ROYAL ACADEMY OF ENGINEERING

PETRAS

Internet of Things

realising the potential of a trusted smart world

March 2018

www.raeng.org.uk/internetofthings

ISBN: 978-1-909327-37-5

Published by
Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel: 020 7766 0600
www.raeng.org.uk

#RAEngDigital

Registered Charity Number: 293074

The report should be referenced as follows:

Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H., Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, D., Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B., Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A., Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R., Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., Thompson, R.J., Westbury, P.S., (2018). *Internet of Things: realising the potential of a trusted smart world*. Royal Academy of engineering: London.

Contents

Foreword

Internet of Things (IoT) technology is finding application in many areas of industry and society, offering new services and promising increased time and resource efficiencies, and greater social wellbeing. However, much has been learned in the three years since the IoT Blackett review, with new challenges that cross social and technical areas, and that are interdependent in nature.

The PETRAS Cybersecurity of the Internet of Things Research Hub recognises that IoT comprises complex socio-technical systems and explores critical issues in privacy, ethics, trust, reliability, acceptability, and security. It brings together international research leaders from nine universities across the UK and works with cross-sectoral industry, government and NGO partners to identify barriers to IoT adoption, opportunities for IoT advancement, and the ability to develop best practice demonstrators.

As chair of the PETRAS Steering Board I have championed the use of the Hub's outputs to facilitate further adoption of IoT, unlocking potential economic value for the widest possible array of stakeholders and user groups. As a Fellow of the Royal Academy of Engineering I am committed to promoting excellence in engineering for the benefit of society and enhancing UK prosperity as an impartial adviser to government. The goals of both the research hub and the Academy are well demonstrated in the production of this report.

The report considers applications of IoT in three broad categories – consumer, industrial and public space – and examines the most pressing policy challenges, raising a broad range of issues that need to be considered to maximise impact.

It is particularly pertinent, in an uncertain international landscape, that this report highlights the UK's opportunity to lead the development of international IoT strategy. Any international strategy needs to include the sharing of knowledge and best practice relating to both technical and social aspects of the IoT, as well as policy implementation. Ensuring the UK leads this development will give the best opportunity for the UK to become an established, leading player in the emerging international IoT product and service market.

Dr Mike Short CBE FREng
Chair of the PETRAS Steering Board
Chief Scientific Adviser, Department for International Trade

Executive summary

This report examines the policy challenges for the Internet of Things (IoT), and raises a broad range of issues that need to be considered if policy is to be effective and the potential economic value of IoT is harnessed. It builds on the Blackett review, *The Internet of Things: making the most of the second digital revolution*, adding detailed knowledge based on research from the PETRAS Cybersecurity of the Internet of Things Research Hub and input from Fellows of the Royal Academy of Engineering. The report targets government policymakers, regulators, standards bodies and national funding bodies, and will also be of interest to suppliers and adopters of IoT products and services.

Key messages are summarised below:

Strong leadership and oversight from government is vital to address complex and interdependent challenges

The approach to developing appropriate governance and regulation for IoT will need to reflect the disparate requirements of different sectors and areas of application, while identifying their points of commonality. A systems approach to policymaking will help to map out sector-specific and common issues, the roles and responsibilities of the different stakeholders, and how stakeholders should work together. The IoT agenda needs a recognisable home within government.

For the purposes of defining policy objectives, IoT applications can be divided into three broad categories – industrial, public space[1] and consumer

Each category has broadly different objectives, communities of stakeholders, legal and regulatory contexts, governance arrangements, and public expectations. Policymaking should reflect the differing objectives of these categories while adopting an approach that acknowledges there are disparate requirements and constraints relating to sectors or domains within each category.

Obtaining value from data is at the heart of IoT and a key business driver

Looking to the future, IoT's value will enhance because of its convergence with technologies such as artificial intelligence (AI), which can usefully extract information from the large volumes of data generated by IoT.

Three years on from the Blackett review, many of the barriers it identified are still present

Security and interoperability remain key issues. Technical standards, including those that promote security and interoperability, remain fragmented. However, overcoming barriers goes beyond the technical and requires a change of mindset and culture too: for example, greater security awareness and a willingness by organisations to create interoperable systems.

Policies and technologies will be more effective if an understanding of interdependent social and technical factors underpins them

An understanding of what influences trust and acceptability, and how this varies across different groups of end-users, is vital for ensuring that policies that support adoption are successful. Analogously, technologies that enhance privacy and trust will be more effective if their design incorporates an understanding of human behaviour.

The UK will need a strategic approach if it is to fully harness the economic potential of IoT

A forward-looking approach will help to identify how policy and other interventions might influence progress towards strategic goals. A strategy for IoT should align with key policy initiatives such as the government's industrial strategy, and related initiatives such as the AI Sector Deal, the *Made Smarter* review, and the Robotics and Autonomous Systems (RAS) 2020 strategy.

The UK should lead internationally

Many IoT components and devices are manufactured outside the UK, with implications for the UK's global competitiveness and its role in international regulation. The UK will need to focus its efforts on where it has strengths and can lead, whether these strengths lie in industry, research or regulation.

Consolidation of national and international knowledge and forums for sharing best practice will help

These will benefit policymakers as well as suppliers and adopters of IoT. They will also stimulate the cohesion of IoT ecosystems that are emerging, but still fragmented. The generation of knowledge through research – fundamental or applied to particular policy, technology or business challenges – remains vital.

IoT is an enabling technology that has the potential to fundamentally change society and business processes within and across sectors. At its most basic, IoT connects devices through the internet, which consumer applications such as smart home appliances or wearable technologies already do. IoT systems used in industry or smart cities may be more complex, and owned, governed and controlled by many different bodies. With applications across energy, construction, infrastructure, manufacturing, health, agriculture, defence, and transport, as well as public sector and consumer applications, there will be few parts of society not affected by IoT. As with other emerging technologies, there are substantial and interdependent issues around privacy, ethics, trust, reliability, acceptability, safety and security for the systems that are created, whether these are the smallest connected sensors and devices or large-scale platforms deployed in physical infrastructure. These issues play out very differently across sectors and applications.

Three years on from the Blackett review, a growing, if fragmented, IoT market is beginning to capitalise on new business opportunities around IoT products and services. However, greater economic gains are likely to be from increases in productivity or efficiency in industrial sectors and, looking further ahead, from applications that help to solve global challenges such as affordable healthcare and a cleaner environment. Many more innovations are expected as the technology develops, particularly when coupled with other technologies, such as AI and robotics, and with new business models. Capitalising on IoT's potential will help the UK government to deliver both its industrial strategy and digital strategy. It is an important technology for enabling the delivery of the industrial strategy's four Grand Challenges.

Leading sectors, such as the mining industry, already benefit from implementing IoT where the business case has been made. For other sectors, it can be harder to develop viable products and services, particularly for startups and SMEs targeting new – and possibly volatile – markets. End-users need support to identify IoT's potential value with greater clarity on liability and responsibility. Industry also faces the challenge of how to introduce nimble, flexible and scalable IoT solutions rather than massive and unwieldy non-interoperable platforms, so that systems are cheaper and quicker to design and build.

As IoT devices and systems continue to proliferate, it is vital that security is an integral part of their design. There is also the challenge of how to deal with legacy systems that did not need to address security when initially built – particularly those used in critical infrastructure – and with partially trusted IoT systems that are a combination of old and new. Security challenges are dynamic, and it may be that new vulnerabilities are discovered in devices that have already been deployed. There are generic security challenges across applications, as well as application-specific challenges in

THERE ARE SUBSTANTIAL AND INTERDEPENDENT ISSUES AROUND PRIVACY, ETHICS, TRUST, RELIABILITY, ACCEPTABILITY, SAFETY AND SECURITY FOR THE SYSTEMS THAT ARE CREATED.

areas such as critical infrastructure, connected and autonomous vehicles, medical devices, and consumer appliances.

The massive volumes of data generated by IoT will require robust data management, to ensure that the provenance of data, its quality and integrity are understood and that privacy is preserved. Privacy-sensitive approaches to the collection, transfer, processing and storage of data will help to maintain trust in IoT. As the number of IoT devices increases in homes, workplaces and public spaces, there is greater potential for aspects of people's lives to be observed. Ethical frameworks will encourage those developing and deploying innovative IoT devices and systems to practice responsibly.

Cross-sectoral regulations of relevance to IoT already exist in areas such as data protection (General Data Protection Regulation (GDPR)), network and information security (Network and Information Systems (NIS) Directive), and radio equipment while sector-specific regulations are also emerging. Recent international developments, such as the US IoT cybersecurity bill[2] and the proposed EU cybersecurity certification scheme, are also likely to shape the regulatory landscape in the future. The unique characteristics of IoT are such that the development of new policy or amendments to existing arrangements are likely to be needed. There is also a challenge in ensuring that developers of IoT products and services comply with the appropriate regulation.

This report is published alongside the Royal Academy of Engineering's report, *Cyber safety and resilience: strengthening the digital systems that support the modern economy*, which considers regulatory and non-regulatory measures, including engineering approaches, for improving the safety and resilience of interconnected physical and digital systems.

The next section discusses the key messages in detail, along with recommendations on: policymaking; governance and regulation; overcoming technical and business challenges; education and skills; infrastructure; security standards and policy; risk management and resilience; liability; commissioning; and ethics and privacy.

AS IoT DEVICES AND SYSTEMS CONTINUE TO PROLIFERATE, IT IS VITAL THAT SECURITY IS AN INTEGRAL PART OF THEIR DESIGN.

Key messages and recommendations:

Overarching IoT policy and governance environment

1. Policy objectives for industrial, public space and consumer applications of IoT

IoT is an overarching term describing networks of connected devices that are deployed in many different sectors and applications. While there are various ways in which these applications can be characterised, it is useful for the purposes of policymaking to separate them into industrial, public space and consumer applications. While these three categories are not entirely distinct, each category has broadly different communities of stakeholders and differing public expectations, legal contexts and governance arrangements. Each category also has varied desired outcomes upon which policymaking should focus. Policy for industrial applications should focus on realising tangible productivity and efficiency gains, plus developing the secure provision of services through connected products or assets. Consumer IoT policy should focus on customer benefits such as reduced utility costs and improved quality of life, while proposing ways to reconcile the demands of security, privacy, cost and ease of use. Policy outcomes for public space applications share common elements with industrial and consumer applications – for example, outcomes might include both public sector efficiencies and customer benefits – and will need to balance the benefits between the various stakeholders. Focussing on these outcomes will help to ensure clarity in a complex landscape.

Recommendation 1: In developing policy for IoT, the Department for Culture, Media and Sport (DCMS), the Department for Business, Energy and Industrial Strategy (BEIS) and other government departments should distinguish the differing policy outcomes for industrial, public space and consumer applications of IoT. Policy for industrial applications should reflect the need to drive productivity and efficiency as well as threats to national infrastructure, manufacturing capability and safety. Policy for consumer applications should reflect consumer benefits such as improved quality of life but not compromise security or privacy. Policy for public space applications should reflect desired outcomes around both improved efficiency and consumer benefits.

2. Governance and regulation – a heterogeneous approach

A heterogeneous approach to governance and regulation of IoT should be pursued, rather than a one-size-fits-all framework that addresses IoT as a single entity. This approach should acknowledge the disparate requirements and constraints of sectors or domains along with their points of commonality. New policies should build on the existing regulatory contexts of each individual sector. Where possible, common approaches across sectors and domains will help to avoid duplication and support multi-sector supply chains and applications. Sectors must work together to ensure consistency between policies for existing cross-sectorial applications or those that may emerge in the future, for which strong government leadership will be required. Policymakers should consider adaptive methods for governance and regulation, which are built on forward-looking analysis of the benefits and risks of IoT. These methods will help to ensure that regulation keeps up with the fast pace of technological development.

There will need to be new mechanisms, and perhaps new regulatory frameworks, for cooperation between sector regulators and a genuine systems approach to policymaking. This will require joining-up across government departments, which will need government to have strong oversight of policymaking, to take on a convening role for the many stakeholders involved and develop ways of enabling cross-departmental working. Government should also have a strong international focus, and address issues around establishing and regulating both national and international markets. There is an opportunity for the UK to contribute to, and where appropriate lead, development of an international harmonisation of standards and governance of IoT – the involvement of the US and EU will be needed for this to be effective. International benchmarking of organisations will be key to achieving this successfully.

Recommendation 2a: The IoT agenda – encompassing industrial, public space and consumer applications – should have a recognisable home within government. That part of government should take a leadership role in coordinating policy across departments and internationally, and in using government's convening power to bring the relevant stakeholders together. As part of a systems approach to policymaking, government should have strong oversight of IoT policymaking activities and of the various stakeholders that need to be involved in developing policy. This will help develop the combination of regulatory and non-regulatory measures required to ensure that IoT systems underpin a secure and trusted future.

Recommendation 2b: Stakeholders involved in governance and regulation of IoT, including government departments, regulators, standards bodies and industrial alliances, should collaborate to identify points of commonality between sectors, while distinguishing sector-specific requirements for governance and regulation. They should work together to develop common approaches to governance and regulation across sectors, where possible. These approaches should have flexibility to accommodate the applications that might emerge in the future. Government should coordinate activities between sectors. The market is very fast-moving, driven by business need and business opportunity. It is therefore important to ensure that the main players – for example, the major device manufacturers and network providers – engage in these activities.

Recommendation 2c: Government should continue to facilitate the development and deployment of standards for IoT where needed, building on progress to date. It should use its considerable convening power to bring together standards, policy and regulatory communities to develop an approach that best promotes the values and interests of the UK in a global context. Government should actively support UK national standards bodies in leading on the development of international standards, including coordinating and funding UK delegations. The BSI's Publicly Available Specification (PAS) is one mechanism that can increase the tempo of standardisation and promote UK interests. To maximise expert involvement in standardisation and ensure independence from individual industry lobbying, the government should fund academics' participation in IoT standardisation and ensure that involvement brings credit in research impact assessments.

Recommendation 2d: The UK government should work with other governments and international institutions – with the main providers of IoT components, devices and systems – towards 'umbrella agreements' that set out an international baseline for IoT data integrity and security for all parties to adopt. This will support the international supply chain in offering products and services globally.

3. Building capacity and coordination in cybersecurity policymaking and governance

Given the challenges of policymaking for IoT, as well as its complex, interdependent nature, developing global security solutions will require support in the form of capacity-building measures for governance and policy at an international scale. Very few

governments have the resources to fund large-scale IoT security policy research, but their decisions and approaches may have implications that will affect the UK. To maximise knowledge sharing and minimise the duplication of effort, and to enable dissemination of best practice findings to a global policy community, policymakers and researchers working on these issues require more cohesion through conferences, themed meetings and working groups, which will help to develop an international IoT policy research community.

As it did with the 'London Process[3], there is an opportunity for the UK to coordinate and shape debates about international cybersecurity policy in the context of IoT. There is a lack of focus and leadership in key international organisations on these matters, where legacy cybersecurity concerns continue to drive discussions. To guide the advancement of norms and agreements that will be necessary to ensure a safe and secure IoT, international policy coordination and cooperation will be essential.

Recommendation 3a: Existing UK cybersecurity capacity-building initiatives should be expanded to include IoT policy support for states without the research capacity to address these challenges. Existing policy-relevant research should be coordinated and disseminated through the establishment of an international IoT policy research community.

Recommendation 3b: The UK government should exercise its leadership to begin discussion on how it will integrate IoT into current international political negotiations over global cybersecurity.

Harnessing economic value

4. A strategy for IoT

IoT is widely recognised as an important underpinning technology for improving productivity and innovation, and creating a data-driven economy. A clear strategy for IoT is needed, building on the industrial strategy White Paper[4] and sector-specific reviews and strategies such as the government's *Made Smarter* review[5], the National Infrastructure Commission's new technology study[6], the AI review[7] and the RAS 2020 strategy[8]. The strategy should integrate best practice and current initiatives such as test beds and demonstrators, address where research and development effort is needed, and consider barriers to adoption. The strategy should go beyond IoT towards the 'Internet of Everything', with a greater focus on people, data and processes. This approach would build on the important support provided by Catapults.

There are lessons to be learned internationally about how IoT technologies are being applied in key sectors and how value from these systems is being created. It would be of great benefit to gather information about which IoT systems have been designed and deployed, the associated economic costs and benefits (where they can be identified), and the technical and social outcomes. This would ensure that testing, deployment and implementation of IoT in the UK could build on international best practice.

The strategy should identify the roles of the different stakeholders. While it is the market that determines which IoT systems are used and where, government has an important role in ensuring appropriate levels of safety, security and privacy in the deployment of these systems, whether they are in manufacturing plants, driverless cars or medical devices. The systems need to be trusted and trustworthy; for example, the end-user requires assurance that products or services bought comply with assured standards.

Recommendation 4a: As part of its leadership role, government, working in partnership with industry, should develop a clear strategy for IoT. The strategy should align with related strategies around digital technologies and encourage innovation, commercialisation and adoption of the technologies, and stimulate the development of the UK's industrial IoT ecosystem. The strategy should recognise IoT as a socio-technical system, with a focus on people, data and processes in addition to the technologies that underpin the development of products and services. It will need a systems approach to tackle the complexity and interdependent nature of the challenges. This links to Recommendation 2a, which advocates the adoption of a systems approach to policymaking.

Recommendation 4b: Government should commission an ongoing review of best practice at both a national and international level to consolidate knowledge about how IoT solutions have been realised in industrial, public space and consumer applications and inform how testing, deployment and implementation of IoT in the UK can build on best practice. This is pertinent across all areas of IoT but particularly important in security, and in understanding how best to balance risk and reward in IoT implementation and how they are shared between stakeholders. The review should include the use of existing or new, innovative business models. Detailed information about the approach that a specific industry can take to adopt IoT in their upstream and downstream processes would also be of value.

5. An infrastructure roadmap

Accompanying the IoT strategy, a clear and widely-shared infrastructure roadmap for IoT that inputs into the National Infrastructure Delivery Plan[9] (NIDP) will be of great value and it should identify funding requirements. This aligns with the Blackett review recommendation for an IoT infrastructure roadmap. Such input to the NIDP should embed a clear understanding of the ownership, responsibility and extent of liability in relation to constituent parts of the IoT infrastructure, which is fragmented in nature.

