Enabling the information society

Internet of Things

Definition: The Internet of Things (IoT) - Everyday objects increasingly contain embedded technology (e.g. sensors) to communicate, sense and interact with the environment in which they are placed, with humans, and with remote information systems. As more information is produced these objects will interact between themselves with the aim to improve the quality of human life. An example - Your car detects from a tyre sensor that the tread depth will be illegal in around 200 miles and will need replacing in one week's time based on your driving habits in the last seven days. The car interacts with a system that you have permitted to interact with it, and automatically books an appointment at the local service centre and orders the exact tyre required from the supplier offering the best price.

Background: There should be no doubt that the IoT is already here, though the public and many organisations do not yet have visibility of current activity and future potential. The IoT has gradually emerged over the last 5 to 7 years in many industries, and will continue to grow exponentially in scope and scale. Falling costs are driving an inexorable rise in the number of distributed sensing and data collection devices, sometimes with compute capability, attached to more pervasive Internet communication channels, often mobile, as well as local and remote data storage and flexible power sources. Sensors now can work for years on a fraction of power historically required, and send data rapidly to anywhere in the world. This data can feed into real-time systems, dramatically increasing decision-making timeliness, feedback opportunities and service quality.

The IoT is a distributed system with no central architect, investor, grand master plan, one-off infrastructure build or over-arching technical architecture – it is the sum over time of personal, local, national and international installations across many industries and millions of locations, provided by many organisations, and touching all aspects of citizens daily lives, as well as the operations of public and private enterprises. Its great potential is to reduce costs, waste, response time and improve quality of life, energy consumption, market growth etc. through new pervasive services unimagined until the recent past other than in science fiction. IoT's very nature as a distributed system means it has the potential to lower the costs and complexity to enter IoT-enabled markets for SMEs as much as major corporations. These are all positive impacts of the increasingly sensed, connected environment.

Such potential connection of the environment – human:human, human:machine and machine:machine - brings with it though new challenges for citizens, regulators, investors, public sector and private industry. IoT is an aggregated system crossing many traditional silos – home, transport, workplace, urban design, wearable devices, education, health and care. Therefore the potential benefits have a counterpart in the consequences of high-speed pervasive data aggregation and analysis. These consequences will arise from:

- **Unintended**, perhaps even accidental data amalgamation. Two or more separate systems designed for simple, worthy purposes when combined have impact on security, privacy or process safety of individuals, businesses or governments;
- **Un-consented** data collection and amalgamation. The intentional combination of data sources, to which individuals or organisations never explicitly consented (or did not consent at all) could be analysed together, for marketing, surveillance, public safety and security;
- **Cyber-risk**. Lastly, as pervasive data collection and feedback systems develop, integrate and become relied upon to operate national or even personal infrastructure, the impact and risk of cyber-crime, cyber-terrorism and cyber-war will rise inevitably.

The power of the business case for each IoT element - driven by falling costs of sensors, computation, data storage, communication, globalisation of markets and economic growth – means that the IoT is here and will expand without intervention, incentive or infrastructural investment by government. The consequences of IoT, **unintended, unconsented and related to cyber-risk**, should therefore be a concern for regulators, investors, government and industry.

There are some key issues that need to be carefully managed:

Privacy: There has been undoubted concern in some quarters about the Internet's impact on privacy. So far this does not seem to have discouraged the bulk of consumers, public sector bodies and companies from engaging with it. But progress in delivering the benefits promised by IoT could be delayed if organisations and consumers lose confidence in data protection arrangements. IoT may magnify existing risks, as well as introducing new, often invisible sources of personal data and derived knowledge from combined data-sets. For example there will be many more devices streaming specific types of information, often without a user interface which may make setting permission more difficult.

These risks can be mitigated. Many companies in the sector are looking at how to improve the security arrangements around the collection and transmission of data to protect against hacking and to provide secure authentication of senders and recipients of data. Further, clear guidelines, and compliance indicators via traffic lights, could increase the transparency to consumers, and organisations, of what data is collected and why, and to what uses it could be put.

