prompts new actions.

As in the case of many emerging technologies, different experts may use different terms to refer to similar or overlapping concepts. *Machine to machine (M2M)* processing emphasises the sharing of data and processing that takes place between these devices. On the other hand, the *Internet of Everything* explicitly includes people as participants in this global network. *Ubiquitous computing* emphasises the fact that network and computing resources are available almost everywhere, whereas *pervasive computing* highlights the fact that processors are embedded in everyday objects all around us.

Figure 1 – IoT landscape



Adapted from: Leveraging enterprise architecture to enable business value with IoT innovations today / M. Walker, Gartner Group, 2014.

The application of the IoT to different sectors also gives rise to specific terms. *Smart homes* or *smart buildings* refer to IoT concepts applied to the management and control of buildings including heating, cooling, lighting, entertainment devices, security systems and household appliances. *Smart cities* typically use networks of sensors and computers to maximise the efficiency of traffic, public transport, street lighting or other city infrastructure. IoT networking in an industrial setting (including service industries like the hospital sector) may be referred to as the *Industrial Internet of Things (IIoT)* or described as the architecture underlying *Industry 4.0*, the imminent (fourth) industrial revolution.

Connecting physical devices to the Internet is not a new idea.[1] However the rapidly falling cost of sensor and Radio Frequency Identification (RFID) technology and the greater coverage and availability of wireless and mobile networks (including Wi-Fi and 2G/3G/4G mobile networks) have opened up new opportunities.[2] Version 6 of the Internet Protocol (IPv6) supports sufficient IP addresses to allow theoretically for 3.4 x 10^{38} internet-connected devices. Moreover, the internet-accessible Cloud now provides an easily accessible, low-cost platform for storing and processing data collected, while Big Data tools support the analysis of vast amounts of data. The promise of future social and economic benefits that these developments could offer is stoking current interest in the IoT.

The future impact of the IoT

While estimates vary, ICT consulting firms and other experts foresee exponential growth in the IoT over the next few years. According to the Gartner Group, worldwide by 2020, the IoT will connect 26 billion devices;[3] IoT product and service suppliers will generate incremental revenues of more than US$300 billion; and the IoT will result in US$1.9 trillion in added value through sales in diverse markets. Market research firm IDC is even more optimistic, estimating that the worldwide IoT market will grow from US$1.9 trillion in 2013 to US$7.1 trillion by 2020. A 2015 Verizon report predicts the IoT will quadruple by 2020 to an estimated 5.4 billion business-to-business (B2B) connections, concentrated particularly in the automobile and health/fitness sectors.

This rapid growth is based on expectations that the IoT will bring tangible benefits to European businesses and consumers. In a 2012 consultation of citizens and organisations by the European Commission, three out of four respondents said they expected benefits from IoT applications; more than four out of five experts canvassed by the Pew Research Center in 2014 said that the IoT would have widespread, beneficial effects by 2025. Those benefits can take different forms for citizens, for businesses and for governments.

Consumers can get more personal product or service offers, based on what they actually do or where they are. They can travel more efficiently by avoiding traffic jams when their connected car suggests an alternative route, based on traffic reported by other vehicles. They can save money by reducing energy usage or by paying lower car insurance premiums based on verified safe driving practices. They can be healthier, safer and more independent due to wearable devices that provide feedback on health or that monitor the elderly in the home.

Health, home care and the IoT

With an ageing population and rising health and long-term care costs, the IoT can help to improve care and reduce costs through eHealth services. Sensors placed in the home or in clothing can monitor vital signs and activity levels of older people. Families or caregivers can be alerted if problems arise. Recovering patients can be discharged earlier from hospital, or people with chronic disease can avoid hospital stays, if they can be monitored remotely in their homes.

Wearable devices can also play a part in preventing health problems, by tracking heart rate or blood pressure or encouraging healthy activity. Pilot studies have shown that bracelets or watches that measure activity can increase the participation rate and improve the effectiveness of fitness programmes for overweight people.

Businesses can provide better products and services by studying how customers behave; they can also discover needs for new products or services. They can protect buildings via remote security; secure assets like cars and machinery with location trackers and remote locking devices; and ensure that sensitive products (e.g. pharmaceuticals) are consistently stored in correct conditions. They can become more efficient, as in the case of utilities using smart meters to eliminate waste or loss, or in the case of equipment sellers providing just-in-time preventive maintenance. Farmers can be more productive with smart irrigation that provides water just where and when needed. New business models based on selling final outcomes rather than just equipment (so-called 'servitisation') may boost business revenues. Verizon estimates that by 2025, organisations that have fully embraced IoT will be 10% more profitable than competitors that have not; Germany's National Academy of Science and Engineering (acatech) estimates that firms could increase productivity by 30% by implementing Industry 4.0.