Recommendation 5: Government should commission the development of an infrastructure roadmap for IoT that will feed into the NIDP. This will provide valuable information for developers and operators of IoT infrastructure, as well as for device and system manufacturers that will require connectivity from IoT infrastructure.

6. Overcoming technical and business challenges

Interoperability in IoT systems continues to be a central issue in harnessing economic value. Interoperability is needed at many different levels to ensure that the ecosystems can be created, components and systems are secure, and that the data generated can be effectively and responsibly shared and used. To date, much of the focus has been on the interoperability of devices, networks and communications protocols. Interoperability of communications is an intrinsic characteristic of the internet, and IoT solutions created today are generally all IP-enabled. Although technical interoperability may be feasible, organisations may be reluctant to create interoperable systems if they perceive that it will put their competitive advantage at risk. Demonstrating the business benefits of interoperability will be important.

In future, broader aspects of interoperability – for example, security controls, data and platforms – should be addressed. Support for interoperability technology demonstrators would clearly be helpful and should be an important consideration for UKRI. The government should explore investment incentives for the embedding of smart sensor networks with non-proprietary access. The role of testing and certification to demonstrate that IoT products achieve compliance with standards that promote interoperability should also be investigated.

There is a need to improve data management to ensure that the right data supports business needs. This requires a change in culture and business practices that enables the use of data as an asset. Access to data with high quality and integrity is a requisite part of realising

THE EDUCATION SYSTEM ACROSS THE UK NEEDS TO INCENTIVISE INCREASING NUMBERS OF STUDENTS FOLLOWING PATHWAYS TO ENGINEERING. THE RECENT INVESTMENT IN COMPUTER SCIENCE IN SCHOOLS IS WELCOME.

the significance of IoT. To realise the value of the large volumes of data generated, there is a need to incentivise and facilitate privacy-sensitive collection, secure trading and controlled sharing of proprietary data. Better understanding of data value chains and fair mechanisms for sharing value would be of benefit. Where personal data is shared, the consumer must have clear and potentially transferable rights under the GDPR. New models of ownership of data rights will be needed.

Recommendation 6a: UKRI should provide funding for interoperability demonstrators, including the necessary security controls, data and platforms. These demonstrators should be developed alongside the recommendations on standards (2c and 8a) that are central to achieving interoperability. They could be implemented as part of the *Made Smarter* review that recommends setting up large-scale demonstrators within Digital Innovation Hubs. Funding for interoperability demonstrators for health, energy and transport would help to address the Grand Challenges identified in government's industrial strategy White Paper. In addition, the Catapult network[10] should pursue actions to explore ways of incentivising and facilitating the controlled sharing of proprietary data, building on early exemplars from the UK and abroad. UKRI should promote the best practices defined in guidelines and regulations while encouraging the use of available services, toolkits, open source software and open application programming interfaces (APIs) to exploit IoT opportunities.

Recommendation 6b: As part of the knowledge transfer initiatives in Recommendation 4b, conferences, exchange schemes and networks should target business and industry leaders – CEOs and board members. This will enable knowledge transfer about the culture change needed to bring about the effective adoption of IoT and transform companies' approach to protecting and using data. It would also help to develop the emerging industrial IoT ecosystem and support adoption (this links to Recommendation 4a).

7. Education and skills

Appropriate digital skills are required at all stages of the pipeline to deliver the IoT strategy and harness its economic value. While the UK government's commitment to helping people develop the skills needed (including the focus on reskilling and upskilling) for jobs of the future as part of its industrial strategy[11] is welcome, the ongoing skills shortage highlights the need for a major expansion of existing educational initiatives, programmes and strategies, or for a completely new way of delivering them. In addition to technical skills, other important skills include design, strategic planning, leadership and change management.

Curricula and training activities require adjustments to suit the skills demands of the emerging IoT market. These should be tailored for people requiring sector-specific IoT skills such as healthcare workers or factory employees. Stakeholders should support initiatives that encourage diversity of the talent pool. Schools should foster greater awareness of technologies and how they work around us to create a basic level of digital understanding and future generations of informed consumers that can make use of IoT. The government's plans to evaluate the impact of current Digital Skills Partnership[12] initiatives are welcome.

Recommendation 7a: Government should ensure that the reforms to post-16 education (T levels and new apprenticeships standards) include appropriate levels of skills development for end-users of IoT in the workplace. The basic digital skills content across all routes of the T levels should be sufficiently generic to cover all sectors and occupations, while specific T levels should provide the necessary specialisation. Implementation of the reforms will need to consider local employer needs.

Recommendation 7b: Government should examine the practical and scalable solutions needed to upskill the existing workforce. The creation of high-quality, employer-endorsed online training platforms is one possible option, as proposed in the recent *Made Smarter* review.

Recommendation 7c: The education system across the UK needs to incentivise increasing numbers of students following pathways to engineering. The recent investment in computer science in schools is welcome. Government should consider similar investments in design and technology in schools, as this subject provides excellent opportunities for young people to understand interfaces between physical and digital systems as well as practical opportunities to apply this, for example to IoT.

Recommendation 7d: Building on its plans to 'build digital capability for all' as part of the Digital Strategy[13], government should work with business and industry to deliver evidence-based initiatives to educate the public about IoT. These should improve technical and data literacy by raising awareness of the benefits and limitations of such technologies and ensuring that the public are informed users.

Security and Risk Management

8. Security standards and policy

To ensure end-to-end security of the IoT across different domains and application areas, formal standards that address security considerations in the design of IoT reference architectures are needed. The current standards landscape for IoT security remains fragmented, with several industry associations, interest organisations and regional standards-development organisations proposing guidelines, specifications and certification schemes for IoT security. As far as possible, baseline security specifications that apply across sectors should be developed, given the multi-sectoral nature of IoT ecosystems, while recognising that end-to-end standards solutions are easier to achieve within one sector.

Cybersecurity policies should require that there is transparency throughout the supply chain about the level of cybersecurity provided in products and services, and how this has been traded off against cost and ease of use.

Recommendation 8a: Government, working with the National Cyber Security Centre, UK national standards bodies, regulators and industry, should enable the development of security standards for IoT that provide a baseline across sectors, recognising the multi-sectoral nature of the supply chain, while working within specific national and international industry contexts. This recommendation should be carried out alongside Recommendation 2c.

Recommendation 8b: Government departments should ensure that policy reflects the critical importance of cybersecurity and the need to trade-off cybersecurity against other considerations that contribute to achieving policy objectives. DCMS, BEIS and other government departments should work with the National Cyber Security Centre and others to explore ways of ensuring levels of cybersecurity are transparent for products and services throughout the supply chain.

9. Risk management and resilience

In addition to 'security by default', government should help promote 'resilience by design', so that resilience thinking is embedded in the design and management of IoT systems across their lifecycle. This will help to ensure that resilient systems are created with appropriate secure and safe behaviours to minimise impact in the event of failure or compromise.

Recommendation 9: Government should commission guidance on how to integrate 'security by default' and 'resilience by design' principles and methods into the development of IoT products and services, on a sector-by-sector basis. Evidence that these approaches have been followed could help to demonstrate that products, services and systems have been developed with due attention to risk management and provide adequate security and resilience. This feeds into the recommendation on ensuring transparency about cybersecurity in products across the supply chain (Recommendation 8b). Guidance should be promoted widely to industry. Alongside government, professional institutions should play a role in encouraging security-mindedness[14] and resilience-mindedness in professions.

10. Liability

Liability and chains of liability are significant issues for IoT, especially in an international context where the supply chain is global. However, it will be a challenge simply to assign liability in relation to IoT. Further exploration of this issue is required, along with consideration of alternative approaches and alignment with ongoing international initiatives in this space.

Recommendation 10: Government departments, regulators, legal bodies and industry organisations should work together on a sector-by-sector basis to explore the suitability of existing liability regimes for IoT applications, and to develop new approaches to liability where necessary. These actions should align with international initiatives.

Adoption and implementation

11. Ethical frameworks, privacy and consent

Designers, engineers, scientists and managers of IoT technologies are increasingly stewards of whole ecosystems, with moral responsibilities and liabilities. Appropriate ethical frameworks that support ethical behaviours should be developed and applied. These will be necessary for minimising risks to society, and ensuring that IoT systems do not create or enhance negative biases against certain groups nor underpin unethical approaches to surveillance or censorship. The potential use of IoT data in law enforcement also needs to be addressed.

Consent in IoT presents a complex and multi-faceted problem that is currently unresolved. While the GDPR strengthens the principle of consent, how the principle will apply in the context of IoT remains uncertain. Consumer IoT solutions pose important issues in terms of safety and consent, and social equality. As new uses of IoT data emerge, further focus is required to address the issue of consent, alongside related issues of data rights ownership and processing. Data protection authorities will need to develop clear guidelines about how to achieve consent in complex systems[15].

Further questions around how the regulation is implemented in practice will need to be resolved, for example where a service provider using cloud services is based outside jurisdictions that implement the GDPR. Monitoring GDPR introduction could be useful to learn from implementation challenges and to identify unintended side effects.

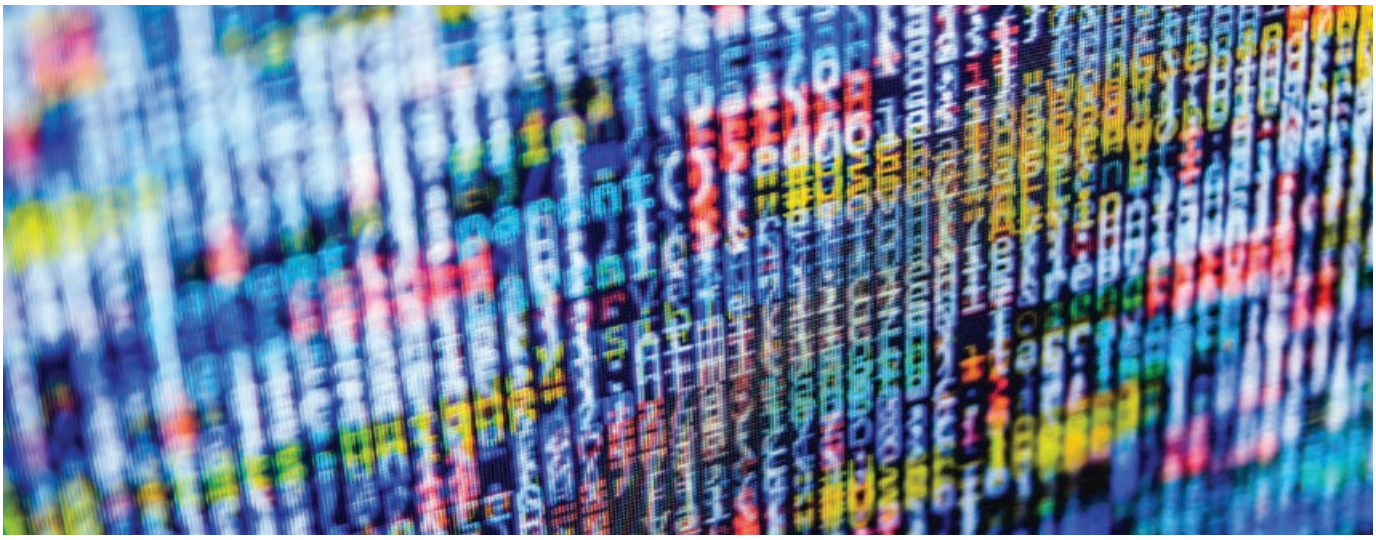
Recommendation 11a: Professional engineering institutions and other professional bodies, working alongside DCMS and the Centre for Data Ethics and Innovation, should build on existing ethical principles developed for professions to create an ethical framework for IoT to encourage ethical behaviours. They should provide case studies to illustrate how the principles are applied in practice.

Recommendation 11b: The Information Commissioners' Office should develop best practice guidance for IoT stakeholders that nurtures a clear understanding and implementation of the data protection regulations.

12. Commissioning

Government can exert major influence on adoption through its own procurement actions. In these emerging technology areas a government preference for specialised purchasing from entrepreneurial SMEs could have great benefit. However, the perception remains that public procurement decisions continue to prioritise low cost over best value, and risk aversion hinders the introduction of innovative solutions[16]. Government should adopt the established best practice around intelligent procurement, which will involve cultural change and a greater willingness to establish and accept an appropriate level of risk.

Recommendation 12: Government should consider how best to change the culture of risk aversion in public procurement decision-making, and encourage government departments and other public bodies to embrace innovative solutions to support the adoption of emerging technologies such as IoT.



1. Introduction

This report is published three and a half years after the publication of the Blackett review of IoT[17], which identified the opportunities for the UK to create economic value from the Internet of Things (IoT). Drawing on research from the PETRAS Cybersecurity of the Internet of Things Research Hub (PETRAS) and other sources of evidence, this report builds on the Blackett review and discusses the developing governance and regulatory context for IoT, and the key issues that need to be addressed if the benefits of IoT are to be realised.

The key issues are grouped under three interdependent themes:

- harnessing economic value
- security and risk management
- adoption and implementation

Many of the issues are interdependent, which creates additional complexity and greater difficulty in developing solutions to the challenges. The report suggests ways of tackling this complexity and puts forward policy recommendations to help the UK to position itself to capitalise on the opportunities provided by IoT. A strategic research agenda identifies areas for future research (see Annex). It is published alongside a Royal Academy of Engineering report, *Cyber safety and resilience: strengthening the digital systems that support the modern economy*[18], that examines in detail the issues around safety and resilience of systems, including IoT.

IoT is an umbrella term that reflects an evolution of technology towards a proliferation of cheap 'embedded systems'[19a] connected to a network. It may comprise sensors that collect and transmit data, systems that make use of aggregated data and actuators that, on the basis of this information, take action with or without direct human intervention[19b]. The term IoT is used across a whole spectrum of applications, from the smallest connected sensors and devices to large-scale platforms that can be deployed with physical infrastructure. IoT is considered a disruptive innovation in the sense that it has the potential to fundamentally change societal and business processes within and across sectors[20]. Box 1 shows key considerations – technical and regulatory – for developers of IoT systems.

IoT has wide-ranging industrial, public space and consumer applications. Consumer applications are attracting much public and media interest, and there is a growing market for products and services in domestic and other consumer environments. The value

THE TERM IoT IS USED ACROSS A WHOLE SPECTRUM OF APPLICATIONS, FROM THE SMALLEST CONNECTED SENSORS AND DEVICES TO LARGE-SCALE PLATFORMS DEPLOYED WITH PHYSICAL INFRASTRUCTURE.

gained from IoT's industrial applications may eventually dwarf that from consumer applications, since industrial sectors such as manufacturing, oil and gas, agriculture, and transportation make significant contributions to the UK and the world economy[21]. Public space applications such as smart cities and intelligent mobility have the potential to underpin consumer-focused services and reduce traffic congestion, for example.

A fragmented IoT ecosystem is emerging in the UK, Europe and globally, as would be expected in an evolving market. The ecosystem is complex and includes providers of hardware, software and communications services, systems integrators and users. Cloud service providers and big data companies are also increasingly involved in the ecosystem[22]. Commercial opportunities around hardware and software arise at every scale, particularly where products can be patented and sold in high volumes. For example, companies such as Arm and IQE supply hardware components. In the future, some companies may find a way to commodify components that use energy harvesting technologies. Other companies may provide communications subsystems. Others may implement increasingly complex subsystems and systems, including traffic sensors, traffic lights and journey planning for a city, for example.

There are also commercial opportunities around data-enabled services and the technologies that enable such services. IoT data marketplaces[23] or data platforms that allow controlled sharing of data between organisations are emerging and will allow the volumes of data to be used effectively. Personal data stores that allow consumers to control how they share data with organisations are also evolving, with potential benefits to both[24]. Developments that enable access to new forms of data will in turn provide opportunities for new uses of technologies, such as data analytics and artificial intelligence[25], that are able to generate value from the collected data, but also offer the opportunity for its misuse.

A technology push and a demand pull have driven the market to date. The technology push derives from improvements to network connectivity, the creation of new devices and platforms, developments in cloud computing, and progress in data management and analytics techniques. The demand pull is from business and consumers, as well as public sector initiatives such as smart cities. These two driving forces continuously inform and support each other. Small firms could play a significant role in meeting growing demand, possibly supported by innovative sources of funding[26]. Big industries, which tend to be conservative in nature,

Box 1: Developing an IoT system – key considerations

- What are the applications and what system architecture will they need? Developers should consider system architecture, before individual components.
- What hardware is required, where is it located and in what is it embedded? What should any sensors measure?
- What are the power requirements for sensors, processing, actuators, displays and communications?
- What communications protocols do systems need?
- Where is data stored? Where and how is it processed?
- What security is needed for the hardware and software, and data at rest and in motion? What are functional considerations resulting from a loss of security?
- Is it possible to update firmware – the computer programs that run a device – in a safe and secure way?
- Have issues of ethics, trust, acceptability and reliability been addressed?
- What are the legal requirements around data protection, including the need for informed consent and other aspects of GDPR compliance?
- What are the legal requirements around safety (Health and Safety at Work Act 1974)?
- What are the legal requirements around security and continuity of service (NIS Directive)?
- What are the arrangements for maintenance, updating and revocation, especially if the hardware is not readily accessible (for example, if it is embedded in a bridge or implanted in a patient)?
- Has the impact on end-users and change management aspects been addressed?

THERE IS THE EXPECTATION THAT IoT COULD INCREASINGLY BE USED TO HELP ADDRESS GLOBAL CHALLENGES SUCH AS IMPROVING PRODUCTIVITY AND RESOURCE EFFICIENCY, CLIMATE CHANGE AND DEMOGRAPHIC SHIFTS.

can adopt technologies developed by smaller firms that are more agile and flexible, because market competition incentivises them to strive for innovation and accept higher economic risks.