Data Management: Many companies collect data about us from e.g. supermarket loyalty cards. We have got accustomed to trusting how they use it. The ease of collecting data in the digital world, and the ability to analyse bulk data quickly has already given rise to a growth in the data industry, with data brokers active already in the US. Companies also collect significant amounts of data on other companies and their interactions – with similar consequences.

We need to increasingly focus onto how data is used (rather than simply collected). Up to a point consumers, and indeed organisations, both public and private, are probably content with data being used to offer them a wider range of goods and services. What worries them most is where the data is used to generate a conversation about them which may not be in their interests e.g. sharing health profiles with employers or insurance companies, financial data with mortgage lenders, making predictions about health from analysing shopping habits, predicting price changes based on commercial usage of commodities. The concerns are caused partly because the mitigation is often opaque – that in return for sharing data, services are improved, quality rises, and costs may reduce.

Security: The IoT will create new risks from cybercrime as the number of connected systems increases. There will be new orders of risk as these systems become more intimately associated with domestic life, the delivery of critical services and the management of infrastructure. An additional dimension of risks will arise from the unpredictable emergent behaviors of interactions between complex, distributed, extensive real-time systems which are themselves capable of taking decisions.

There are grounds for scepticism that the current technical security architectures will scale to a possible number of devices which is many orders of magnitude greater than at present. The costs of assurance, especially of heterogeneous networks, are at odds with both the envisaged scale of the IoT and the rate of new product introduction. The lack of agreed security standards is also a concern. Cryptography and associated key management will be essential, but the cost pressures on the designers of "things" will limit rigorous use and updates. We are already seeing smart devices which are designed with minimum security and with no method of updating what security they have over their lifetime.

BCS position on key issues – Unintended, un-consented use of data and increased, often cyber-risks:

A clear traffic light system might help overcome the problem that no one reads the current terms and conditions, where the uses of data collected are usually described; the traffic light system could be used to flag to people the non-obvious consequences of others using the data collected – as well as summarising the essential features of, or changes to, the agreement they have just made. The principles behind the traffic lights could also include an emphasis on the benefits data can bring, including, for instance, the use of anonymised data for a range of public health and other benefits.

More needs to be done to reassure consumers about the security arrangements for (i) protecting their data against hacking and (ii) ensuring their data is not wrongfully transferred to an unauthorised recipient. Such action needs to be co-ordinated across national boundaries – since the data and interactions themselves are frequently international.

An important aspect of this is informing consumers of the benefit they gain from agreeing to their data being used in various ways. We need a sensible debate about this, which ensures that consumer confidence is maintained without stifling the opportunity for innovation. Maybe this debate should be framed around some key principles that need further research; for instance there may be the need to provide consumers with a clear and succinct method of understanding how their data will be used (and the possibility to opt out).

There is a need for a data-handling framework that categorises different types of data and associated management strategies required to unlock the potential of IoT. This needs to bring together specific proposals on how to put these principles into practice. Its aim should be to reassure consumers while at the same liberating data to drive innovation.

In researching the principles it may helpful to distinguish between certain key uses of data. There may be two broad use scenarios:

(i) **Customer as target:** this is where the aim of assembling and analysing data about a customer is to offer them additional products or services.

In some cases these offers will be directly linked to an action a customer has taken (for instance researching specific products or entering into a specific contract). In other cases it may be the result of drawing inferences (e.g. about a consumer's life style based on various sources of information).

(ii) **Customer as topic:** this is where the primary aim of analysing data is to generate a 'conversation' about the customer.

The sorts of situations this includes are where, without your permission, your health data is sent to your insurer, or your employer, or your financial data goes to your Mortgage Company or employer etc. It also includes particularly sensitive situations where data is used to make sensitive 'predictions' about a consumer's health etc., or to categorise consumers in ways consumers may not approve.