Part of the conference series
Breakthrough science and technologies
Transforming our future

The Internet of Things: opportunities and threats

Conference report

THE ROYAL SOCIETY

Introduction

On 3 October 2017, the Royal Society hosted a conference on the subject of the Internet of Things (IoT). The conference brought together scientists, technologists and thought leaders from across academia, industry and government, to discuss the disruptive potential of the IoT and how the future of technology and society will be shaped by it.

Presentations and discussions outlined the ways in which the IoT may increase productivity and change lifestyles, and considered potential economic, security, ethical and legal implications. Furthermore, challenges to the wider translation and adoption of this technology were highlighted.

This conference is part of a series organised by the Royal Society, entitled *Breakthrough science and technologies: Transforming our future*, which addresses the major scientific and technical challenges of the next decade. Each conference focuses on one technology and covers key issues including the current state of the UK industry sector, the future direction of research and the wider social and economic implications.

The conference series is organised through the Royal Society's Science and Industry programme, which demonstrates our commitment to reintegrate science and industry at the Society, to promote science and its value, build relationships and foster translation.

This report is not a verbatim record, but a summary of the discussions that took place during the day and the key points raised. Comments and recommendations reflect the views and opinions of the speakers and not necessarily those of the Royal Society.

Full versions of the presentations can be found on our website at: **royalsociety.org/science-events-and-lectures/2017/10/tof-internet-of-things**

Executive summary

The internet of things (IoT) describes the billions of connected devices that exist in an increasingly networked society, pervading homes, workplaces, industries and cities. The opportunities afforded by this technology are huge, connecting humans to their environments and allowing analysis of the world at new levels of detail. Whilst these opportunities are significant, they are accompanied by risks to society and its infrastructure.

This meeting covered the topics of technology, security, business and economics, and social science, ethical, legal and global issues. Several key points arose during the presentations and panel sessions.

- Cyber-attacks on IoT devices are inevitable and the resilience of devices and networks must be carefully considered. Segregation of valuable network assets may be the best way to protect them from attacks.
- The legacy of devices is important when they are placed into environments for long periods. They must be resilient in terms of security, power supplies, software and hardware, but also remain interoperable with IoT devices of the future. Devices should be 'secure by default'.
- Society needs to reconsider legislation and regulation in a networked society to take account of the data generated by IoT devices and the power it gives to those that possess it. More transparency of who collects data and what it is used for should be provided to device users.
- Owners of IoT devices, the networks they are hosted on and the data they generate need to be accountable when problems occur, especially as artificial intelligence and machine learning becomes more commonplace.
- Device users should understand the choice they make when they consent to providing their data to service providers. Consent in this context should be reviewed, and awareness of the keys issues promoted.
- Industry is likely to drive for standards in the IoT faster than government can legislate. The public sector may drive the creation and adoption of standards through procurement policies.

Image: conference organisers (from left to right) Professor Dame Wendy Hall DBE FREng FRS, University of Southampton, Professor Jeremy Watson CBE FREng, University College London, Dr Jeremy Silver, Digital Catapult and Dr Patricia Lewis, Chatham House.

The Internet of Things: an introduction

The Internet of Things is comprised of 'smart' devices that use wireless technology to talk to one another and to users[1]. These connected devices offer smarter, more efficient experiences for users, impacting business, manufacturing, healthcare, retail, security and transport.

IoT products can be found in the home, the office, industry and across our cities, with numerous applications already realised (see figure 1 overleaf). In addition to a connection that allows them to communicate, these devices usually have digital sensors to collect relevant data and a processor to process the data.

As of 2015, the IoT was comprised of 15 billion devices and is set to grow to 30+ billion by 2020, equivalent to 3 smart objects for every human on Earth[2]. Though an IoT user's main interest is the data gathered, devices need to be designed so that they operate safely and securely for their intended lifetimes and purposes.

Collected data is used for a variety of purposes that can be either known or unknown to the user. For example, a wearable fitness monitor may provide real-time health data to the user, whilst the service provider simultaneously collects all its users' data, aggregates it, and monetises it. Data ownership and cybersecurity are two of the core issues at the heart of the IoT debate.