Personalised services will increasingly emerge that have the potential to improve individuals' quality of life, such as those that support assisted living or help improve energy efficiency and reduce costs. Other more commercially driven consumer products and services will continue to emerge, such as the 'connected home hubs' being developed by large players such as Amazon and Apple. New uses of IoT will also improve efficiencies in industry and underpin new services. Organisations such as IBM and General Electric are developing industrial IoT platforms, as are emerging specialist IoT companies such as Telit[27] and Teezle[28]. Some organisations within existing industrial sectors may have the expertise to implement IoT solutions by realigning existing in-house capabilities, while others will need to bring in or outsource expertise.

There is also the expectation that IoT could increasingly be used to help address global challenges such as improving productivity and resource efficiency, climate change and demographic shifts[29]. For example, smart city applications could reduce energy use and waste, ease traffic congestion, and improve the efficiency of public services. Health IoT applications could reduce healthcare costs by enabling remote monitoring and treatment of patients, reducing the pressure on hospitals.

Privacy, safety, security, ethics, trust, accessibility and reliability are all key areas of concern, and should be considered from the outset in design, operation and maintenance of IoT devices and systems. IoT covers several technologies and processes, with a variety of regulatory frameworks that apply to them (see Box 1 and Section 4.1). Approaches to designing and operating IoT systems will need to acknowledge the physical, human, social and digital dimensions of IoT to address the areas of concern. Challenges around privacy, safety, security, ethics and trust play out very differently across different sectors and applications, depending on the sensitivity of personal or commercial data collected, and on individual, operational, commercial or national security requirements.

2.
Policy context

The Blackett review of IoT[30] highlighted the challenges around the adoption of IoT and the role that government can play in helping to achieve the economic potential of IoT. It outlined the actions for government to maximise opportunities and reduce the risks associated with this new technology.

More recently, IoT was identified as a key emerging technology sector in the government's Digital Strategy[31]. The government acknowledges that it can play a part in supporting the growth of such technologies through strategic interventions, with the aim of the UK remaining an international leader in R&D and adoption of IoT. PETRAS is part of a £30 million IoTUK programme of research and innovation funding that also includes the large-scale CityVerve smart cities demonstrator in Manchester, NHS test beds, and support for IoT entrepreneurs.

In the same vein, the Digital Strategy also outlines how the government can help unlock the power of data in the UK economy and improve public confidence in its use. It recognises that the increasing adoption of new technologies such as IoT produces increasing volumes of data, which creates new opportunities for business growth across sectors. The strategy also recognises that data infrastructure – 'the assets, technology, processes, and organisations that create data, open it up and allow it to be shared'[32] – is integral to the successful development of technologies such as IoT, as are data handling and analytical skills.

In broad terms, the Digital Strategy signals the government's plans to address the shortage of specialist digital skills to fill specific digital jobs, as well as digital capability for the public as a whole. However, it is not specific about skills for IoT. The Blackett review highlights specific skills that will be required in the design, development, installation and maintenance of IoT. Although not addressed in either document, it is important that there are people who can understand the technology's potential and limitations and can see how it might be used in business. Consumers also need to be aware of how the technology might benefit them, along with the risks.

The diversity of IoT applications across a wide range of sectors, including energy, construction, infrastructure, manufacturing, health, agriculture, defence and transport, means that policy implications will be of relevance to a wide range of government departments. IoT is a key underpinning technology that will help the government put the UK at the forefront of the AI and data revolution[33]. It will also support the success of other Grand

AN UNDERSTANDING OF THE GLOBAL COMPETITION IS VITAL FOR THE UK TO ESTABLISH ITS OWN POSITION IN A GLOBAL MARKET.

Challenges set out in the industrial strategy White Paper – clean growth, the future of mobility and an ageing society – by enabling smart systems and greater resource efficiency, underpinning new business models in transport and driving innovations in health and care.

There are several detailed policy studies that illustrate application of IoT in specific contexts. For example, IoT is one of the emerging technologies of interest to the National Infrastructure Commission in its study on how technology can improve infrastructure productivity[34]. Another example is the *Made Smarter* review that considers how UK industry can benefit from the accelerated adoption of digital technology, including IoT, across advanced manufacturing[35,36]. Its recommendations focus on three areas: adoption, innovation and leadership. It recognises that convergence of IoT with other technologies will maximise impact and that good security, along with other trust-enabling solutions, is vital in ensuring IoT will be adopted by industrial organisations. The AI Sector Deal[37], which aims to boost the UK's global position as a leader in developing AI technologies, is relevant since AI will be a key technology for analysing the large volumes of data generated by IoT. The strategy for robotics and autonomous systems is also relevant as some systems will be enabled by IoT[38].

The potential for the UK to create economic value from IoT and optimise its competitive advantage internationally is of interest across government, including HM Treasury. There is international interest as well. For example, the European Commission has recognised the economic potential of IoT as part of its Digital Single Market Strategy[39]. The Commission identifies the risk of fragmentation of policies across countries that could prevent the creation of a Single Market for IoT, as well as fragmentation between industries as a result of unilateral action that could reinforce silos and prevent the adoption of cross-cutting approaches that promote interoperability[40]. The forthcoming GDPR[41] and the NIS Directive[42] are two major interventions that will help harmonise legislation across Europe. There is also a high level of interest in IoT in countries outside the European Union such as China, US, Japan and Korea[43]. An understanding of the global competition is vital for the UK to establish its own position in a global market.

3. Industrial, public space and consumer applications of IoT

IoT is characterised by a huge diversity of applications that reside in different sectors, with differing technical and social requirements, and necessitating a variety of approaches to policymaking and regulation. Most of its applications can be grouped within three categories: industrial, public space and consumer. Stakeholders that stand to benefit will differ by category: while industrial IoT will result in productivity and efficiency gains for industrial sectors, consumer IoT is expected to enhance quality of life or bring financial benefits to individuals. However, the scale of these benefits have yet to be fully quantified. Public space IoT applications have desired outcomes shared by both industrial and consumer applications. For example, benefits from IoT applied to transport have the potential to impact on multiple stakeholders, including planners, transport operators and the public. For some industrial applications, consumers share benefits too. For example, smart meters – in conjunction with other innovations such as new tariff options – stand to benefit both the energy industry and consumers.

The different categories of application are regulated in different ways. For example, industrial applications are subject to the Health and Safety at Work Act, while public space applications are not. The categories are also served by different commercial players and operate in differing legal and social contexts. Any disputes around the deployment of IoT in different contexts would be need to follow very different paths to resolution. Boxes 2, 3 and 4 describe examples of consumer, public space and industrial IoT applications.

The main differences between industrial, public space and consumer applications are identified in Table 1, although it should be noted that many characteristics are shared across the three categories of application.

Policy objectives for industrial, public space and consumer applications of IoT

Recommendation 1: In developing policy for IoT, DCMS, BEIS and other government departments should distinguish the differing policy outcomes for industrial, public space and consumer applications of IoT. Policy for industrial applications should reflect the need to drive productivity and efficiency as well as threats to national infrastructure, manufacturing capability and safety. Policy for consumer applications should reflect consumer benefits such as improved quality of life but not compromise security or privacy. Policy for public space applications should reflect desired outcomes around both improved efficiency and consumer benefits.

Box 2: Consumer IoT: wearable fitness monitors for a healthy lifestyle

Consumer IoT has a diverse range of applications that benefit the user, both within the home and on the person. One such driver for consumers is to help track and manage a healthy lifestyle.

Wearable fitness trackers such as 'Fitbits' enable real-time activity tracking by monitoring step counts, heart rate, sleep quality and estimated calorie expenditure. Wi-Fi connectivity of such devices enables information to be transferred to cloud platforms and provides user access via computer, tablets and smart phones.

Sharing data on applications such as MyFitnessPal enables consumers to track their food intake, exercise and goals in a single place, bringing together information from multiple sensors such as GPS monitors and internet-connected weighing scales. This allows consumers to review and assess lifestyle changes. Such platforms also act as a social community, enabling consumers to share their progress with family and friends, and compete.

While fitness trackers represent the first step that consumers are taking into wearables IoT, other applications include personal safety wearables, 'exact measure' wearables with the ability to recommend clothing that matches the consumer's shape or 'thermal bracelets' that provide thermal comfort.

The insurance sector is starting to use data from wearable tracking devices to adjust premiums according to the level of physical activity of the insured person. For example, Vitality offers rewards for customers based on their level of activity, as measured by a range of approved tracking devices.

Ericsson Consumerlab (2016), *Wearable technology and the internet of things – consumer views on wearables beyond health and fitness.* https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/wearable-technology-and-the-internet-of-things

IBM Internet of Things blog (2017), Breaking fitness barriers with the IoT, www.ibm.com/blogs/internet-of-things/breaking-barriers/

Vitality, Activity Tracking webpage, www.vitality.co.uk/rewards/partners/activity-tracking/

Box 3: Public space IoT: a green IoT platform for reducing particulate emissions

Several initiatives are being explored for IoT technologies in public spaces to benefit local government and the public. In cities, such as London and New York, benefits include improving traffic flow, reducing pollution and energy consumption, and collecting data for policing.

One example of IoT in a public setting is a green IoT platform project in Uppsala, Sweden. To reduce particulate emissions, the local municipality is driving the implementation of a platform based on open standards, well-defined Application Programming Interfaces and open data. It will enable the testing and experimentation of new sensor technologies, with environmental monitoring used to inform traffic management, and better city planning. A broker will communicate sensor data in an open format for further storage and processing in the cloud, or for direct use by applications and services.

By deploying such a platform, the team in Uppsala aims to generate social, economic and environmental benefits. To help this goal, the platform is demonstrating, and informing guidelines for, the procurement of open IoT infrastructures that avoid vendor lock-in and enable third-party innovation in new services.

Ahlgren, B., Hidell, M. and Ngai, E.C.H., *Internet of Things for smart cities: interoperability and open data,* in IEEE Internet Computing, vol. 20, no. 6, pp. 52-56, Nov.-Dec. 2016.

Box 4: Industrial IoT: improving efficiencies in manufacturing with location tracking

Stanley Black & Decker Inc. is a leading global provider of hand tools, power tools and related accessories. At its plant in Reynosa, Mexico, the company has 40 multiproduct manufacturing lines, thousands of employees, and produces millions of power tools each year.

Working with CISCO, the company deployed Wi-Fi radio-frequency identification (RFID) tags within the plant to enable a real-time location system to track location and status of elements passing through the production lines and the plant. This information was accessible to assembly workers, shift supervisors and plant managers. The deployed IoT solution provided real-time results from good or bad production reports when integrated with quality checkers, such as the weighing of boxed products at the end of production lines, and enabled the tracking of production as it happened. This meant that floor managers were constantly aware of each line's output, and could speed or slow production to meet daily targets. It also indicated how quickly employees were completing their respective stages of production.

The solution provided a 24% increase in overall equipment effectiveness (OEE) on the production line. It allowed faster decision-making because of immediate notifications of any issues. Labour utilisation improved from 80% to 92%, throughput increased by around 10% and there was a 10% reduction in inventory or material holding costs.

Cisco Customer Case Study, *Leading Tools Manufacturer Transforms Operations with IoT,* www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/c36-732293-00-stanley-cs.pdf

SEVERAL INITIATIVES ARE BEING EXPLORED FOR IoT TECHNOLOGIES IN PUBLIC SPACES TO BENEFIT LOCAL GOVERNMENT AND THE PUBLIC THAT INCLUDE IMPROVING TRAFFIC FLOW, REDUCING POLLUTION AND ENERGY CONSUMPTION, AND COLLECTING DATA FOR POLICING.

Table 1. Comparison between industrial, public space and consumer applications of IoT (continued overleaf)

	Industrial IoT	**Public space IoT**	**Consumer IoT**
Examples of sector / application	Energy, other critical infrastructure sectors, manufacturing, mining, construction, healthcare.	Transport (including connected cars), smart cities.	Smart homes, home energy management systems, wearables and fitness trackers, smart locks, smart televisions, smart watches, healthcare.
Beneficial outcomes	Productivity, efficiency.	Efficiency of public services and consumer benefits such as consumer-focused services.	Quality of life, convenience, energy efficiency, health and training improvements, increased time efficiency.
Nature of the technologies[44]	Large platforms often built on evolving technologies, although there is a push towards creating more nimble, flexible IoT solutions for industry.	Large platforms often built on evolving technologies.	Some stable, smaller IoT consumer applications based on mature technologies such as smartphone and web technologies. Other consumer applications use more immature technologies that are inherently vulnerable.
Legacy issues	May be added to complex legacy systems comprising old technologies. Interoperability with existing legacy systems can be expensive, and also creates the challenge of operating within partially trusted environments.	New systems, or added to legacy systems.	Generally new systems, but consumer IoT can also be added to legacy systems.
Scalability[45]	Industrial IoT systems need to be scalable, as they may comprise thousands of devices spread over large distances. Devices may be grouped and connected, and it should be possible to add devices to existing IoT infrastructures without service degradation. However, scalability will be dependent on the availability of communications infrastructure, and its availability cannot always be assumed in the design. Some applications require the ability to transmit large volumes of data, for example, via an existing industrial control system[46]. Other applications may require only occasional transmission of small amounts of data. 'Edge computing' or 'fog computing' capabilities may be required, so that preliminary analytics can be carried out close to where the data is generated, rather than at a central server[47].	Smart city and transport applications are developing 'platform of platform' technologies that allow interoperability between different data platforms, and the sharing of data between many different applications[48].	Some consumer IoT applications have fewer devices and datapoints, so that requirements for transmitting volumes of data are less onerous. Other consumer applications may transmit large volumes of data, such as voice-controlled assistants that send data to the cloud for processing. 'Edge computing' capability may also be required in consumer applications, to limit the connectivity required to transmit data and/or for security reasons. Scalability implies that consumer devices can talk to and synchronise with each other in safe and secure ways, which is a particular challenge in public spaces and large crowds of people.

Table 1 continued over...

Table 1. Comparison between industrial, public space and consumer applications of IoT (continued from previous page)

	Industrial IoT	Public space IoT	Consumer IoT
Communications and power requirements[49]	Sensors may be embedded in remote infrastructure that is physically difficult to access; for example, it may be subsurface, high up, offshore or in desert conditions. Maximum possible battery life is needed, using industrial grade batteries. Energy harvesting could be used to reduce dependence on batteries. New types of communications networks are developing to connect devices to central servers that are better able to accommodate specific power and bandwidth requirements, such as low power. These include LPWAN and NB-IoT[50].	Sensors are embedded in existing city infrastructure – for example, lampposts or other street furniture – or in transport vehicles and trains. Battery life is an important consideration.	Sensors are in easily accessible locations. Cellular networks, WiFi and Bluetooth[51] are more feasible as energy requirements are less stringent, communications distances are small and scalability is less of an issue. Fixed sources of power or conventional, consumer-grade batteries are sufficient.
Resilience requirements[52]	IoT devices and systems may need to survive harsher environments, which may require resistance to high temperatures, corrosion, ingress of fluids. Many industrial IoT devices should have the capability to carry out remote periodic and forced maintenance and control without onsite human intervention.	IoT devices will need to be resilient to the weather conditions as determined by their geographical location. Maintenance of large number of devices by local authority contractors or transport authorities is a challenge.	Resilience requirements are generally less stringent for consumer IoT applications; for example, devices may need to be splash-proof.
Cybersecurity[53]	Potential repercussions may be severe if devices or systems are compromised, hence there are more demanding cybersecurity requirements. There are particular challenges for cybersecurity in integrating IT and operational technology[54]. There are cybersecurity risks from ageing devices that have not been patched or updated, or are unmanaged.	Cybersecurity incidents have implications for safety and privacy of the public, and could have more severe repercussions if systems are compromised. Consequences if smart city interventions designed to improve physical security of the public, such as incident detection, crowd management and smart lighting, are compromised.	Implications for personal privacy and safety. Currently, most consumer IoT systems only need to interface with relatively simplistic control mechanisms on consumer devices. However, in future, some consumer-facing devices such as connected health devices may require more complicated control mechanisms, and security compromises could have a major impact on safety. Healthcare devices such as defibrillators and insulin pumps are already connected and vulnerable. Risk of recruitment of IoT devices for denial of service attacks and other malicious activities.
Safety regulation	In several sectors, regulation requires the development of a safety case; for example, nuclear, chemical, offshore oil and gas, railways and military systems. The Health and Safety at Work Act applies to IoT deployed in industrial workplaces.	Some public space applications may fall under safety case regulation, for example, transport applications.	In many cases, regulation requires a CE mark[55]. This applies to implantable medical devices, toys, hot-water boilers, fridges, gas appliances, electrical equipment. The General Product Safety Regulations 2005 (GPSR) also apply.

4. The IoT policy landscape

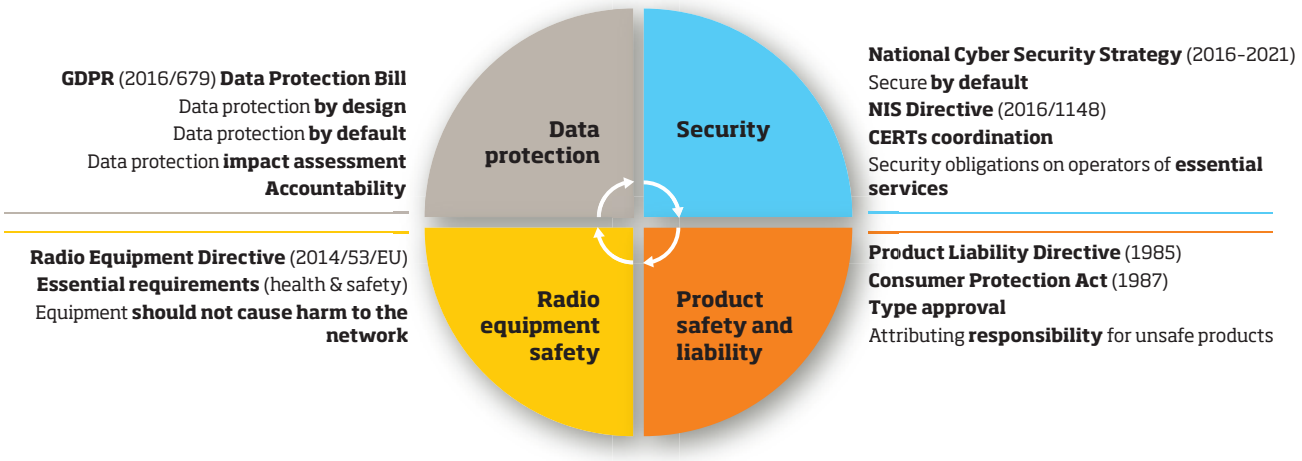
To maximise the IoT's potential to generate social and economic benefits to the UK, while mitigating risks such as possible security vulnerabilities, the government should consider a range of options for policy and regulation. Some existing measures may be adequate to deal with IoT while some unique characteristics of the emerging technologies will require amendments or the development of new policy and governance arrangements. Creating regulation around an evolving technology is challenging, especially in an international context. Addressing the complexities of the global supply chain, data integrity across jurisdictions, and challenges of managing nested liability and consent will demand clarity about implications of IoT for the UK's national interest. If these challenges can be addressed, economic benefits will accrue since IoT standardisation and regulation will help to stimulate growth by accelerating products into the market. Conversely, a lack of suitable regulation or uncertainty for developers about whether systems comply with regulation present a barrier to deployment. Certain IoT solutions will remain illegal until the necessary technologies – for example, privacy-enhancing technologies or security solutions – are developed that enable solutions to comply with regulations. Where regulation is needed, standards should be designed to support the regulator. The regulator will also need appropriate powers to take legal action if regulations are breached.