Governments and public authorities can also benefit from the IoT. For example, health and long-term care costs can be reduced with better remote support for the elderly in

their own homes. Road safety can be improved based on data from thousands of drivers. The efficiency of street lighting can be improved by dimming lights on empty roads.

Of course, benefits for consumers, businesses and governments may arise at the same time from a single IoT implementation. For example, smart meters that report detailed data on electricity usage via the Internet can save customers the inconvenience of a home visit by a meter reader, give them the means to monitor (and reduce) consumption, and allow them to profit from lower rates at off-peak hours. At the same time, the electrical utility will save on meter-reading costs and can use aggregated usage data to plan better for future demand. Governments and society as a whole can benefit from reduced energy dependency and fewer negative environmental effects.

However some observers think these scenarios may be overly optimistic. The Gartner Group positioned IoT at the 'peak of inflated expectations' in its 2014 hype cycle of emerging technology, suggesting that the IoT was still 5 to 10 years from the point where the technology would clearly be paying off in broad markets. Sceptics argue that no one has yet come up with a genuinely exciting application for the smart home, and worry about the loss of jobs that might result from greater efficiencies.[4] A 2014 survey of IT executives found 49% considered the IoT to be 'over-hyped', very largely because too much is unknown. Other experts predict that the IoT will only result in niche or special purpose applications, without much effect on everyday life.

Certainly there appears to be some way to go before the IoT is widely implemented: as of 2014 in the EU28 only 10% of enterprises were using RFID technology, and less than a third of these (3% of the total) were using the technology in production and service delivery. Moreover there are significant challenges to the implementation of the IoT that must be resolved before citizens, enterprises and governments can fully profit from the benefits that this new technology can offer.

Smart parking

Smart parking platforms use low-power wireless sensors to detect the presence of cars in individual parking spaces. Drivers looking for a place can use a free smartphone app to see real-time availability of spots, as well as information on pricing, time limits and payment methods. Studies suggest that as much as 30% of driving time in large city centres is used in looking for a parking place, so not only do consumers benefit in terms of time and petrol used, cities suffer less pollution and traffic congestion, and can adjust parking prices in response to patterns of demand. American company Streetline has partnered with European organisations to bring this technology to cities like Braunschweig (Germany) and Manchester (UK).

Challenges in developing the IoT

Standards and interoperability

Standards are important in creating markets for new technologies. If devices from different manufacturers do not use the same standards, interoperability will be more difficult, requiring extra gateways to translate from one standard to another. In addition, a company that controls different parts of a vertical market (e.g. the acquisition of data, its integration with other data streams, and the use of those data streams to come up with innovative solutions or to provide services) may dominate a market, stifling competition and creating barriers for smaller players and entrepreneurs. Differing data standards can also tend to lock consumers into one family of products: if consumers cannot easily transfer their data when they replace one device with another from a different manufacturer, they will in effect lose any benefit from the data they have been accumulating over time. The European Commission has highlighted the need to develop technological standards to support the IoT.

However much of the current development of the IoT is taking place in vertical markets, where specific technological approaches to network transmission and topology may be adopted (e.g. centralised models where each device connects directly to the internet, or decentralised models where objects that are physically close can discover each other and exchange information directly). Public authorities have a role to play in promoting standards and interoperability in terms of data formats, transmission networks and security mechanisms, by fostering cross-industry consortia and groups to develop, encouraging consensus on standards with other governments and global standards bodies, and commissioning projects that mandate certain standards. At least four major industry consortia are working to define standards for IoT.[5] The European Telecommunications Standards Institute (ETSI) is working to establishing standards for M2M communications over mobile cellular-based networks. On the other hand, a group of Internet, business and telecom organisations, including the European Telecommunications Operators' Association (ETNO), argues that EU policies should be technologically neutral so as not to slow down European innovation and competitiveness.

Smart elevators

ThyssenKrup is using an Internet of Things approach to increase the safety and reliability of their elevators while reducing maintenance costs. Each elevator has thousands of sensors that capture operational data including lift speed, distance travelled, motor temperature and alignment. These data are transmitted to the Cloud, where 'intelligent' software sorts, analyses and visualises the vast amount of data collected for the use of personnel in remote service centres. Signs of problems *before* a lift fails will trigger remote diagnostic testing or a site visit by a technician who can visualise data on a laptop to determine the exact cause and perform preventive maintenance.