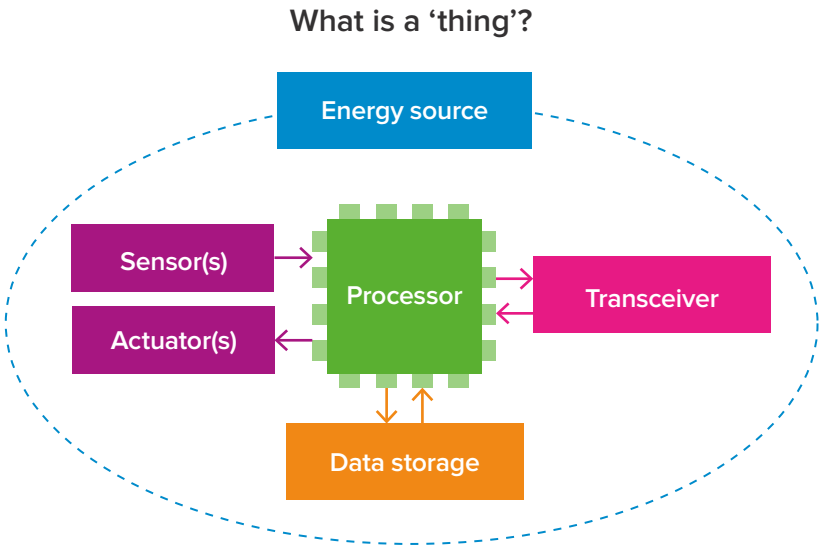
Image: conference attendees.

1 Centre for International Governance Innovation and Chatham House, 2017. Critical Infrastructure and the Internet of Things. See https://www.cigionline.org/publications/critical-infrastructure-and-internet-things-0 (accessed 20 October 2017).

2 IEEE spectrum, 2017. 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated'. See https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated (accessed 22 November 2017).

FIGURE 1

Key features of a typical IoT device. Common components include a transceiver to facilitate communication, a digital sensor and processor for collecting and processing data, and data storage space. The device must also be powered by an energy source.



Examples of IoT devices and where they can be found.

Humans
- wearable devices
- in-body devices
- health and wellness
- disease management

Offices
- energy management
- productivity
- mobile working

Homes
- home controllers
- security systems

Cities
- smart meters
- environment monitoring
- resource management
- infrastructure control

Retails
- self-checkouts
- inventory optimisation

Vehicles
- autonomous vehicles
- real-time routing
- traffic control
- maintenance

Industry
- operation efficiency
- equipment optimisation
- health and safety
- construction

Diagram reproduced with permission from Professor Bashir Al-Hashimi FREng, University of Southampton.

Technology: the basis of the Internet of Things

Device operation

An IoT device must be designed so that it can survive in the environment in which it is placed and in locations that users may not see or interact with, as pointed out by Professor Julie McCann, Imperial College London. Devices are often placed in our critical infrastructure, eg smart cities, distribution networks, farming operations, oil and gas networks and manufacturing plants, presenting challenges such as:

- the device must remain interoperable and be powered throughout its lifetime but problems such as battery drain, device damage, and unreliable connectivity can occur
- as the IoT grows, multiple devices will operate in the same dense spaces, causing issues with network availability
- devices may not be accessible beyond installation and maintenance will have to be done remotely.

Complications may arise from devices that function for much longer than intended. Professor Derek McAuley, The University of Nottingham, imagined a building designed with integrated IoT devices that, 50 years later, speaks an 'ancient language' that new devices cannot understand. As more IoT devices enter our environments, issues such as legacy will get more complicated. By tracking the devices released and where they go, these complications can be avoided.

Powering IoT devices

As Professor Bashir Al-Hashimi FREng, University of Southampton, described billions of batteries are required to operate the IoT, posing a significant environmental risk as many devices will not be correctly disposed of after use. Alternatively, he argued that for some applications, 'energy harvesting', which converts ambient energy sources (eg vibration, light and temperature) into electrical energy, can become the standard for new energy efficient devices. In recent years, such devices have been shown to operate just as well as their battery powered counterparts, and could be viable long-term alternatives.

Image: Professor Bashir Al-Hashimi FREng, University of Southampton.

Device safety

Professor Chris Hankin, Imperial College London, noted that the major security risk associated with the IoT comes from interactions with physical processes. With manufacturers making devices to different standards, problems could include:

- a lack of device interoperability
- devices interacting unintentionally and even representing a risk to user safety
- devices constructed from cheap or inferior hardware
- hardware posing a cybersecurity risk by containing malware, etc.