4.1 Regulation

At present, there are at least four main regulatory frameworks that apply to aspects of IoT, including data protection regulations, security of networks and information systems, product safety and liability laws, as well as radio equipment safety rules (Figure 1, see page 20). Domain-specific legislation is also emerging, such as the Vehicle Technology and Aviation Bill[56]. The main issue is not that IoT is evolving in the absence of rules and regulations that apply to it, but that these regulatory frameworks have developed separately from each other and need alignment in their development and implementation stage[57]. Key questions are whether current regulatory frameworks are sufficient and fit-for-purpose, and how any changes to these frameworks might build on existing regulations for specific sectors and applications.

These regulations set broad principles such as 'data protection by design' and 'security by default', but need translation into clear guidelines and procedures for implementation. The EU's Article 29 Working Party[59] has taken forward the debate on privacy and

Figure 1: Four main regulatory frameworks that apply to aspects of IoT[58]



data protection in emerging technologies, and has defined specific guidelines for implementing the GDPR requirements, such as the steps to conduct data protection impact assessments[60]. It is the role of domestic regulatory authorities – for example, the Information Commissioner's Office or OFCOM – to clarify these and monitor their implementation. Regulatory authorities need to clearly outline and communicate the extent of their responsibilities with regard to the implementation of these rules and how their remits align.

Regulatory alignment has an international dimension too, given the global supply chains for IoT products and the increasing requirement for transnational collaboration in critical infrastructure risk assessment and management, as seen in the NIS Directive. As governments are increasingly considering the adoption of new laws for ensuring a responsible level of IoT cybersecurity, such as the proposed Internet of Things Cybersecurity Improvement Act of 2017 in the US[61], they must also consider the effects of domestic legislation on the international economy and foster international collective action on IoT security.

One challenge is the regulation of network infrastructure for IoT. This infrastructure includes a variety of networks with different configurations and properties, such as cloud and local networks, and public and private networks. The requirements of any given application will partly drive what types of networks are used. For industrial IoT applications, private networks may be essential to ensure quality and timeliness of communication, which is less easy to achieve on public networks. In general, public communications networks and services are regulated, while private networks are not. However, it is possible for public and private networks to share common carriers. The infrastructure's complexity means that there is a risk of regulatory fragmentation and a variety of governance models, with subsequent risks to adoption and the successful creation of business propositions.

There are also challenges around how current regulatory frameworks for data protection and risk management apply. In the case of industrial applications, many different entities own and govern IoT systems that may be complex, distributed and made up of heterogeneous elements, both local and global. It will be a challenge to delineate clear rights and responsibilities between the private and state actors that form the distributed ownership and structure of IoT systems, especially as various actors may have different, unaligned objectives. A further challenge is that organisations may cease to exist in the future, leaving IoT devices online without support. The challenges for data protection, including uncertainties that result from the complexity of IoT systems, are discussed in Section 6.3.

Aside from the regulations that affect the movement of personal data, there are also factors that limit the free flow of non-personal data such as machine data or non-personal transactional data. These may be data localisation restrictions that stem from legal rules, administrative guidelines or practices that dictate or influence the localisation of data for its storage or processing and prevent the free flow of data across borders[62,63]. There may also be contractual barriers that tend to limit re-use of data or sector-specific restrictions.

4.2 Standards

The Blackett review identified that a key uncertainty is the lack of dominant standards to enable a framework for openness, interoperability and security. IoT has evolved from many technologies and domains, resulting in standards that cover individual devices, communications or cloud services rather than an entire IoT system, which could adversely affect openness, interoperability and security. Several competing industry alliances are now developing standards, with corresponding risks. For example, it may be prohibitively expensive for SME innovators to differentiate between these standards and navigate such a complex space. There is a risk that this market competition will drive the adoption of weaker standards[64]. Conversely, premature technical standardisation could constrain innovation and prolong standardisation competition between industry alliances or domestic/regional standardisation organisations.

Standards for technical interoperability are needed at many levels, including device, network, platform, cloud and data levels. Standards for ensuring security and privacy are also vital: end-to-end privacy and security needs coherent privacy and security safeguards for each component as well as between components. Organisational and management standards are also required. In future, human-computer interface standards for voice and sight will emerge, as will ethical standards[65].

Standards that promote interoperability will help develop networks of users, increase the variety of system products and boost efficiency in the supply chain, with corresponding economic benefits[66]. Data standards preserve the meaning of data generated by IoT and the context in which the data originated[67]. Without

AT THIS STAGE THERE ARE ONGOING DEBATES ABOUT WHETHER THE CURRENT MIX OF STANDARDS CAN RESPOND TO INTEROPERABILITY, PRIVACY AND SECURITY CHALLENGES

standards, there is a risk that a lack of interoperability will lead to a proliferation of bespoke systems, which will allow vendors to lock in customers and act as a barrier to new market entrants. Businesses may choose standards based on immediate availability rather than quality, with subsequent risks such as direct business loss, indirect decrease of market value and customer loyalty, and costs related to legal liability. A standard's success will depend on factors such as its ability to promote or stifle innovation, facilitate market growth, increase transparency, and reduce monitoring and compliance costs.

Standards and requirements may be specific to a particular industry sector, such as healthcare or transport. Within industry domains, standards may be easier to achieve and agree as they would apply to a smaller group of market players and a well-defined IoT ecosystem, as seen for instance in the security standardisation efforts of the Industrial Internet Consortium (IIC)[68] .

Voluntary standards for IoT are emerging ahead of formal standards, since the latter take longer to develop, agree and institutionalise. Given the wide application scope of IoT, this is leading to fragmentation, which manifests itself in at least two ways. Domain-specific standards are evolving such as semantics and interoperability standards, for example, for smart city applications. At the same time, industry alliances and organisations are putting forward a considerable number of good practice principles and standards for data integrity, security, trust and resilience of IoT systems (such as the IoT Security Foundation, GSM Association, Online Trust Alliance, Open Connectivity Foundation (OCF))[69].

Also, increasingly, industry associations are putting forward their own voluntary testing and certification schemes, such as the OCF IoT Certification Program[70] or the BSI IoT Assurance Programme[71], which may lead to duplication of efforts rather than convergence. However, the proposed EU cybersecurity certification scheme may form the basis for future international discussions on trust and standards in this space, and could lead to a collectively agreed baseline for IoT security[72]. While the certification scheme is at a proposal stage and meant to be of voluntary nature, the planned scheme is set out to provide security provisions across the entire lifecycle of, for example, IoT products and services and would require formal standards to be set in place.

At this stage, there are ongoing debates about whether industry and the policy community should promote domestic, regional or international technical standardisation of IoT, and whether the current mix of standards can respond to interoperability, privacy and security challenges. Furthermore, it is uncertain whether voluntary standards will be sufficient, or whether there is a need for formal standards, supported by new regulatory frameworks such as the European Commission proposal for a cybersecurity certification scheme. Given the global nature of the supply chain, the debate about the geographical reach of standards and their possible impact on international trade is vital. Industry or specific industry sectors will drive the emergence of reference architectures[73] , and it is unlikely that either governments or standards bodies will have significant influence over these.

4.3 The international landscape

While establishing a UK approach to the cybersecurity of IoT is essential, the nature of these challenges is that they are not contained within state borders but rather, require international coordination and collaboration. There has been progress at an international level on technical aspects by organisations and groups such as ETSI Smart M2M, ITU-T and International Energy Research Centre (IERC) European Research Cluster on IoT. In addition, there are several public-private arrangements for information sharing[74] as well as the Computer Security Incident Response Team (CSIRT) community that works collectively to mitigate against cybersecurity vulnerabilities as they arise.

However, there is a lack of global coordination at a political level. Ongoing disputes about data jurisdiction, the application of international law in cyberspace, and conceptions of sovereignty continue to impede progress on international political agreement on what constitutes responsible state behaviour in cyberspace[75]. The inability of the 2016–17 UN Group of Governmental Experts (UNGGE) to deliver a consensus report highlights the challenges of international coordination that will become further complicated by IoT. How and where these issues are taken up will be of significance to every state and the UK government is well situated to shape this.

As it did with the 'London Process[76]', there is an opportunity for the UK to coordinate and shape debates about international cybersecurity policy in the context of IoT. There is a lack of focus and leadership in key international organisations on these matters, where legacy cybersecurity concerns continue to drive discussions. International policy coordination and cooperation will be essential to guide the advancement of norms and agreements that will be necessary to ensure a safe and secure IoT. The World

A SYSTEMS APPROACH WILL BE NEEDED IN POLICYMAKING TO HELP CAPTURE THE INITIAL COMPLEXITY AND KEY RELATIONSHIPS, ENSURING THAT DIFFERENT ELEMENTS OF POLICY AND REGULATION WORK TOGETHER AS A COHERENT WHOLE.

Economic Forum has taken early initiative and may be one forum where relevant players will unite on IoT security[77]. This, together with the OECD and potentially the WTO, would be the best routes through which to influence the international agenda. A deeper understanding of the structures of these forums, along with a clear understanding of the current and future marketplace over the next five years, is going to be essential to securing the UK's interests.

The challenges of policy and governance in IoT are significant and research into possible solutions, interventions and best practice is taking place in parallel, without consultation or collaboration. However, the policy community can learn from the work of international bodies on technical issues, which itself has important policy implications. To maximise research outputs and minimise duplication of efforts in this demanding area, academic, security and policy communities need coordination through focused conferences, themed meetings and working groups, which will help form an international IoT policy research community. This initiative would present an opportunity for UK leadership and has implications for the development of important capacity-building measures that will be essential to developing global IoT security policy solutions.

4.4 The road ahead

A systems approach[78] will be needed in policymaking to help capture the initial complexity and key relationships, ensuring that different elements of policy and regulation work together as a coherent whole. It will facilitate a joined-up approach across government and other stakeholders. The standards, policy and regulatory communities will need to work together to develop an approach to regulation and governance of IoT that best promotes the values and interests of the UK in a global context. There will need to be new mechanisms, and perhaps new regulatory frameworks, for cooperation between sector regulators. There should be a two-tier approach that addresses what can be done at a national level, and how this connects with work at an international level. A systems approach should consider adaptive methods to governance and regulation of IoT to ensure that regulation keeps up with the fast pace of technological development[79]. Adaptive approaches should draw upon continuous cross-domain policy learning by monitoring the adoption and implementation of data protection and cybersecurity guidelines and standards, and by establishing policy reviews and potential sunset clauses[80]. Clear communication strategies with stakeholders will be essential.

A systems approach recognises IoT as a complex, socio-technical system where social and technical aspects interact, affecting the desired outcomes of openness, data integrity, security and interoperability. Given the complexity of IoT, this systems approach cannot rely on a single policy or regulatory intervention, but on a complex co-regulatory model that is likely to combine mandatory rules for data protection, network and information security, product safety and risk management with voluntary guidelines, codes of conduct and standards[81]. It is likely that current legislative and regulatory frameworks will require more careful alignment to respond to the societal challenges of this evolving technology, rather than the introduction of IoT-specific legislation.

A fully coordinated approach will require government to have strong oversight of the policymaking process, to take on a convening role for the many stakeholders involved and develop ways of enabling cross-departmental working. Government should also have a strong international focus and address issues around establishing and regulating both national and international markets. There is an opportunity for the UK to contribute to, and where appropriate lead, the development of an international harmonisation of standards and governance of IoT. Other aspects of coordination could include facilitating public and private sector cooperation and providing oversight on funding and support for new technologies.

GOVERNMENT SHOULD BRING TOGETHER STANDARDS, POLICY AND REGULATORY COMMUNITIES TO DEVELOP AN APPROACH THAT PROMOTES THE INTERESTS OF THE UK IN A GLOBAL CONTEXT.

Governance and regulation – a heterogeneous approach

Recommendation 2a: The IoT agenda – encompassing industrial, public space and consumer applications – should have a recognisable home within government. That part of government should take a leadership role in coordinating policy across departments and internationally, and in using government's convening power to bring the relevant stakeholders together. As part of a systems approach to policymaking, government should have strong oversight of IoT policymaking activities and of the various stakeholders that need to be involved in developing policy. This will help develop the combination of regulatory and non-regulatory measures required to ensure that IoT systems underpin a secure and trusted future.

Recommendation 2b: Stakeholders involved in governance and regulation of IoT, including government departments, regulators, standards bodies and industrial alliances, should collaborate to identify points of commonality between sectors, while distinguishing sector-specific requirements for governance and regulation. They should work together to develop common approaches to governance and regulation across sectors, where possible. These approaches should have flexibility to accommodate the applications that might emerge in the future. Government should coordinate activities between sectors. The market is very fast-moving, driven by business need and business opportunity. It is therefore important to ensure that the main players – for example, the major device manufacturers and network providers – engage in these activities.

Recommendation 2c: Government should continue to facilitate the development and deployment of standards for IoT where needed, building on progress to date. It should use its considerable convening power to bring together standards, policy and regulatory communities to develop an approach that best promotes the values and interests of the UK in a global context. Government should actively support UK national standards bodies in leading on the development of international standards, including coordinating and funding UK delegations. The BSI's Publicly Available Specification (PAS) is one mechanism that can increase the tempo of standardisation and promote UK interests. To maximise expert involvement in standardisation and ensure independence from individual industry lobbying, the government should fund academics' participation in IoT standardisation and ensure that involvement brings credit in research impact assessments.

Recommendation 2d: The UK government should work with other governments and international institutions – with the main providers of IoT components, devices and systems – towards 'umbrella agreements' that set out an international baseline for IoT data integrity and security for all parties to adopt. This will support the international supply chain in offering products and services globally.

Building capacity and coordination in cybersecurity policymaking and governance

Recommendation 3a: Existing UK cybersecurity capacity-building initiatives should be expanded to include IoT policy support for states without the research capacity to address these challenges. Existing policy-relevant research should be coordinated and disseminated through the establishment of an international IoT policy research community.

Recommendation 3b: The UK government should exercise its leadership to begin discussion on how it will integrate IoT into current international political negotiations over global cybersecurity.

5.

Theme one: harnessing economic value

5.1 Context

Several industrial sectors have established mature business models and successfully adopted IoT, particularly where the economic benefits of implementing IoT are clear. One example is the mining sector, where the benefits of adopting IoT include improved efficiency, safety, maintenance and quality. It is estimated that the value added of IoT in mining and resources will be $370 billion per year by 2025[82], and it is expected that 90% of the value will accrue to the users of the technology rather than the developers[83]. Another example is the aerospace sector, where the monitoring of aircraft engines has allowed Rolls-Royce to develop new services around its products, improve reliability, predict when maintenance interventions are needed, and improve long-term business forecasting. As a result, reliability across the fleet of engines has increased by 73% over a decade[84]. Early deployment indicates technology brings benefits when used in a straightforward way to address known business-critical needs, for example the use of IoT sensors and predictive analytics to optimise large aircraft fleet and drive down maintenance costs[85].

Once initial barriers to adoption are overcome, other industrial and business sectors also stand to benefit from adopting IoT through increases in productivity and efficiency, and the adoption of the technology is predicted to grow rapidly[86]. Manufacturing, smart cities and healthcare are areas that all expect growth[87]. The World Economic Forum[88] has also identified a number of specific opportunities for IoT, which will increase productivity and create more engaging work. These include supporting the emergence of the 'outcome economy'[89], the creation of new connected ecosystems that cross traditional industry boundaries, and collaboration between humans and machines.

The economic benefits resulting from consumer IoT deployment are less well-defined, although there is potential for consumers to benefit from a wide range of new products and services[90]. These include services that are responsive to individual user demands, quicker responses by goods and service providers when faults or deficiencies are discovered, remote fixes to update security or address identified faults, greater convenience, decision-making support, better allocation of resources, and remote control of home services when not physically present.

MANY IoT BUSINESSES STRUGGLE TO IDENTIFY IoT DEVICES OR SERVICES THAT COMPLEMENT EXISTING SERVICES, SUCH AS DOMESTIC IoT APPS USED WITH A SMARTPHONE OR TABLET, THAT COULD CREATE VALUE AND DRIVE GROWTH FOR THEIR CORE BUSINESS.

A strategy for IoT

Recommendation 4a: As part of its leadership role, government, working in partnership with industry, should develop a clear strategy for IoT. The strategy should align with related strategies around digital technologies and encourage innovation, commercialisation and adoption of the technologies, and stimulate the development of the UK's industrial IoT ecosystem. The strategy should recognise IoT as a socio-technical system, with a focus on people, data and processes in addition to the technologies that underpin the development of products and services. It will need a systems approach to tackle the complexity and interdependent nature of the challenges. This links to Recommendation 2a, which advocates the adoption of a systems approach to policymaking.