Radio spectrum

The anticipated growth in the number of wireless devices will require more radio spectrum. However the type of use to which spectrum should be allocated depends on the largely unknown extent to which different technologies such as mobile wireless (using licensed spectrum) or Wi-Fi (using unlicensed spectrum) will be employed in the IoT. To take advantage of economies of scale in the manufacture of devices, spectrum allocation should be harmonised, not just within Europe, but also across the globe. What makes spectrum decisions even more challenging is that IoT devices tend to have a long lifetime (around 30 years) as opposed to the much shorter average lifespan of mobile telephones (5 to 7 years). For example, operators in Europe may have problems in the future in shutting down 2G wireless support since that would render obsolete smart meters that currently use that technology.

Security

The IoT presents a number of security risks to both consumers and to businesses. Cybercriminals could get unauthorised access to devices or intercept local wireless communications in order to capture sensitive data. They may also attack servers or Cloud-based servers where the large quantities of aggregated data make an attractive target. Malicious hackers could take control of local networks or devices to cause harm, e.g. by sending out spam, bringing down a factory or power grid, disrupting the normal functioning of a personal health device or causing a connected car to react in a way that leads to a crash.

Encrypting data can help to reduce security risks, but many of the sensor devices currently on the market lack the battery or computing capacity to implement sophisticated encryption techniques. While there is currently no perfect solution, IoT companies can minimise security risks by taking security issues into account during the

design of their products; collecting only essential data; implementing multiple layers of defence against threats; building in access controls to limit access to their device; and (where possible) updating software regularly to patch vulnerabilities.

Privacy and data protection

IoT consumer devices often collect private and personal data, whether information on the users' location, their daily habits or the condition of their health. Data may be transmitted to central servers, or shared with other devices or third parties, without the opportunity for the user to review that data. Many devices such as wearable bracelets lack large displays or touchscreens, making it difficult to provide information to the consumer about possible uses and get user consent. Consent is needed not just to collect data but also to analyse or share it with third parties.

Businesses can minimise problems by collecting only information that is required for an immediate purpose. However this limits the data's usefulness since part of the benefit can only be realised by combining one set of data with others or through analysing very large quantities of data to establish patterns or trends. These benefits can accrue to society at large as well as for a particular device manufacturer or third parties: for example, data on driving patterns can be used to improve road safety. The ultimate consumer choice is, of course, not to interact with the device at all, or for the consumer to exercise a so-called 'right to chip silence'. However in many cases, this will mean that the consumer cannot benefit from much of the functionality of the device.

Moreover, making data anonymous as early as possible in the data transmission and processing chain can help to reduce risks. However, again, not all IoT devices will have the processing capabilities to do so and data may be so comprehensive that rendering it completely anonymous may be technically difficult or impossible.

Agriculture and the IoT

The IoT can help farmers to reduce waste and improve productivity. For example, studies show as much as 60% of irrigation water is wasted. A smart irrigation system can collect data on soil conditions and plant needs, so as to selectively water different plots of land. 14 European pilot sites for the Waterbee system demonstrated a 40% reduction in water use. Data can also be combined with weather forecasts to hold off irrigation if rain is imminent.

Smart farms can also benefit from other kinds of intelligent objects. 'Smart' bins and silos can report on the levels of grain and other feedstuffs they contain to simplify management and avoid risky physical checks. These devices can also send alerts when temperatures in the containers rise to levels that might damage or degrade their contents.

An informal consultation by the Juncker Commission on what the Digital Single Market (DSM) means for stakeholders came to the general conclusion that internet users feel reasonably protected and that privacy is a problem only when data are used out of context (e.g. data on driving patterns from a connected car, to evaluate personality types and then used in making decisions on hiring employees). On the other hand, 72% of Internet users in Europe already say they are worried that they are being asked for too much personal data online.

The EU and the Internet of Things

Research and innovation

The EU has funded IoT research, notably through the European Research Cluster on the Internet of Things and other projects under the Seventh Research Framework Programme. The successor Horizon 2020 research programme has an objective (ICT 30) on the IoT and platforms for connected smart objects in order to bring together different ICT technologies to develop platforms. A 2015 call aims to develop

architecture and concepts for interoperability, as well as fund large IoT reference implementations in areas such as smart homes, health and energy. Other Horizon 2020 areas of research, including low-power computing, smart cyber-physical systems[6] and process chain optimisation will also contribute to IoT development. The Commission will also finance large-scale pilot projects using the IoT, particularly with the goal of encouraging the use of open systems and platforms. The IoT European Research Cluster (IERC) organises Internet of Things Weeks (the fifth takes place on 16-18 June 2015 in Lisbon) as a forum for discussing large-scale IoT deployments.