We must accept that systems will fail and that we can't predict all the situations that they will live in' said McCann. Networked systems can be designed to cope with change, eg bioinspired computing where devices share a common workload, building in collateral that protects the system and using the same tools to analyse cybersecurity infections as biological ones.

"There are clearly huge opportunities with this technology but there are also major threats to society, and we need to be cognisant of what can go wrong."

Professor Dame Wendy Hall DBE FREng FRS, University of Southampton

Data flow

McAuley noted that whilst it is often reasonable for a company to aggregate user data (eg so customers can compare their energy usage), considerable amounts of data are unnecessarily collected. This could be avoided by having end-to-end communication that doesn't involve a service provider (though such an arrangement is unlikely to be favoured by the provider). Alternatively, additional mathematical computing could be applied to data before sharing to preserve privacy. The IoT is generating more data than ever before, offering the ability to analyse systems and patterns in incredibly high detail. "Never before have we had the ability to monitor and understand what's going on to this level", said Professor Sadie Creese, University of Oxford. Though this offers opportunities to be more predictive than before, it also leaves systems and users open to threats by those that might use this insight maliciously.

"The IoT is the ultimate fusion of humanity, the natural world and technology."

Professor Sadie Creese, University of Oxford

Image: Professor Julie McCann, Imperial College London.

Business and economic issues concerning the IoT

The IoT in industry

As Professor Hugh Durrant-Whyte FRS, Chief Scientific Adviser, UK Ministry of Defence commented, the main benefit of the IoT to industry and business is the data collected. Networks, sensors, platforms, analytics and automation allow for monitoring, optimisation, the tracking of people and things and the promotion of safety – all of which can generate profit. A challenge for industry is the secure fusion of data sources from IoT devices, often achieved without central processing. This task requires both security and data privacy, eg privacy algorithms can allow data processing to take place without the user knowing the contents of the involved datasets.

As an early adopter of the IoT, industry has long grappled with issues that governments are only recently engaging with, such as the varying standards across different industries, which hinders the open use of IoT devices across them. Though the use of the IoT in industry isn't yet mature, industry will likely drive standards before governments impose them.

> "There is an enormous opportunity to exploit the IoT for business profit."
>
> **Professor Hugh Durrant-Whyte FRS, Chief Scientific Adviser, UK Ministry of Defence**

Responsibility and transparency

Elizabeth Linder from The Conversational Century noted that for many businesses, customer experience is key. They will go to great lengths to disguise cybersecurity and software procedures in order to deliver a 'seamless customer experience'. Challenges arise when governments ask companies to be more transparent for their customers. Whilst companies may be reluctant to police their users' data, many are still willing to collaborate with regulatory and enforcement bodies to maintain safe online environments.

As Dr Mike Short CBE FREng, Telefonica, told us, companies have the capabilities to offer much more than the user may want. For example, a cellular telephone company could offer security, customer care, updates or alerts, yet users may prefer to source these from elsewhere.

Though businesses have, in the past, considered cybersecurity a daunting and challenging task, many are now realising its potential as a profit making tool. Companies demonstrating the safety and security of their intellectual property are more likely to command customer trust, and thus their business. Many are even taking cybersecurity into their own hands by building their own data centres instead of outsourcing them, to ensure that they can control exactly how they connect with their customers.

Image: Elizabeth Linder, The Conversational Century (left) and Dr Jeremy Silver, Digital Catapult.

Investment in the IoT

Caroline Gorski, Digital Catapult, explained how private investment in the IoT has mostly been in the development of software for smart homes and buildings. It is here that venture capitalists predict the highest return on their money in the short term. This focus on software has detracted attention from investment in hardware (a tougher and more expensive challenge), leading to a market containing higher volumes of cheap and insecure hardware that pose security risks.

The IoT market will likely be shaped by:

- the desire for cost-effective solutions to expensive services, eg healthcare provision in remote areas
- the cost of products, their usage and maintenance
- the volume of uptake across different markets, eg low-cost disposable devices may attract more attention than specialised devices requiring long term investment.

> "The real value [of the IoT] is no longer in the product... but in the opportunities it offers to users, in terms of accessing information and experience."
>
> **Marina Kaljurand, Chair of the Global Commission on Stability of Cyberspace (GCSC)**

Image: Marina Kaljurand, Chair of the Global Commission on Stability of Cyberspace (GCSC).