Recommendation 4b: Government should commission an ongoing review of best practice at both a national and international level to consolidate knowledge about how IoT solutions have been realised in industrial, public space and consumer applications and inform how testing, deployment and implementation of IoT in the UK can build on best practice. This is pertinent across all areas of IoT but particularly important in security, and in understanding how best to balance risk and reward in IoT implementation and how they are shared between stakeholders. The review should include the use of existing or new, innovative business models. Detailed information about the approach that a specific industry can take to adopt IoT in their upstream and downstream processes would also be of value.

An infrastructure roadmap

Recommendation 5: Government should commission the development of an infrastructure roadmap for IoT that will feed into the National Infrastructure Delivery Plan. This will provide valuable information for developers and operators of IoT infrastructure, as well as for device and system manufacturers that will require connectivity from IoT infrastructure.

5.2 Challenges

5.2.1 Business models

Development of business models

The Blackett review identified that there were relatively few established business models for achieving profitability for businesses that might consider integrating IoT into products and processes. The review also commented on the challenge for both government and large businesses of making use of the volume and variety of data generated by IoT.

Three and a half years on from the publication of the Blackett review, new business models continue to be scarce in many areas because of outstanding technical, ethical, business and other challenges, and many organisations lag those in leading sectors that have successfully established business models. Many current business models in the IoT space are empirical[91] or conceptual[92] in nature. Black market business models are also emerging that use technology to circumvent standard pay models – the Kodi App is a key current example that makes use of smart devices[93]. A legal application that can be loaded with additional plugins to allow streaming of video without payment, this has had a notable impact on Sky Television[94]. As service-based models are increasingly introduced around data and IoT devices, then increasingly there will be devices to avoid payment. This may not be new to technology but the mass adoption of Kodi boxes in the consumer IoT space is of note and should be highlighted as a threat to future economic models.

There are several reasons for the slower development of business models in areas that are less high-value. One reason is that the new product development process for IoT is not mature and therefore the ability for organisations to develop strategy and business models is in a similar position. This is a particular challenge for new and small businesses targeting lower-value markets that may be in their infancy and volatile. Many IoT businesses struggle to identify complementary goods – IoT devices or services that complement existing services, such as domestic IoT apps used with a smartphone or tablet – that could be commoditised in order to create value and drive growth for their core business. Commoditisation will depend on the sustained commercial success of a product or service over a period of time. Another reason for slower development of

business models is that the deployment of IoT technologies in some applications may require a large upfront investment, without certainty about the return on investment. The current work on pricing models for IoT applications is developed for segments of the IoT architecture and focuses either on rather particular service configurations or on generic representation of functionalities, which does not support real-life end-to-end business models. The challenge of accurate economic costing is discussed further in the next section.

A situation where many large IoT businesses are in competition and positioning themselves in various business alliances also impairs the quality of business models. In addition, while the increase in venture capital funding is welcome, startups receiving this funding can make losses for several years. Therefore, even those who survive do not rely entirely on the success of their business models during this time. This situation is a consequence of a new politico-economic environment, characterised by new ways to distribute risk and a pressure to constantly push technology forward. Furthermore, a bottom-up appetite for data rather than a top-down quantified need drives IoT deployments in certain situations, and struggles to find ways to make use of the data that has been collected.

The adoption of IoT consumer products and services brings unprecedented changes to people in terms of autonomy and dependence, privacy and sociality, with resulting social, cultural and economic effects. Traditional businesses know how to shape their products or services in a way that is sensitive to the diversity of social and cultural contexts, or they go on and create new business propositions that respond to new social and cultural contexts to maximise success in the market. However, many customer IoT solutions are levelling in scope across populations, pose important issues in terms of safety and consent, and social inequality. There are also critical ethical questions about the fairness of business models that are based on the exchange of personal data.

Societal and personal approaches to risk, which influence how risk-adverse individuals and organisations are, will affect willingness to adopt IoT. To benefit from IoT, industry will have to accept a certain level of risk and will benefit from becoming more agile and less risk-adverse. For example, a reticence to adopt cloud services could limit the power of IoT. UK consumers have shown a willingness to adopt online shopping, for example, and have embraced it more wholeheartedly than other nations; whether the same is true for adoption of IoT remains to be seen.

Challenges of accurate economic costing

IoT involves the addition of physical components and is costly to develop, roll out and maintain when compared to social media and similar platforms. The cost of developing, implementing and maintaining complex IoT products, services and infrastructures can be difficult to quantify accurately and can vary significantly with customised solutions producing a key barrier to developing successful business models. There may be uncertainties, such as the required resiliency or the level of response to emerging security threats, that make costing a challenge. Initial savings from IoT forecasted by market researchers do not fully consider the challenges of permanent monitoring and constant updates, a real departure from the old paradigm to 'write, deploy and run ICT systems'. Industry and market analysts are aware of these issues but there is little evidence that might help to address them.

There is considerable uncertainty around the costs involved in implementing specific parts of systems, such as sensing, actuation, and the capture, storage and processing of data. Further uncertainties arise where IoT systems are in use alongside legacy systems or where they replace them. There is pressure to keep costs down while, in reality, they could escalate considerably. For example, the cost of replacing an inexpensive battery in a field-deployed device may be many times greater than the initial cost of the battery. The commodity hardware used in many consumer IoT devices is unlikely to be sufficiently dependable for use in industrial applications, particularly given the high costs of replacing deployed components. Consequently, IoT devices developed for industrial applications are likely to be costlier than consumer devices. There are unassessed costs in key economic areas for the UK economy, such as in infrastructure monitoring, and there is no established risk-assessment methodology for cybercrime economic costing[95].

In future, the value to IoT businesses potentially lies in the data services that they can create, going beyond simply the provision of IoT infrastructure. Again, the costs of ensuring that businesses can usefully analyse the data captured while securing end-to-end security, privacy and other social, cultural, and ethical commitments is unclear. Realising the potential value in the market place and the broader economic, social and environmental value is a further uncertainty.

5.2.2 Adoption, implementation and interoperability challenges for industry

Adoption and implementation

A major barrier to adoption in industry is the lack of awareness and knowledge about how IoT can benefit organisations and how to go about adopting and implementing IoT. Technology selection is a challenge for organisations. Measures that build the IoT ecosystem or enable 'matchmaking' between industry and suppliers of IoT products and services will help to address this barrier.

There is still considerable scope for improving the way in which IoT technologies are designed and deployed to be useful to industrial sectors. While cheap and scalable solutions are possible due to the low cost of hardware, there are still many challenges for IoT providers in ensuring that systems are secure, safe and reliable, as well as commercially viable. Cyber attacks such as the recent Mirai botnet attack[96] show that the model of low-cost, low-security IoT solutions is not sustainable. Furthermore, business models that do not factor in GDPR compliance may be at risk of failure, putting both companies and users at risk.

Industry faces the challenge of how to introduce nimble, flexible and scalable IoT solutions to tackle key problems, without constraint from massive and unwieldy non-interoperable platform architectures. Startups may not consider whole ecosystem implications, so ensuring flexibility in the application of their products is an important consideration. A potential solution may be to use an object-oriented architectural approach in which different components of the architecture deliver different IoT services. This approach would result in a more lightweight architecture and would reduce the time to market. Industry 4.0 is trying to facilitate a similar approach through its 'administrative shell' concept, which aims to create a digital representation of all the information available about an object, thus allowing smart industrial devices to communicate and understand each other[97].

All major systems integrators are developing IoT-capable management tools that allow faster development of business solutions and increased efficiency to meet the needs of potential new markets. These include, for example, Microsoft's Azure IoT Suite, IBM's Watson IoT platforms, Verizon's ThingSpace and Cisco's Jasper.

Industry can learn lessons about how key sectors in other countries are applying IoT technologies and how these systems

HARNESSING ECONOMIC VALUE FROM IoT PLATFORMS WILL REQUIRE A BUSINESS ECOSYSTEM IN WHICH BUYERS, SUPPLIERS AND MAKERS OF RELATED PRODUCTS OR SERVICES JOINTLY PROVIDE A VARIETY OF APPLICATIONS, PRODUCTS AND SERVICES TO END-USERS AND EACH OTHER AND IN WHICH DATA CAN BE BROKERED AND SHARED.

are creating value. It would be useful to know about the way in which IoT systems have been designed and deployed, the associated economic costs and benefits – where these can be identified – and the technical and social outcomes, so that testing and implementation of IoT in the UK can build on international best practice.

Interoperability and the development of business ecosystems

IoT will include many systems that only connect to and interoperate with specific devices. There will also be systems that discover devices within range or connected to the same network and that exploit services on those devices, benignly or malevolently. Ideally, there will be standard architectures, protocols, and policies that make it cheaper and quicker to design and build IoT systems from standard components. These components may be hardware or software or both. They may range in complexity from individual transducers and simple sensor modules through to complex subsystems that control many devices, log and analyse data, prepare reports, and apply local legal frameworks, such as GDPR, at the boundaries of jurisdictions.

Harnessing economic value from IoT platforms will require a business ecosystem in which buyers, suppliers and makers of related products or services jointly provide a variety of applications, products and services to end-users and each other. Such platforms would be easily expandable and provide incentives for developers' contribution, promoting bottom-up development of the ecosystem[98] by allowing others to have access to what is already there and to build on top of it. This will prevent fragmentation of the ecosystem and maximise economic value.

This approach may provide commercial benefits to companies. An integrated solution, including data analysis, model development, model maintenance and integration with third-party products and applications, could be prohibitively expensive compared with the use of open standards and interfaces that enable a greater diversity of providers. While large providers may compete to provide integrated end-to-end solutions[99], technology startups will tend to promote more open-access and lower quality or free services. Ideally technology startups should be able to focus on what they do best – for example, developing new sensors or analytics – without concern about how they integrate with other parts of the IoT system, in whatever context they are deployed. One challenge is the support that startups might need to become part of the IoT ecosystem and how they can link up to a customer base with low risk for the customer.

IoT marketplaces

The creation of standardised and dedicated IoT marketplaces[100] can boost economic value gained from IoT, but there is a lack of established IoT marketplaces. These marketplaces allow businesses to access emerging technologies more easily. Telus[101] and ThingWorx[102] are two examples of such marketplaces. Standardised and dedicated marketplaces can disseminate IoT innovations, increase trustworthiness and adoptability of IoT solutions, and therefore create new horizontal markets and define new value points and market values. There is a view that IoT marketplaces might operate more effectively if they were sectoral rather than generic, although the deployment of IoT across sectors, such as transport and health or between public and private domains, may result in greater innovation and efficiency.

Integrating digital products into industries

IoT has potential to impact upon business operation across many industrial sectors. It requires the dynamism of the IT industry to be brought together with particular dynamics in other domains, which may have longer cycles and different requirements. Domain expertise is vital for identifying whether IoT is a suitable solution alongside alternative approaches, and how it might be used in a particular context. New risk-assessment approaches and combinations of interdisciplinary expertise may be required. For example, embedding 'risk engineering' in the design and development of future IoT systems and evaluating it throughout their entire service lifecycle would represent an important alternative to reactive cybersecurity[103].

5.2.3 Data management and data sharing

Improving data management

There is a lack of data management in many IoT architectures. The design approach for IoT architectures tends to focus on technology and interconnection rather than the integrity of the business or operational process. This approach could limit the usefulness of the data generated and the creation of business applications. To maximise economic value, organisations must first identify the business needs that require data and then specify the requirements for data management accordingly. There is a need for culture

change to improve the way data is governed and used and to recognise data as an asset[104]. However, it also needs recognition as an expensive responsibility as the costs of secure data management become better understood[105]. Currently in industry, a large amount of resources is spent getting the data in the required form to make it useable, so there is considerable value in finding methods to reduce this.

To be able to judge the quality and integrity of data, organisations must be able to understand the provenance and creation of data. Data quality is influenced by several factors that include bias, timeliness, granularity, the quality of metadata and the possibility of calibration error[106]. There is a need to understand metrology and the use of metadata better. Data integrity – including accuracy and consistency – could be compromised intentionally or unintentionally without the knowledge of the data recipient, the data controller or the data processor[107].

The use of data standards could be of benefit, where they do not hinder the market. However, the co-existence of legacy datasets and systems will continue to raise problems here. Some standards already exist, but are sector-specific and have not been widely implemented[108].

Improving data sharing and trading

Access to high-quality data from different sources, sectors and organisations is a key challenge, and necessary in realising the value of IoT. The reluctance of companies to share data that they perceive to be commercially sensitive is widely recognised[109]. IoT data marketplaces provide a means of using the large volumes of data generated by IoT, and connect providers and consumers of data[110]. There are challenges around creating such marketplaces because of the difficulty of creating clear contractual agreements regarding ownership, use of the data and the allocation of value, and legal and regulatory issues around what data can be shared[111]. Several emerging platforms are developing architectures that allow organisations to retain ownership of their data and specify who uses it and how[112]. Business models for third-party organisations who broker searchable data, provide cleansing or analytics services, or other data services, are also emerging.

Ownership of rights in data allows businesses to prevent others copying it or lets them charge revenue for its access[113]. In the context of complex systems that characterise IoT, it can be difficult to identify who owns data rights, as data may be collected and analysed as a collaborative effort. For example, it may be unclear whether data generated by an implantable health device belongs to the person in whose body it is implanted, the manufacturer of the device, the doctor responsible for the patient's care, the service that handles the data or some other actor. Similarly, there is a question over who owns energy data used to monitor the performance of buildings[114] and who owns data generated by connected cars[115]. A European Commission study on free flow of data is exploring the legal uncertainty surrounding data ownership[116], which acts as a barrier to the flow of data.

Many consumers are not aware of the economic and social implications of sharing their personal data, although attempts to clarify these should help[117,118]. Trust and consumer loyalty relies on ensuring that stakeholders hold a balance of individual, corporate and broader social benefits from data. There is some evidence that the public is willing to share personal data with companies to get a better service[119], but in many instances asymmetries still exist between organisations and consumers so that the organisation has a much better idea of how it can benefit from data than the consumer. For example, consumers will be aware that data from smart meters can help them reduce energy costs, but may not know about the myriad ways in which the utility company can make use of the data. The growing realisation that current arrangements do not allow individuals to exercise appropriate control over their personal data has led to research into platforms[120,121,122] that allow them to control data securely, make data available as they see fit with safeguards, and benefit from sharing their personal data more directly and in a more equitable relationship.

5.2.4 Infrastructure, design and power challenges

Challenges for digital infrastructure

Currently, there is strong competition in IoT centered on innovations in technologies such as devices, sensors and wearables, as well as innovations in data collection and management, and cloud services. Less resource is used to improve infrastructure. Smart home IoT systems are built on the erroneous assumption that all consumers have high-end broadband. Where smart home systems become part of a national plan – for energy saving for example – then design assumptions need to be more realistic to cover most the population. To realise the full potential of IoT, the infrastructure – for example, last mile solutions, wireless technologies, communications protocols and backbone services – requires improvements.

Good design

Good design is the underpinning element that brings together technology, human factors and standards. The consumer IoT landscape is currently overly complex with devices requiring a level of technical knowledge often beyond the standard consumer. This is a limiting factor in the current adoption of IoT technology, especially within the smart home market. Installing smart devices is becoming an emerging 'service' with Nest, which sells a range of products including security cameras, smoke alarms and monitoring systems, being an early example. For example, Nest runs a 'Nest Pro' network of installers, providing a service to install Nest thermostat controllers to a boiler system since this involves hard-wiring of the controllers to the boiler system. The level of service required for other aspects of consumer IoT indicates that it is beyond the current consumer level of plug and play and is a restriction to adoption.

A responsible approach to design would help to ensure that IoT systems and devices are created that benefit individuals and society, and are designed with operation, maintenance, modification and end-of-life in mind. Designers can learn from the ideas of responsible research and innovation research programmes[123,124], which bring together stakeholders, such as researchers, citizens, policymakers, business and third-sector organisations, to better align both the process of research and innovation and its outcomes with the values, needs and expectations of society.

Alternative methods for powering IoT devices

Minimising environmental impact is another dimension of good design. The environmental impact of many billions of devices requiring battery power could be very large because of the difficulty of disposing of batteries in a safe way. A further difficulty is that battery-powered devices are susceptible to power failure with ensuing implications. An alternative approach is 'energy harvesting', where ambient energy sources such as vibration, light or warmth are converted into electrical energy. Developments in energy-harvesting technologies are making their use in IoT devices such as wireless sensors increasingly viable.

THERE IS A REQUIREMENT FOR PEOPLE WHO CAN IDENTIFY OPPORTUNITIES FOR USING IoT IN BUSINESS. IN ADDITION TO TECHNICAL SKILLS, OTHER IMPORTANT SKILLS INCLUDE DESIGN, STRATEGIC PLANNING, LEADERSHIP AND CHANGE MANAGEMENT.

Overcoming technical and business challenges

Recommendation 6a: UKRI should provide funding for interoperability demonstrators, including the necessary security controls, data and platforms. These demonstrators should be developed alongside the recommendations on standards (2c and 8a) that are central to achieving interoperability. They could be implemented as part of the *Made Smarter* review that recommends setting up large-scale demonstrators within Digital Innovation Hubs. Funding for interoperability demonstrators for health, energy and transport would help to address the Grand Challenges identified in government's industrial strategy White Paper. In addition, the Catapult network should pursue actions to explore ways of incentivising and facilitating the controlled sharing of proprietary data, building on early exemplars from the UK and abroad. UKRI should promote the best practices defined in guidelines and regulations while encouraging the use of available services, toolkits, open source software and open application programming interfaces (APIs) to exploit IoT opportunities.

Recommendation 6b: As part of the knowledge transfer initiatives in Recommendation 4b, conferences, exchange schemes and networks should target business and industry leaders – CEOs and board members. This will enable knowledge transfer about the culture change needed to bring about the effective adoption of IoT and transform companies' approach to protecting and using data. It would also help to develop the emerging industrial IoT ecosystem and support adoption (this links to Recommendation 4a).

5.2.5 Education and skills

The employment landscape and education

The economic benefits of IoT will be optimised if the UK has a workforce with the necessary skill set. However, the science, technology, engineering and mathematics (STEM) skills pipeline remains a fundamental challenge, which needs to be addressed at all stages of the education system. Schools must provide strong foundations to create the specialists needed for the emerging IoT ecosystem. The Blackett review recommended that the maths curriculum in secondary school should move away from an emphasis on calculation *per se* towards using calculation to solve problems. In addition, teaching of the underpinning principles of mathematics and the development of computational thinking in primary and secondary school level are required.