Individual Member States are also investing in IoT. In March 2015, the UK government committed £40 million (€54.5 million) to IoT research in addition to the £73 million allocated in previous years. As part of its High-tech Strategy 2020 Action Plan, Germany has earmarked up to €200 million for an Industrie 4.0 'future project' intended to help the country become a leader in innovative, internet-based manufacturing, automation and embedded systems. And France is financing embedded software and connected object projects from a €50 million fund for digital development.

EU Institutions and bodies

In 2009, the European Commission issued a Communication on the Internet of Things COM(2009)0278 that highlighted the deep societal changes being introduced by the IoT, as well as the potential for economic growth and improvement in well-being for individuals as well as society. The Commission promised a limited range of actions, including stimulating discussion, monitoring developments, and funding research and innovation projects. The European Parliament's response was cautious, emphasising the large number of potential problems that the technology posed (particularly in the use of consumer devices) including privacy, data protection, data ownership, 'the right to chip silence' and social inclusion. However in 2011 the EP noted the need to ensure spectrum allocation for the IoT's wireless communication needs and to address the IoT in the Commission's 2012 Work Programme.

From 2010 to 2012, the Commission convened an Internet of Things Expert Group that reported on a number of different aspects. More recently in 2014, the Article 29 Working Party issued opinion 8/2014 on recent developments on the IoT, calling for the highest possible guarantees for individuals, at least in terms of wearable devices or personal measurement devices and 'smart home' devices. While acknowledging the problems that the IoT poses, the Working Party argued that users must remain in complete control of their personal data throughout the life cycle, and consent should be fully informed and specific in terms of exactly what would be measured and how the data would be used. In its 2015 Digital Single Market strategy, the Commission described the IoT as a technology 'central to the EU's competitiveness'.

Outlook

The potential of the IoT appears to be great, despite the range of issues that need to be addressed. A critical question for policy-makers is what role they should play in the process. After a 2013 consultation with industry participants, academics and individual citizens, the European Commission concluded that there was no consensus on the need for public intervention in the terms of IoT governance or on the scope that such an intervention could take. Industry participants in particular emphasised that inappropriate action early in the development of the IoT could stifle investment and innovation. (This echoes the January 2015 conclusion of US Federal Trade Commission

staff that specific legislation would be premature, and self-regulatory programmes for individual industries should be preferred.)

On the other hand, many individuals and civil society organisations believe that economic considerations are secondary when it comes to fundamental rights such as privacy and security. IoT concerns will arise as the Commission advances its plans for the Digital Single Market, including areas such as smart industrial systems ('Industry 4.0'); the ownership and data protection of Big Data; and e-services, including e-health.

Main references

Industrial Internet of Things: unleashing the potential of connected products and services / World Economic Forum, Accenture, 2015.

Internet of Things: privacy and security in a connected world / US Federal Trade Commission, Staff report, 2015.

Regulating the Internet of Things: first steps toward managing discrimination, privacy, security and consent / S. Peppet, Texas Law Review, v. 93, n.1, p.85-176, 2014.

Internet of Things : From research and innovation to market deployment / O. Vermesan, P. Friess, River, 2014.

Internet of Things (IoT): a vision, architectural elements and future directions / A. Gubbi et al., Technical report CLOUDS-TR-2012-2, University of Melbourne, 2012.

Internet of Things: a new avenue of research / P.-J. Benghozi et al. (ed.) Communications & strategies: Digiworld economic journal, no. 87, 2012. Special issue.

Europe's policy options for a dynamic and trustworthy development of the Internet of Things / H. Schindler et al., Rand Europe, 2012.

Endnotes

[1] For test or demonstration purposes, research and university labs have been connecting toasters, vending and coffee machines to the Internet for at least 25 years.

[2] Nevertheless, some observers believe that a wireless solution that meets all the requirements of IoT (extremely low cost, available everywhere, low power) has not yet been found. Others point out difficulties with existing technologies and business models, e.g. mobile telephone (SIM) cards are linked to the service provider, so that a company wanting to change provider would have the daunting task of physically changing cards in all of its devices.

[3] Networking equipment supplier Cisco puts the number even higher at 50 billion.

[4] See, for example, Useless cool / John Dvorak. PC magazine, January 2015. To IoT or not to IoT / Krzystof Plaza, FPInstruments, 2015; At CES 'Internet of Things' showcases the connected life / A. Chang, LA Times, March 23, 2015.

[5] The AllSeen Alliance, the Open Interconnect Consortium, Thread and the Industrial Internet Consortium.

[6] Systems in which physical and computing, network and physical processes are tightly integrated and interact extensively.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)