Security: protecting our interconnected world

Device and network resilience

With cyber-attacks against companies and individuals becoming increasingly common, network breaches are an eventuality that must be planned for. Network breaches can have disastrous consequences, including:

- loss of confidential customer information
- disruption of network services
- impairment of critical industrial systems, especially physical outputs.

As more IoT devices are brought into our homes, workplaces and infrastructure, so are more gateways to private networks. If introduced without consideration of their safety, these gateways provide potential attackers with opportunities to infiltrate these networks.

As Robert Hayes, root9B, noted:

- security is often forgotten or challenging to include during device design
- hardware may have hidden capabilities, such as unexpected function or malicious software
- organisations may have completely unknown items contained within its network
- devices with limited or no capacity to have their software patched or upgraded pose a security risk.

Cybersecurity and the IoT

Hayes explained that security measures are most effective at the network level, but only if a full network map exists. This is because organisations that do not know what is on their network will be unable to isolate threats when they appear. A strong security strategy for an organisation considers:

- What, how and where an adversary will attack?
- Whether they will use IoT devices to accomplish this?
- How an attack will affect the organisation or its network?
- Whether important sections of the network need to be isolated to protect them?

Unless an organisation can answer these questions, they cannot properly act.

IoT devices add complication to network security but the threats are still manageable. If a network owner has knowledge of what is in their network, they can be alerted when an attack is imminent by using devices on the periphery of the network as ‘flags’. This allows time to isolate important parts of the network before extensive damage is done. To be successful, all devices in the network must be properly patched, with network owners understanding that software patches do not necessarily compromise safety simply because of their external origin. Knowing the provenance of firmware upgrades and patches is vital to good cybersecurity. As the IoT expands beyond industry, good industry practices such as detailed network surveillance could be passed onto the growing consumer market.

"The IoT will complicate several already existing cybersecurity questions, including legal ones... liability, attribution but also the effect of foreign acquisition of critical technologies ."

Marina Kaljurand, Chair of the Global Commission on Stability of Cyberspace (GCSC)

Image: Charlie McMurdie, PwC and formerly Metropolitan Police Service.

Cybercrime

The modern world contains increasingly complex cyber threats that the police struggle to identify or tackle, reflected Charlie McMurdie, PwC (formerly Metropolitan Police Service). With few police officers trained in cybercrime, it is unclear who will respond to it as it becomes more frequent and sophisticated. McMurdie argued that cybercrime is everybody's responsibility, not just that of the government, and industry should use their superior infrastructure and resources to supplement that of the police.

Frameworks and legislation

Dr Irina Brass, University College London, believes that the IoT is often described as 'disruptive innovation' because of its pervasive nature into society's increasingly connected lives, thereby changing socio-economic environments and the fundamental privacy and security principles on which our societies are organised.

As the IoT blurs the lines between data protection, security, safety and liability, current regulations may need to be adapted and aligned to match this change. Legislation has been designed without an integrated approach to these issues. The implementation of current and forthcoming regulatory frameworks will require more coordination and information sharing between the public agencies that monitor the adoption and enforcement of security by default measures.

Education and awareness

With IoT devices being attractive consumer goods, customers need to know the risks they are taking by bringing them into their homes. It is the responsibility of both public institutions and private companies to educate citizens in the security controls they should adopt. Service providers have a responsibility to protect user data but must also avoid becoming too intrusive when helping their customers. Users must also be aware that technical controls may not work if they keep agreeing to unreasonable terms and conditions and avoid best cybersecurity practice. Public bodies and the private sector have a responsibility to ensure that only IoT devices that adhere to 'secure by default' principles enter the market. In order to achieve this, governments might consider making 'secure by default' principles mandatory or adopt their own procurement policies that drive this.

Ethical, legal and global concerns

The IoT: we are never alone

By introducing sensors into public and private spaces and extracting data from everything people do, the public has accepted that every choice and movement is now 'data-fied', argued Maria Farrell, internet policy consultant and writer. The session speakers highlighted a number of implications.

- Data is possessed by entities who claim ownership over it and about whom users have very little knowledge.
- Users are expected to provide their data to a company for unlimited use and that company gets to deny all liability. Emily Taylor, Editor of Chatham House's Journal of Cyber Policy, warns that "we've come to tolerate an incredibly exploitative deal in return for free services".
- Those being observed have less power than those doing the observing, and many people feel unable to refuse surveillance.
- Being permanently watched could affect an individual's behaviour and ability to do deep, sustained, creative, radical work.
- Aggregated metadata can reveal a lot about the individuals from whom it was collected. Shorter lifespans of collected data may prevent misuse, as well as challenging of the terms and conditions that apply to the data given over to companies.
- Social machines, eg social media sites, rely on both human and machine input and increasingly occupy our society. New behaviours will emerge from these machines arising from deeper coupling of artificial intelligence and the data users share with it.