The government's commitment in the industrial strategy White Paper to improve computer science in schools is welcome[125]. This includes investing £84 million over the next five years to deliver a comprehensive programme to improve the teaching of computing and drive up participation in computer science. An increase in the number of suitably skilled computer science teachers is vital, since computing education is currently 'patchy and fragile'[126] across the UK. The new national computing curriculum is welcome as it now covers computer science in addition to information technology and digital literacy[127]. However, the decision by government to withdraw ICT at GCSE and A level has in effect made computer science a specialist subject for a minority of pupils, with the risk that an insufficient number of school leavers have the necessary digital skills to support delivery of the UK's industrial strategy[128].

For the higher education sector, curricula should be designed to address the needs of the market in order to ensure a suitable and sustainable workforce with high-level, specialist knowledge. For example, UCL's Future Living Institute[129] is strongly cross-disciplinary and focuses on the establishment of IoT skills, from building devices to the deployment and development of new economic models. While the UK university system is generally strong on teaching computer science, there tends to be much less emphasis on computer systems engineering in comparison to other countries such as the US. Many of the relevant skills are focused in electrical and electronic engineering departments, but are variable as they depend on the particular skills of the academics employed in these departments.

There is a requirement for people who, although not technical experts, can identify opportunities for using IoT in business. An engineering domain that adopts IoT will require digital, IT and engineering cross-disciplinary expertise. In addition to technical skills, other important skills include design, strategic planning, leadership and change management. A major transformation of the professional education landscape will be required and is expected to prioritise the education of people with the ability to lead or be part of cross-disciplinary teams. The support of the social sciences in tackling the evolving socio-technical challenges will also be increasingly important. Career pathways will need to be updated.

Technical and data literacy are important areas to focus education on across the spectrum of business, developers and users. They

will need to be able to understand the potential and limitations of data, including the risks of dependence on data and the use of data in artificial intelligence and machine learning. Technical and data literacy should be addressed in schools, and in accessible ways – such as television, courses and websites – for adults. It should be taken as seriously as the 3Rs since it is vital that a broad population with these skills is available to support industry and other economic activity.

Upskilling is one of the main challenges for industrial applications of IoT. The scale of the upskilling requirement in industry is reflected in the *Made Smarter* review, which recommends that one million industrial workers should be reskilled or upskilled over the next five years to enable successful exploitation of digital technologies. Further education aimed at developing IoT capabilities should be appropriately tailored to reflect sector- or application-specific needs.

The Cyber Security Body of Knowledge project, sponsored by the National Cyber Security Centre[130], will provide exemplar learning pathways relating to education at different levels. Its scope includes cyber-physical systems and IoT, and there is potential to develop education guidelines around the privacy and security of IoT.

Existing initiatives and strategies will need to be updated. It is vital that digital skills programmes promote inclusiveness[131]. Early findings from PETRAS indicate that UK initiatives remain too England-centric, find implementation in urban rather than rural contexts, and are often exclusive to UK citizens. Additionally, the persistent gender imbalance of the tech industry is of pressing importance, with persistent challenges in attracting women to work in technology. Those women who do pursue a career in technology continue to face difficulties in progressing at the same pace as male counterparts[132]. Any new digital skills initiatives should incorporate learning from the evaluation of past initiatives, and should put in place metrics to measure impact.

Education and skills

Recommendation 7a: Government should ensure that the reforms to post-16 education (T levels and new apprenticeships standards) include appropriate levels of skills development for end-users of IoT in the workplace. The basic digital skills content across all routes of the T levels should be sufficiently generic to cover all sectors and occupations, while specific T levels should provide the necessary specialisation. Implementation of the reforms will need to consider local employer needs.

Recommendation 7b: Government should examine the practical and scalable solutions needed to upskill the existing workforce. The creation of high-quality, employer-endorsed online training platforms is one possible option, as proposed in the recent *Made Smarter* review.

Recommendation 7c: The education system across the UK needs to incentivise increasing numbers of students following pathways to engineering. The recent investment in computer science in schools is welcome. Government should consider similar investments in design and technology in schools, as this subject provides excellent opportunities for young people to understand interfaces between physical and digital systems as well as practical opportunities to apply this, for example to IoT.

Recommendation 7d: Building on its plans to 'build digital capability for all' as part of the Digital Strategy, government should work with business and industry to deliver evidence-based initiatives to educate the public about IoT. These should improve technical and data literacy by raising awareness of the benefits and limitations of such technologies and ensuring that the public are informed users.

Consumer understanding and adoption

There is a huge gap in explaining the benefits of IoT solutions and services to individuals, and the broader economic and social value they bring. In addition to the development of specialist skills, an improvement in digital understanding among both schoolchildren and the public will help to promote an appreciation of these benefits, and encourage consumers to adopt IoT. The Blackett review highlighted that digital exclusion would be a key issue if those who do not have the necessary skills or capabilities to adopt and use IoT are unable to realise the benefits. Public awareness about IoT privacy and security risks is also important, although efforts to educate the public in 'cyber hygiene[133]' have had limited success to date.

IoT products and services will become attractive to consumers when they become a general-purpose technology that impacts on the whole of society and the economy, at which point the technology may be used for purposes beyond those for which they were initially designed. In a domestic setting, this will occur when the home becomes a 'platform' for apps, rather than solutions being separate. The history of communication and computing technology suggests that future mass adoption of IoT would dramatically change the use of this technology and possibly some important aspects of the technology itself.

5.3 Policy implications

The lack of agreement on common standards, inadequate interoperability between standards, and sometimes the drive to advocate inappropriate standards[134] can limit the creation of economic value. Governments might find it challenging to quantify and harness economic benefits in a highly unregulated and fragmented space. Current progress on standards development is discussed in Section 3.2.

Competition law plays an important role in regulating the existing electronic communications market in the UK. EU competition rules address issues of antitrust, state intervention and corporate mergers. The UK Competition and Market Authority and OFCOM are responsible for ensuring that market players in the communications sector follow competition rules and ex-ante regulations. As has been the case over the past 25 years of digital technology evolution, market players have raised concerns about the extent to which future interventions around competition could risk stifling innovation in the development of the IoT market. However, it is vital that this these concerns are balanced with the need to protect the public interest and the risk of creating systems with poor cybersecurity.

6. Theme two: security and risk management

6.1 Context

Privacy, safety and trust are the central ethical and policy challenges for IoT. The successful adoption of IoT depends critically on meeting these challenges, which will demand appropriate levels of cybersecurity. Many consumer grade devices are coming to market with little or no attention to the security of the device, the data it gathers, uses and transmits, and the ramifications if security is compromised. These issues are not limited to the IoT device and the information it holds alone, but affect the security and resilience of connected infrastructure globally, as exemplified by the large-scale Distributed Denial of Service (DDoS) attack launched using the Mirai botnet that harvested a range of IoT devices. There is a complete lack of a coherent security architecture.

There is also a misconception that IoT is purely a technical system. In fact, IoT is a complex socio-technical system with interacting physical, digital (cyber), human and process aspects. These represent the aspects through which the system can be compromised, and through which attacks can propagate inside a system. Equally, each plays a vital role in protecting the other aspects and the system as a whole. A key challenge is designing secure and safe systems that combine physical, digital and human aspects, determining the role each aspect should fulfil and the responsibility it should take.

While there are tools to reason about the physical security and the cybersecurity of an IoT system and methodologies to reason about its human aspects, there is a lack of tools to model and analyse the propagation of threats from the human to the physical and cyber domains in turn, although analyses of the threats exist[135]. There is a lack of tools and methodologies to guide how to distribute the protection functions and responsibilities across the human, physical and digital aspects of an IoT system.

6.2 Challenges

6.2.1 Incorporating human factors and ergonomics into security

A human-centred view of IoT security recognises that errors and failures in complex systems exist and that the human is not to blame[136]. Where humans are a point of failure, this erroneous behaviour might have been fostered or made inevitable by other aspects of the system or the environment within which the system operates. Latent flaws in the technical design of IoT products can worsen the impact of errors and create the means for potential attackers to gain access.

Depending on the context, users may be unmotivated to make good security choices as security is generally a secondary activity compared to the real task at hand. Furthermore, users' perceptions of the impact of security violations play a role in their decision-making around security. There needs to be a better understanding of users' motivations and mental models relating to security risks arising from IoT and a focus on improving users' awareness of such risks without complex and counter-intuitive user interface designs. Users often adopt appropriate products and services in ways that are not anticipated by designers and producers, and designers may not take into account the social and cultural diversity of users that they are designing for.

Given that most user interactions with IoT devices do not provide an explicit means of interacting – in contrast with point and click or similar screen-based interfaces in typical computing devices such as laptops and smart phones – security ergonomics[137] becomes a fundamentally important consideration. This requires both designers of IoT devices and IoT app developers to consider how security information is conveyed to users and how to empower them to make informed security decisions without complex and cumbersome interactions with the device.

Human factors add a critical dimension that should be taken into consideration throughout the entire system lifecycle, from inception through design and build to usage and maintenance. There is much to learn from more mature engineering areas such as aviation, rail transportation and mining, where the whole system lifecycle already incorporates human factors[138]. Security-aware human-centred design is vital for both consumer applications, including healthcare, and for industrial applications, even where machine-to-machine communications predominate[139,140].

6.2.2 Generic security and resilience challenges

Common challenges across all IoT applications include the existence of insecure software and firmware[141], unauthorised access to sensor data, man-in-the-middle attacks[142] – since the risks can be greater for devices that are used as a central controlling hub – and a lack of transport encryption. Identification, authentication and access control need to cope with differing device capabilities and contexts in which devices will be used, as well as power consumption requirements. The evaluation of the risks resulting from unanticipated use and misuse remains a fundamental challenge, as is ensuring system integrity[143]. An understanding of the trade-offs facing designers – for example, between power consumption and security, and between cost and security for cheap devices – remains elusive. Current products often do not make this choice appropriately.

Improving this situation requires introducing good engineering practices, enabling robust approaches to the design, implementation and operation of IoT systems. To achieve this, appropriate engineering policies and procedures are required, which must take into account the many complex organisational and human factors at play[144].

Augmenting legacy industrial systems with IoT

Because IoT devices will often be embedded in a physical infrastructure they are expected to have much longer lifetimes, not unlike industrial control systems in use today whose life often exceeds 30 years. Over such long lifetimes, technology invariably becomes obsolete, particularly when the number and nature of threats are constantly evolving. This could be partially mitigated if the design of IoT-enabled products considered upgrade and replacement as fundamental from the design stage and throughout the lifetime of the product. This a challenge for legacy industrial control systems, and systems operators will need to take a different approach to reducing cyber-risk. Building management systems face similar challenges when IoT augments legacy building instrumentation.

Rapid expansion of IoT makes retrofitting IoT devices to existing systems popular. It allows systems to adapt much more swiftly, cheaply and easily. However, system operators do not always conduct careful risk assessments when retrofitting IoT devices to such systems. Numerous vulnerabilities, including in critical systems, may be introduced through the addition of new devices that were not part of the original design intentions. Risk engineering processes can be embedded into the development and lifecycle of IoT systems to address these shortcomings. There is a lack of methodologies to conduct and update risk assessments rapidly enough to keep pace with demand, and that consider the dynamics of interconnected systems[145]. Systems operators severely need new techniques that enable the retrofit of security controls to legacy products. In addition, there will be a need to assess and monitor the impact of retrofitting IoT devices on system safety and to develop ways to derive device-level constraints. There will be many different solutions and trade-offs between system vs device.

The challenge of operating systems within partially trusted environments, where only some elements are fully trusted or secure, is something that will need to be addressed in the near future. It arises because of legacy and new devices becoming interoperable, and requires a rethink in the way that security is addressed in large-scale IoT implementations.

Balancing security, safety and privacy

While it is well established that security, safety and privacy are all essential to the deployment and use of IoT systems, the trade-offs between these are not always well understood and appropriate choices are not always made. It is accepted that poor security leads to loss of privacy; however, there are also cases where the security of a system may be undermined because of privacy considerations. There are also situations in which security concerns anchor privacy and individual rights, for example transparency, or where overly protective security controls undermine the safety of the system. For example, in an emergency, safety considerations may require information and systems to be available and this may be in conflict with security goals[146]. It will be important to characterise these trade-offs accurately and conduct analyses that enable the right choices to be made according to the context in which a particular IoT system is used. These aspects are also subject to national policies – for example, the US has a strong record of national rights dominating over individual right to privacy.

IoT resilience

The dynamic assembly of new IoT systems and the augmentation of existing physical and digital systems with new devices may result in systems that exhibit new behaviours, whether intentionally, accidentally through combinations of devices coming together, or as a result of malicious intent. The attack surface of these systems is increased, and thus the likelihood that they will be compromised. While manufacturers focus on individual products, they do not always consider the system into which these devices will be deployed, nor their full lifecycle. New assemblies of IoT systems come about because of the empowerment that IoT affords – whether for industry, business or consumers – which enable innovation but also have other consequences.

Systems must be designed to be as safe and secure as possible but in the face of current and future threats, keeping systems free from compromise is, in many cases, not an achievable goal. It is therefore necessary to prepare for the consequences by designing IoT systems in such a way that they can continue to operate, even

WHILE IT IS WELL ESTABLISHED THAT SECURITY, SAFETY AND PRIVACY ARE ALL ESSENTIAL TO IoT SYSTEMS, THE TRADE-OFFS BETWEEN THESE ARE NOT ALWAYS WELL UNDERSTOOD AND APPROPRIATE CHOICES ARE NOT ALWAYS MADE.

when they have been partially compromised. Systems must also be able to recover from a complete loss of service in a situation where disruption to components cannot be contained.

However, the science and methodologies to design systems that can 'gracefully degrade'[147] and maintain trustworthy operations of critical functions, even when partially compromised, requires further development. Subsystems – for example, the future IoT house – may need to be capable of autonomous operation for extended periods, if the defence against a cyberattack is to isolate that subsystem. The government specifies 'segregation' as a means of defence in its cybersecurity principles for connected and autonomous vehicles[148]. Existing risk-assessment methodologies are insufficient, since systems are changing dynamically and a periodic assessment assuming consistent behaviour or a closed system is no longer adequate[149]. Assurance methods for such systems will also need to be developed. Such an effort will require multidisciplinary collaboration and will need to integrate and build on existing methods.

6.2.3 Sector-specific challenges

Industry and critical infrastructure

In conventional industrial control systems and 'supervisory control and data acquisition' (SCADA) systems, data is monitored within an industrial process and provides the means for automation. The growing use of IoT technologies in industrial control systems is emerging alongside the trend towards integration of traditional IT systems and operations technology systems, which has been progressing for some time[150]. However, legacy industrial control systems were designed without security in mind, as connectivity was not envisaged. Original security assumptions are no longer valid as the way in which systems interact with the outside world changes.

The vision of the *Made Smarter* review[151] envisages devices such as sensors and controllers integrated with other emerging technologies such as mobile computing, cloud computing and big data. The success of this depends on how secure and resilient devices are. Given the hyper-connectivity of such systems, and the need to ensure availability and integrity, resilience and security are key concerns. Such systems are at risk from DDoS attacks, jamming, cascading faults, value tampering, malicious data injections as well as cyber-physical attacks – all of which can compromise the security and safety of critical infrastructure on which society relies.

Connected and autonomous vehicles

Connected and autonomous vehicles (CAVs) will not only use onboard sensors, but will also most likely communicate with surrounding vehicles and infrastructure, providing a large potential for attacks on their integrity or communications. The systems they interact with may themselves be malicious or compromised. Vulnerabilities exist that are exploitable through direct physical attacks and remotely. There is still much to do to integrate the autonomous and connected parts of CAVs, but tensions exist between ensuring both safety and security. For example, the use of cooperative data might provide critical information to enhance safety and performance, but also introduces new potential attacks such as malicious data injections. The connected nature of the eco-system may bring individual benefits but also increases the risks of systemic, fleet-wide losses.

Healthcare and medical devices

The security of connected medical devices is a particular challenge, existing alongside the challenges of privacy, transparency, trust and the user's autonomy. These include both implantable medical devices and medical-grade wearables. The latter often builds on existing consumer devices[152].

Newer implantable medical devices (IMDs)[153] have started to incorporate communication and networking functions to provide telemetry plus increasingly sophisticated computing capabilities. This has provided IMDs with more intelligence and patients with more autonomy as medical personnel can access data and reconfigure implants remotely. Benefits include cost reductions as well as the ability to monitor a patient's condition and new diagnostic techniques. IMDs usually have limited energy and computational capabilities, hindering the use of cryptographic techniques, and instead using lightweight protocols. Innovations in implantable sensors, such as biodegradable sensors, share the characteristics of small physical footprints and low power consumption with other IoT devices, with similar challenges around safety and security.

Consumer environments

There are a growing number of consumer applications of IoT such as smart homes, building management systems, smart/electronic locks, baby monitors, smart televisions, fitness trackers and wearables, and smart watches. These have extensive security issues and vulnerabilities, and there is little or no user guidance and

REGULATORS AND POLICYMAKERS NEED TO CLARIFY HOW EMERGING IoT NETWORKS AND SERVICES RELATE TO CURRENT SECURITY LEGISLATION.

awareness relating to their security. Little analysis has been carried out of the systems built from such devices, their interdependencies, the implications of compromise on the services provided and their resilience. The academic literature emphasises the impact of security on confidentiality or the loss of privacy to the user, rather than on integrity or availability of the system, which may be important in certain applications, or unintended consequences of data sharing[154].

6.3 Policy implications

Standards and security

The term IoT applies to a wide range of products, services and architectures. There is therefore not going to be a single solution to standardisation. Similarly, to technical standards more generally, security standards have been emerging in large numbers, and will continue to emerge for individual technology components, such as those developed by GSMA[155]. A key concern is how to create end-to-end security – that is to say, how to secure the 'edge' (the device) or the communication layer, how to ensure a device or system is secure throughout its lifecycle, and how these elements fit together to create systemic security. Existing standards are, to a degree, contradictory and provide incomplete protection. The addition of yet more standards will not solve the security problem if they do not enable end-to-end security. End-to-end security standards will be difficult to create given the diverse range of stakeholders in the design and operating supply chains. In addition to the fragmentation of IoT security standards within industry, there is also an imperative to understand how IoT cybersecurity and safety standards should be integrated. For example, existing security standards may be limited in a particular context, such as where the application of certain security techniques to safety critical systems might hinder their safe operation.

An alternative approach would be to develop principles and good practice guidance on a sector-by-sector basis, as has already been done for ports and port systems[156] and connected autonomous vehicles[157]. In addition, open-source software that acts as a reference implementation is useful alongside guidance, as it is less open to misinterpretation by an inexperienced technical developer. There would also be a need to address the problem of regulatory misalignment between broad privacy and security rules – the GDPR and the NIS Directive – and sector-specific regulations and product certification schemes.

Security standards and policy

Recommendation 8a: Government, working with the National Cyber Security Centre, UK national standards bodies, regulators and industry, should enable the development of security standards for IoT that provide a baseline across sectors, recognising the multi-sectoral nature of the supply chain, while working within specific national and international industry contexts. This recommendation should be carried out alongside Recommendation 2c.

Recommendation 8b: Government departments should ensure that policy reflects the critical importance of cybersecurity and the need to trade off cybersecurity against other considerations that contribute to achieving policy objectives. DCMS, BEIS and other government departments should work with the National Cyber Security Centre and others to explore ways of ensuring levels of cybersecurity are transparent for products and services throughout the supply chain.

Regulation and risk management

In the UK, legally explicit security obligations only apply to 'providers of publicly available electronic communications services', although there are also several 'soft laws' such as the *Cyber Essentials Scheme*[158], which are applicable to any organisation wishing to improve its 'cyber hygiene[159]', and a growing number of risk management guidelines[160] for operators of critical infrastructure. However, security issues extend beyond the public network element of the IoT system to embedded systems and cloud services. There is uncertainty about the security responsibilities of manufacturers of IoT endpoints and digital service providers such as cloud computing services. However, this could be addressed by tackling the civil law presumption regarding the operation of equipment[161]. While standards for security management systems exist[162], it is not always straightforward to apply them, making it challenging for service providers to secure systems. There may also be challenges in applying principles and guidelines. For example, there are difficulties in applying guidelines on cloud security[163] because of the nature of the cloud supply chain.

Policymakers and regulators need to clarify the extent to which emerging IoT networks and services relate to current legislation around security. There are questions about how effectively

government departments communicate the pervasiveness of IoT risks within and across each other[164]. There is also a question about whether 'soft laws' or guidelines such as 'security by default' can overcome cost/benefit analyses within the private sector to contribute to broader public objectives around national security, and whether the regulatory burden is efficiently distributed between private sector and public authorities to respond to the challenges.

The UK government will need to address the EU's NIS Directive. The NIS Directive extends security obligations to 'network and information systems' operators and providers of essential services, rather than just 'providers of electronic communication services'. It is broadly more applicable to industrial applications of IoT than consumer applications such as fitness trackers. The UK government will need to determine whether the provisions of the NIS Directive are sufficient to respond to the security challenges of IoT and whether it effectively distributes the regulatory burden between the government and the private sector[165]. There are also tensions between requirements for safety and the NIS Directive that will need the directive's demands for continuity of service.

There is potential to improve cyber-risk management of IoT systems through applying knowledge of human factors, learning from other areas such as aviation and clinical practice. However, there is a tension between the ideas from human factors and cyber-risk management. The latter tries to identify and address bad things before they happen, whereas human factors try to identify retrospectively 'how did that thing happen?'. For example, in security the 'common vulnerability scoring system' identifies software vulnerabilities that have already been discovered and verified, whereas the 'common weakness scoring system' takes a more forward-looking approach, working with incomplete data, that is similar to risk management. Government should investigate the use of such techniques towards a more comprehensive resilience of systems approach. The use of cyber insurance as a risk management tool is discussed in the next section.

'Security by default' and 'resilience by design'

Proactive approaches to the design of IoT devices and systems would help to ensure that manufacturers build essential requirements such as security and resilience into the device's design or systems at the very earliest stages, rather than having to bolt on security at a later stage. For example, 'security by default' principles would help to reduce common security flaws such as insecure user interface design or the lack of proper upgrade mechanisms such as patching. Government advocates the use of 'security by design' in its recently published principles on cybersecurity for connected and automated vehicles[166]. The National Cyber Security Centre has developed 'secure by default' principles that are relevant to hardware, firmware and software developers to create products that mitigate the latest threats but are still useable[167]. Similarly to 'security by default' principles, 'resilience by design' principles would help to embed resilience thinking early in the design of a system. Sector-specific guidance will need to be developed to help sectors apply the principles in their own areas. In addition, services, toolkits and open-source software that embody best practice are of great practical benefit to the developer community. There is a role for UKRI in promoting these through Innovate UK and the Research Councils.

The success of 'security by default' will in part depend on whether other challenges have been successfully addressed, for example around standards and interoperability. In turn, 'security by default' will have implications for liability, regulation, consumer education and consumer protection. This is one example of the interdependent and complex nature of the challenges for IoT.

Risk management and resilience

Recommendation 9: Government should commission guidance on how to integrate 'security by default' and 'resilience by design' principles and methods into the development of IoT products and services, on a sector-by-sector basis. Evidence that these approaches have been followed could help to demonstrate that products, services and systems have been developed with due attention to risk management and provide adequate security and resilience. This feeds into the recommendation on ensuring transparency about cybersecurity in products across the supply chain (Recommendation 8b). Guidance should be promoted widely to industry. Alongside government, professional institutions should play a role in encouraging security-mindedness and resilience-mindedness in professions.

Governance of IoT: insurance, disclosure and liability

Insurance has the potential to be a valuable tool for enhancing the management of, and resilience to, cyber-risk. There is a growing cyber insurance industry[168] that supplies a range of cyber insurance products. For industrial IoT applications, business operations and continuity is the key concern with insurance broadly covering the losses relating to damage to, or loss of information from, IT systems and networks. Insurance may also cover damage to digital assets. In the case of consumer IoT applications, privacy and GDPR are central concerns and would require a different type of insurance such as credit monitoring. There are many questions about the extent to which the various insurance products are fit for purpose for IoT. There are also opportunities for developing more accurate, data-driven insurance products.

IoT intensifies existing debates around responsible disclosure of vulnerabilities. Clarity is needed on the extent to which software developers and vendors are expected to commit sufficient resources towards identifying and removing flaws during the initial product and service development stage. Clarity is also needed about what actions they are expected to take in response to identified vulnerabilities after products have reached the market. International cooperation between Computer Security Incident Response Teams (CSIRTS) and Product Security Incident Response Teams (PSIRTs) will become increasingly important[169] . Given the complexity and scale of the global supply chain for IoT, as well as the criticality of certain IoT systems, issues around responsible disclosure require further exploration. For example, there are questions about whether security can 'legally' be guaranteed throughout the lifecycle of an IoT device, and what exactly will constitute vendor responsibilities for updating products throughout their lifecycle.

Liability and chains of liability are significant issues for IoT, especially in an international context where the supply chain is global. Tighter product liability laws that establish accountability for manufacturers of software, hardware and systems, and thus provide an incentive for improving the quality of products, should be considered[170]. Further exploration of this issue is needed, along with consideration of alternative approaches and alignment with ongoing international initiatives in this space.

Liability

Recommendation 10: Government departments, regulators, legal bodies and industry organisations should work together on a sector-by-sector basis to explore the suitability of existing liability regimes for IoT applications, and to develop new approaches to liability where necessary. These actions should align with international initiatives.

7. Theme three: adoption and implementation

7.1 Context

The Blackett review argued that any potential benefits from IoT depend on take-up by individuals, businesses and governments. The review further recognised that public trust and acceptability are central to the implementation of IoT, and providers and operators would need to demonstrate their trustworthiness. It would be important for all participants to be part of a public debate, to help build support and address concerns.

Policymakers need to investigate the attitudes of the public if acceptability of IoT is to be understood, including the factors that shape user attitudes to adopt IoT technologies and services. A change in the public's understanding of how organisations use personal data may also influence attitudes in the future[171]. The ability for organisations to help the public understand how they use their personal data is also a new design challenge[172]. Policymakers also need to understand the attitudes of companies and the factors that influence acceptability of IoT in industrial applications. Technical adoption and implementation challenges for industry are discussed on page 26.

7.2 Challenges

7.2.1 Acceptability and adoption for consumers and industry

While economic drivers push larger businesses and government to adopt IoT, the adoption and use of IoT by individual consumers, domestic groups, communities and some small businesses is a result of a complex combination of social, economic and cultural factors. For example, in the case of smart cities, citizens see potential improvements brought about by IoT technology, such as a reduction in air pollution or reduced traffic congestion, as a right rather than a service. In such cases, it is challenging to reshape that dynamic from a citizen/public good arrangement into a client/paid service arrangement. For consumers, the pathways of adoption and choices manifest in them are the result of large numbers of individual judgements by consumers of value and acceptability. Value for businesses and consumers may only be fully realised through network externalities arising from collective mass adoption.

CURRENTLY THE WAY IN WHICH ORGANISATIONS USE, SHARE OR RESELL PERSONAL DATA IS POORLY UNDERSTOOD BY USERS.

Acceptability for consumers

To design IoT and services that are acceptable to consumers, it is beneficial to understand the needs of consumers and gaps in routines where IoT can efficiently help and fit in, in very familiar, mundane environments such as the car or home. Ignoring natural interactional strategies and routines may lead to lower levels of adoption. There is also a need for businesses to develop the capacity to look beyond current practices as the technology is likely to disrupt familiar routines, such as those that are typical of the home environment today. While IoT needs to appeal to the 'innovators' and 'early adopters'[173] who will invest effort and money for uncertain returns, the IoT industry must develop ways to engage with and learn from their experiences if they are to then push through to mobilise the interest of the 'early majority'. 'Social learning', where individuals learn from the experiences of others[174,175], will affect adoption.

Usability will influence adoption, which is in turn affected by factors such as the degree to which the system can be understood at an intuitive level, the necessary amount of engagement required with the system, and whether security is easily managed. There is also an inherent danger that if the system is opaque, there is a loss in trust when problems inevitably arise. Furthermore, having to manage interaction with multiple devices may be disruptive to users' attention and to their routines.

It is likely that with the proliferation of devices and services, the so-called 'cost of ownership' borne by consumers will increase, placing on them a responsibility to ensure devices and services are properly maintained, for example by changing passwords or installing latest security updates. Furthermore, many IoT device manufacturers' lack of focus to date on even basic security, for example devices sold with fixed and easily guessed passwords[176], points not only to high levels of risk to privacy and system attacks, but to future problems managing combinations of legacy and up-to-date devices.

There is more to be done to understand and promote trust in IoT. For example, for an automated system, there is a tension between the need for user control and the user's trust in the system to work without their attention, but there may be liability issues associated with partial automation. There are also issues around data privacy and security, and user control. A user could control individual privacy settings depending on needs and expectations, or they could control data processing. If feedback from data processing is easily understood by users, they may be more likely to continue using a system.

There may be privacy threats from data sharing and aggregation for both service providers and the end-user, although data sharing realises the value from data. Currently, the way in which organisations use, share or resell personal data is poorly understood by users, although the GDPR may change this. It is not clear how people understand the value of their personal data with respect to specific IoT technologies and services, and how environments can be created for informed consent for data sharing in smart homes or automatic vehicles. This may impose further burdens on consumers and their daily routines. Innovative visualisation tools could enable this understanding. It is also unclear, how devices will implement the right to be forgotten.

The impact of security and safety of IoT on adoption would benefit from more detailed exploration. There are questions about how security controls impact adoption and acceptability, whether as a hindrance or as an enabler of trust, and correspondingly how manufacturers can design systems that enable users to move from the former to the latter.

A key challenge will be to identify ways of minimising the barriers to acceptability as IoT scales up across multiple connected devices and services. This includes understanding the incentives and risks for adoption across different groups, such as early adopters, pragmatists, conservatives and sceptics, and how these vary according to context of use. Adoption of IoT in the public sphere, such as in smart cities, healthcare and education, could increase social adoption, as many consumer services are created in this sphere.

The social challenges around use of IoT goes well beyond the adoption by the public. Government should consider the implications of using IoT in surveillance or censorship, and its use in law enforcement. The interest and rights of individuals and social groups must be taken into account, as must ensuring access for all to information and technology. Education and the professional landscape are two key areas of impact. IoT should not disrupt the social contract, although it may lead to new forms of social, political or economic engagement.

ETHICS IN IoT CAN BE MAPPED ONTO THREE MAIN AREAS: ETHICS OF DATA, ETHICS OF ALGORITHMS AND ETHICS OF PRACTICES.

7.2.2 Ethics, privacy and trust

Maintaining public acceptability requires robust approaches to ethics, privacy and trust across the different applications of IoT. The uses of IoT range from data collection and transmission, through methods of interpreting and inferring information from the data, to applications of the information. Protocols for each of these uses should be designed in ethically acceptable ways. Accordingly, ethics in IoT can be mapped onto three main areas: ethics of data, ethics of algorithms and ethics of practices.

Practical approaches to privacy and trust require significant technical effort and need to take human factors into account. While these approaches will be needed to address issues of privacy and trust in consumer applications of IoT, such issues must also be addressed in industrial applications. In the case of certain industrial applications, for example connected vehicles or healthcare equipment such as MRI scanners, the privacy of customers may be at risk if manufacturers are able to see how their products are being used. Organisations also require confidentiality for commercial reasons.

Ethical frameworks

The ethics of data focuses on problems concerning the risk of re-identification of individuals through data-mining, -linking, -merging, and reusing of large datasets. The analysis shows that the transmission of personal data by IoT devices can transgress privacy-protecting natural, social, spatial, temporal, ephemeral, and transitory borders. The problems rest on the lack of control and oversight on data flows. Controlling data flows can enhance a user's autonomy and privacy in relation to data controllers' and data processors' capacities for regulation, behavioural control, and social sorting of users.

The ethics of algorithms addresses the ethical problems following the use of algorithms embedded in software. Algorithms are inescapably value-laden and developers specify operational parameters, which users configure with desired outcomes in mind that privilege some values and interests over others. At the same time, operation within accepted parameters does not guarantee ethically acceptable behaviour. This is even more pertinent for IoT and, especially, machine learning applications.

The ethics of practices must address the pressing need to define an ethical framework to shape a 'deontological'[177] code about responsible innovation and use. The ethical framework should encourage ethical practices that foster both the progress of IoT and the protection of the rights of data subjects. Designers, engineers, scientists and managers of IoT technologies are increasingly stewards of whole ecosystems, with moral responsibilities and liabilities. However, it may be a challenge to foster this approach as it will need to counter the current practices of large data companies that may also influence how emerging organisations behave. Where existing ethical principles for the various professions exist[178], these should be extended to address the specific ethical challenges for IoT.

Ethical frameworks, privacy and consent

Recommendation 11a: Professional engineering institutions and other professional bodies, working alongside DCMS and the Centre for Data Ethics and Innovation, should build on existing ethical principles developed for professions to create an ethical framework for IoT to encourage ethical behaviours. They should provide case studies to illustrate how the principles are applied in practice.

Recommendation 11b: The Information Commissioners' Office should develop best practice guidance for IoT stakeholders that nurtures a clear understanding and implementation of the data protection regulations.

7.2.3 Technical challenges around ensuring privacy and trust

There are few standards for privacy and trust, which is to be expected given the rapid development of large numbers of heterogeneous devices. Trust relationship models are needed that consider identity and access management, entitlement management[179] and associated behaviour, but these are a challenge for IoT because of resource constraints on devices and the dynamic and ad-hoc nature of IoT.

Without user consent, the data that drives IoT cannot legitimately be collected, stored or processed. Current mechanisms for obtaining user consent on the web include privacy policies, cookie notices, and terms and conditions, with associated challenges around their presentation in a user-friendly and understandable manner. Indeed, consent is usually collected without the user being fully aware of what they have agreed to, but rather ticking boxes to accept terms and conditions as part of product initialisation and set-up, although this should change with the GDPR coming into force. It is questionable whether such mechanisms apply to IoT.

APPROPRIATE INTERACTIONS BETWEEN IoT DEVICES AND USERS ARE ESSENTIAL TO OVERCOME THE FEELING OF 'BEING WATCHED' AND TO ENSURE THAT DEVICES DO NOT POSE, OR ARE PERCEIVED AS RISKS, TO PRIVACY.

Managing fine-grained consent in IoT is very challenging. In various cases, consent is not appropriate, either because the user cannot anticipate uses of data or because other interests are involved – for example, DNA data implicitly has other data subjects linked to it[180] such as family members – or because public good overrides personal risk.

There are many challenges around data management and privacy. Robust data management processes enable the protection of personal data, requiring clarity on who is collecting data, how it is being collected and the time of collection process. Ideally, data collection should be limited, only that which is authorised, and storage and access should also be authorised. There are difficulties in implementing data minimisation, whether the data is used for commercial or surveillance purposes. It is also a challenge to enhance the data subject's control of data, which would allow them to access, delete or move it. A further difficulty is protection of data by cloud service providers during transmission, processing and storage. There are challenges of anonymity, especially for data brought together in combination. A trade-off exists between obtaining the functional benefits of combining data and the danger of revealing potentially sensitive information. As well as the more established work in protecting data in storage and transmission, methods to protect data in computation are improving but still have some way to go to be useful in IoT contexts. This include methods such as homomorphic encryption[181], multi-party computation[182] and differential privacy[183].

Current methods of authentication need to be adapted for use in wide-scale adoption of IoT. Improvements to the interfaces that enable authentication are needed; these currently tend to be non-standard or even barely existent. The use of different authentication credentials for many different devices, possibly situated at many different locations, increases the risk that credentials may be compromised. So-called zero-knowledge proofs, which allow an entity to prove they know a particular piece of information – for example, a password or biometric identifier – without divulging that information, are currently under-developed in IoT.