Arguably, legislation needs to adapt to protect the identity of both groups and individuals.

> "[The IoT] is where citizens are engaged with the digital world, they're generating data… they're the consumers of that data and sometimes they're involved in the analytics."
>
> **Professor David De Roure, University of Oxford**

Image: Professor David De Roure, University of Oxford.

Governance and infrastructure

Professor Laura DeNardis, American University, asked "how must we rethink internet freedom and internet governance in light of the IoT?". She argued that "The internet is no longer only a communication system – it is a control system in which more things than people are connected and in which infrastructure is a proxy for political power". This makes the IoT a human rights concern, as loss of network connections can mean loss of critical function from our everyday lives, eg damage to vital medical organisations or hacking of automated transport systems. The IoT has implications on our governance of the internet and its networked components, as IoT devices can be both damaged by attacks and used as the attack vector.

Anyone with internet access can be an actor, making internet governance a global infrastructure concern. IoT issues challenge traditional Internet governance norms such as the applicability of the multistakeholder governance model and suggest that IoT fragmentation is not necessarily problematic but can serve as a check on widespread cybersecurity attacks and mass data collection practices.

Accountability

A number of thoughts on accountability were considered:

- Is it the device or the human that programmed it responsible when an automated device fails and threatens someone's safety?
- As machine learning becomes more common in autonomous devices, it must be applied appropriately and safely.
- Autonomous vehicles that operate without human intervention will demand high levels of accountability, as the consequences of failure could be the loss of human life.
- If a company is to programme learning behaviour into its devices it will have to consider intellectual property, transferable knowledge and data ownership, in many ways resembling the procedure applied to humans.

These new concepts challenge current government structures to legislate for the future of the IoT and automation. As Gorski suggested, individuals and society first need to understand what is meant by being a 'digital human' in a networked civilisation if government and industry is to take responsibility on their behalf.

Image: conference participants networking.

Acknowledgements

Organisers

Professor Dame Wendy Hall DBE FREng FRS
University of Southampton Web Science Institute, UK

Dr Patricia Lewis
Chatham House

Dr Jeremy Silver
Digital Catapult CEO

Professor Jeremy Watson CBE FREng
UCL/BRE/Institution of Engineering and Technology

Speakers

Professor Bashir Al-Hashimi FREng
Professor of Computer Engineering,
University of Southampton

Dr Irina Brass
Lecturer in Regulation and Public Policy
Department of Science, Technology,
Engineering and Public Policy, UCL

Professor Sadie Creese
Professor of Cybersecurity, University of Oxford

Professor Laura DeNardis
Professor at American University Washington DC

Professor David De Roure
Oxford e-Research Centre, University of Oxford, UK

Professor Hugh Durrant-Whyte FRS
Chief Scientific Adviser, UK Ministry of Defence

Maria Farrell
Internet policy consultant and writer

Caroline Gorski
Head of IoT, Digital Catapult

Professor Chris Hankin
Director of the Institute for Security Science and
Technology and Professor of Computing Science,
Imperial College London

Robert Hayes
Senior Executive, Global Engagement, root9B

Marina Kaljurand
Chair of the Global Commission on
Stability of Cyberspace (GCSC)

Elizabeth Linder
Founder and CEO, The Conversational Century

Professor Derek McAuley
Professor of Digital Economy, The University
of Nottingham

Professor Julie McCann
Professor of Computer Systems, Imperial College London

Charlie McMurdie
Former Head of Law Enforcement National
Cyber Capability, Met Police

Dr Mike Short CBE FREng
Vice President, Telefonica

Emily Taylor
Editor of Chatham House's Journal of Cyber Policy

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities emphasise its commitment to the highest quality science, to curiosity-driven research, and to the development and use of science for the benefit of society. These priorities are:

- Promoting excellence in science
- Supporting international collaboration
- Demonstrating the importance of science to everyone

For further information
The Royal Society
6 – 9 Carlton House Terrace
London SW1Y 5AG

T +44 20 7451 2500
W royalsociety.org

Registered Charity No 207043
Issued: December 2017 DES5217

Cover Image