IoT devices can violate norms of private space and can cause a feeling of 'being watched'. Appropriate interactions and communications with the users are essential to overcome this feeling and ensure that IoT devices do not pose, or are perceived as, risks to privacy and to foster users' trust.

Particularly in the case of consumer devices, there is a threat to privacy because of determining and recording a person's location through space. Consumer devices such as Amazon Echo[184] are set with camera and voice always on. Smart TVs such as Sky and Fire TV now include voice activation, and are listening to and sharing data. People trade privacy for services, for example Kodi boxes[185] permit data sharing in return for access to Sky. Privacy issues come into the practice of profiling: compiling information dossiers about individuals to infer interests by correlation with other profiles and data. There are risks around the possibility that private information could be conveyed through a public medium and disclosed to an unwanted audience. There is also the risk of disclosure when smart devices change ownership, although the ability to automatically delete data or resetting device would help. Methods that prevent linking of data sets – that is to say, they enable 'unlinkability' – are important for privacy protection but a challenge for IoT.

Currently, there is a clear conflict between the adopted business models in the consumer sector and the right to privacy. The use of cloud services simply allows the shifting of data to jurisdictions where data protection regulations are less strict. One approach to ensuring privacy might be to aggregate data at the edge[186] – close to where the device is generating data, such as a user's home – which avoids the use of cloud services and allows users greater control of what data is used, how it is used and by whom.

7.3 Policy implications

A lack of suitable standards for IoT bears many risks, including both economic risks and social risks. Social risks range from reluctance to adopt insecure technology to ethical and physical damages brought to individuals and groups. These damages can be one-off and quantifiable, or can last over long periods of time and have unforeseen consequences, such as social and reputational impacts.

UK and EU regulation that addresses privacy and data protection is in transition. In May 2018, the GDPR will come into effect alongside a new UK Data Protection Bill, which will replace the existing 1998 UK Data Protection Act. Interpreting how this new regulatory framework will interact with evolving IoT technologies will be central to all aspects of IoT that process or control personal data. The UK has the further challenge of regulation after Brexit, although the recent statement of intent has outlined how the government plans to take data protection legislation forward[187]. This combination of new regulation and emerging technology

IoT SYSTEMS ARE SO COMPLEX, INTERTWINED AND INTEROPERABLE THAT IT CAN BE CHALLENGING TO FOLLOW THE PROVENANCE OF DATA FLOWS FROM START TO FINISH, POSING PROBLEMS FOR REGULATORS AND DATA CONTROLLERS.

results in several 'gaps' or questions of interpretation that will need to be resolved. The question of how GDPR and similar legislation will work in the world of IoT is unclear, particularly where the service provider is based outside the jurisdiction and also uses cloud services as part of the overall service design. There may be uncertainty about where data is stored, processed or accessed. Experience from building information modelling (BIM) Level 2 common data environments[188], which may use cloud services, is not reassuring in this regard[189].

There are complex questions developing about what exactly constitutes personal data in IoT. In Germany, debates are emerging around the use of video cameras in autonomous vehicles that capture human images outside the vehicle[190]. In addition, non-personally identifiable data streams can be de-anonymised in unanticipated ways when aggregated with other data streams. There needs to be clarity about when personal privacy may become vulnerable or exposed in IoT.

Equally, it can be unclear who controls and processes data in the IoT ecosystem. Under data protection legislation, responsibility for this falls to 'data controllers' and 'data processors'. A 'data controller' is an actor who (either alone, jointly or in common with other actors) determines the purposes for which, and the manner in which, any personal data are to be processed. A 'data processor' is any actor (other than an employee of the data controller) who processes the data on behalf of the data controller. IoT systems are so complex, intertwined and interoperable that it can be challenging to follow the provenance of data flows through from start to finish. This poses problems not only for regulators faced with enforcing processes and practices, but also for data controllers themselves. It also poses problems for entities that may be acting as data processors without necessarily realising it or perhaps without a full awareness of the implications of those roles.

There are liability implications regarding the control of personal data, its exchange and aggregation[191]. For example, it is unclear how to implement principles such as 'informed consent'[192] or 'data minimisation'[193] in an automated and adaptive environment, or how to cover automated decisions based on inferences from data in legislation.

Commissioning by government

Government can exert major influence on adoption through its own purchasing. In these emerging areas, a preference for specialised purchasing from entrepreneurial SMEs could have great benefit. However, the perception remains that public procurement decisions continue to prioritise low cost over best value, and risk aversion hinders the introduction of innovative solutions. Government needs to adopt the established best practice around intelligent procurement that will involve cultural change and a greater willingness to establish and accept an appropriate level of risk[194].

Commissioning

Recommendation 12: Government should consider how best to change the culture of risk aversion in public procurement decision-making, and encourage government departments and other public bodies to embrace innovative solutions to support the adoption of emerging technologies such as IoT.

8. Conclusions

A bold and forward-thinking vision for the Internet of Things and how it can benefit the economy and society is vital in capturing the opportunities that it offers. Evolution of technologies is rapid, and there is still uncertainty about how users – industrial, public space and consumer – will adopt and interact with technologies, and the resulting economic and societal impacts. Government and industry need to create a shared vision to be able respond dynamically to future evolution of IoT and the profound changes to the home, workplace and transport over the next 5 to 10 years.

Innovation will occur in many areas, beyond the creation of individual IoT technologies. Technologies will be used in combination to enhance the usefulness of IoT. For example, highly interactive devices and augmented and virtual reality will generate a stronger link between physical and digital worlds, improving users' ability to visualise, interpret and respond to IoT data. Industrial- and home-based autonomous systems will use IoT and robotics in combination. The development of new business models and new uses for IoT are further key innovations, once initial barriers have been overcome. IoT will enable new social models of use, such as the 'Internet of Me', that will allow the individual more control over how they interact with IoT and the data generated from IoT. Less positive uses of the technology will also emerge, as illustrated by the rising use of the IoT black market and associated business models that put future ones at risk[195].

There are many complex and interdependent factors that will influence the ability of IoT to achieve policy objectives, whether improving efficiency and productivity in the case of industrial applications, improving quality of life through consumer applications, or improving both through public space applications. Delivering the vision will require the combined efforts of many different stakeholders, from both private and public sectors. It will also need an international strategy that recognises the nature of the global market and supply chain and promotes the UK's leadership role in international governance and regulation. A systems approach will help to tackle this complexity, identify key relationships and ensure different elements of policy work together.

Economic benefits will accrue from the creation of IoT products and services as a result of existing companies expanding their offer and from new businesses being created. However, the greater gains are likely to be from the increases in efficiency and productivity because of industrial and public space IoT adoption. Successful adoption will depend on implementation of IoT systems with clear business outcomes in mind. There may need to be a change in organisational culture to ensure data generated by IoT is treated as an asset, and properly protected and used. Interoperable systems that allow the involvement of many different players is vital for supporting the growth of IoT ecosystems.

It is important that the IoT industry has the capacity to sustain an effective engagement with its industrial and consumer users so that industry can learn from users' experiences to reshape and develop their products and services. Industry must do this in line with regulatory frameworks and with privacy and security consideration in mind. The IoT industry is at the beginning of what will be a lengthy process of trying to break into a mass market for IoT devices, systems and services. In this time, early users will effectively be testing the value proposition of IoT. Their early experiences may strongly influence the willingness of the 'late majority' to adopt. The extent to which the IoT industry can capture and respond to these experiences and users' expectations will therefore be critical for mass market penetration. However, this could be a challenge because of the current fragmented and heterogeneous IoT ecosystem.

The potential to sustain IoT's wide-ranging use, with subsequent economic and social benefits, will depend critically on maintaining trust. Robust end-to-end security needs to enable privacy and safety. Both regulatory and non-regulatory mechanisms are needed to improve the security and privacy of IoT products and systems. In addition to standards and regulation, ethical frameworks and codes of conduct will also play a role, as will risk management frameworks. The UK can create a competitive advantage both by developing its cybersecurity expertise and industry, and through creating secure and trusted systems.

Annex 1: Strategic research agenda

Future IoT research must extend technical capabilities, solve outstanding technical, economic, social and policy challenges, and pave the way to effective implementation and adoption. This section sets out a strategic research agenda that builds on existing research programmes to extend and refine solutions to current challenges, many of which the report highlights. Recognising that IoT is a socio-technical system, research in the IoT area must be approached through interdisciplinary collaboration.

Collaboration between industry, government and academia will be key to solving many of the outstanding challenges around adoption, security, interoperability and risk management.

Technology demonstration through experimental methods and live testing will help to solve these challenges, as well as demonstrating benefits and raising awareness in the market of where IoT has been successfully applied. Collaboration and sharing of best practice will also be facilitated by the creation of networks of stakeholders.

The UK should learn from and lead in the international landscape in identifying best practice, the gaps within existing approaches to IoT and how stakeholders can work together to address the gaps.

New approaches to regulation, standardisation, legislation and governance

Liability and other legal issues

Understand how data integrity and security obligations are distributed across different IoT stakeholders; understand how the locus of liability might shift between users, owners and manufacturers; understand market structure and the legal implications with regard to competition, service liability, jurisdiction; understand how legal issues play out in mergers and acquisitions; investigate legal data ownership rights, and accountability and liability in relation to data; understand how the application of international law in cyberspace will be further complicated by IoT.

Standardisation

Understand the role of standardisation in IoT and its broader effects; understand the impact of delays in standardisation on implementation, impacts of standardisation on innovation and trade and patent application trends for IoT; understand optimum ways of applying standards for tackling interoperability, privacy and security challenges; understand the optimum role of standards in regulation; understand the broader geopolitical dimensions of standards competition as well as the implications of this for the UK.

Governance

Understand and implement responsible disclosure mechanisms in IoT, and how policy might balance the rights and responsibilities of the reporter(s) of vulnerabilities with those of IoT service and network providers; determine government's role in setting procedures that protect or reward responsible disclosure and sanction opportunistic and reckless disclosure; determine which sectors might require mandated reporting, such as safety-critical systems; explore non-regulatory measures for encouraging responsible design and innovation by organisations, and 'privacy and security by design'; determine the balance between private and public entities providing insurance or assurance.

Regulation

Understand how existing regulatory frameworks need to be adapted for IoT, as new use cases and applications emerge; investigate alternative methods for regulation development that are appropriate for rapidly emerging technologies.

Harnessing economic value

Business models

Assess the economic costs of developing, implementing, operating and maintaining complex IoT products, services and infrastructures; understand how value can be built across an IoT value chain, including the balance of reward and risk; understand the value of social, cultural and wellbeing impacts of IoT on the economy; develop robust methodologies to assess the actual economic output of IoT, including digital economics and their impact on businesses gross value added, taxation and the real impact on the GDP; understand the business models and social and economic impact of alternative markets enabled by digital economies, such as black markets.

Improving methods for the usage of IoT-generated data

Develop data validation methods and methods for ensuring data integrity; investigate the role of data marketplaces and data platforms in allowing controlled sharing or trading of data; explore methods including standardisation for a general approach to data description, data quality, provenance and integrity; assess the

human and social consequences of generating, using, exchanging and interpreting data including outputs of machine learning and AI.

Interoperability: the role of open source versus proprietary solutions

Balance risks of open source and community-led activities with the advantages of open source for business and innovation, depending on level of criticality and use; understand the role of open source in democratising access to services and in the development of business ecosystems; understand how to balance strong competition with ensuring sufficient interoperability and open collaboration; understand the role of IoT marketplaces; understand the role of the cloud and IoT.

Skills development for digital economy

Explore the diversification of the emerging workforce, investigating methods to foster inclusive education and training that explores innovative approaches; propose a model to retrain skilled workers with minimum social and economic impact; assess the impact of IoT on job markets; assess the impact of IoT on major public interest sectors.

Security and risk management

Resilience and reliability

Develop the science and methodologies needed to design resilient systems; understand whole-life risks and when systems or devices become unreliable; investigate systems that can self-identify compromise, promote autonomous isolation of compromised sub systems and enable graceful degradation; understand the reliability of data collected by IoT-based systems, and the extent to which it can reliably inform intelligent autonomous systems; understand the relationship between data reliability and systems resilience in autonomous decision-making, machine learning and AI.

Security design issues

Understand and characterise design trade-offs that reconcile security, safety and privacy of IoT; develop techniques for characterising further trade-offs such as power consumption versus security, or longevity versus affordability; understand how the human element needs to be considered in the design of security and in achieving security and safety trade-offs; ensure interoperability that allows for end-to-end security.

New methods of threat analysis

Develop threat modelling and analysis techniques that can represent human, physical and cyber aspects of a system; determine how such techniques might inform the selection of countermeasures and inform how to balance protection of a system between its human, physical and cyber aspects; develop methods to determine the risks and impacts of compromise.

Risk management in critical infrastructure

Explore whether new risk assessment practices should be adopted where IoT is applied in critical infrastructure; explore whether IoT will change how critical infrastructure is defined; investigate whether IoT will emerge as a critical infrastructure or produce new categories of critical infrastructure, and how policy challenges compare to other utilities; determine how the burden for implementing, monitoring and enforcing privacy and security measures should be distributed between private and public entities.

Organisational decision-making

Generate evidence and develop methods to help organisations improve decision-making around security and IoT; generate evidence to help organisations balance the cost of implementing security measures with the risk mitigation outcomes.

Adoption, societal implications and implementation

Adoption

Understand factors that influence IoT adoption including consumers' incentives and motivation; develop new methodologies and design approaches appropriate to IoT that extend user-centred design approaches so that products and services are driven by user expectations, technical feasibility, and notions of desirability; understand usability and how consumers might adopt and manage multiple, connected devices, services and accounts; develop a framework to map IoT stakeholders, including individuals, businesses, regulators and governments, requirements across application domains.

Consumer trust in IoT

Understand trust and how to foster it in consumers; understand the role of technical and data literacy in promoting trust; understand people's perceptions of security and privacy risks and the influence of high-profile security events; understand whether people trust automated systems and the underlying algorithms, and the point at which it is appropriate not to be in control; determine how to improve trust in autonomous systems and algorithms; develop tools for people to understand and manage what data is being collected about them, the consequences of data sharing, and the value and utility of their data.

Consent

Understand how the principle of 'free and informed consent' stands in the context of IoT and aligns with legislation and guidance; develop forms of consent appropriate to IoT technology and context of use; characterise where consent is needed or where it is not appropriate; develop ways of communicating to users what they are consenting to and consequences of giving or withholding consent.

Privacy-enhancing techniques

Develop data encryption techniques suitable for IoT; develop anonymity models for data management in IoT, for example to protect privacy during data exchange; develop privacy lifecycle management mechanisms for smart things; understand how to achieve 'unlinkability' for data privacy; understand how to enhance users' control over their location information, its disclosure, use and combination.

Ethical issues related to the use of algorithms

Understand factors that influence ethical behaviour of autonomous decision-making, including machine learning and AI – for example, how the respective roles of developers in specifying parameters and users in configuring them might prioritise some values and interests over others.

Societal Implications

Study the effect of IoT for diverse communities, in particular underrepresented, discriminated or underprivileged groups; assess IoT's scope to facilitate, enhance or worsen (inter)national surveillance and censorship dynamics; analyse the longitudinal consequences of emerging technologies on societal structures, behaviours and cohesion.

Annex 2: Acknowledgements

The report was overseen and written by a working group:

Paul Taylor FREng, UK Lead Partner - Cyber Security, KPMG and Chair of the working group

Dr Steve Allpress FREng, CEO, Folio Intelligence

Dr Madeline Carr, Standards Governance and Policy Co-lead, PETRAS and Associate Professor of International Relations and Cyber Security, UCL, STEaPP

Professor Emil Lupu, Deputy Director, PETRAS and Professor of Computer Systems, Imperial College London

Professor Jim Norton FREng, Chair, Royal Academy of Engineering Community of Practice in Digital Systems

Dr Liane Smith FREng, VP Digital Solutions, Wood

with support (including authorship) from the following:

Dr Philippa Westbury, Senior Policy Advisor, Royal Academy of Engineering

Dr Robert J Thompson, Impact Fellow, PETRAS

Ms Graça Carvalho, Impact Champion, PETRAS

The working group acknowledge the following PETRAS academics who undertook the original State of the Art and Gap analyses that formed the stimulus content for this report and provided further contributions throughout the report writing process.

Dr Jason Blackstock (UCL), Hugh Boyes (University of Warwick), Prof. Andy Hudson-Smith (UCL), Dr Irina Brass (UCL), Dr Hassan Chizari (Imperial College), Prof. Rachel Cooper OBE (Lancaster University), Prof. Paul Coulton (Lancaster University), Dr Barney Craggs (University of Bristol), Prof. Nigel Davies (Lancaster University), Prof. David De Roure (University of Oxford), Prof. Miles Elsden (UCL), Prof. Michael Huth (Imperial College London), Joseph Lindley (Lancaster University), Prof. Carsten Maple (University of Warwick), Dr Brent Mittelstadt (University of Oxford), Dr Razvan Nicolescu (Imperial College London), Dr Jason Nurse (University of Oxford), Prof. Rob Procter (University of Warwick), Dr Petar Radanliev (University of Oxford), Prof. Awais Rashid (University of Bristol), Dr Daniele Sgandurra (Royal Holloway), Dr Anya Skatova (University of Bristol), Dr Mariarosaria Taddeo (University of Oxford), Dr Leonie Tanczer (UCL), Rodrigo Vieira-Steiner (Imperial College), Prof. Jeremy Watson CBE FREng (UCL), Dr Sandra Wachter (University of Oxford), Dr Susan Wakenshaw (University of Warwick).

The report should be referenced as follows:
Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H., Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, D., Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B., Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A., Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R., Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., Thompson, R.J., Westbury, P.S., (2018). *Internet of Things: realising the potential of a trusted smart world*. Royal Academy of engineering: London.

The working group would like to thank the following peer reviewers:

Professor Robin Bloomfield FREng, Founding Partner, Adelard LLP and Professor of System and Software Dependability, City, University of London

Professor Joe Butler, Chief Scientific Advisor, Department for Digital, Culture, Media and Sport

Professor Mischa Dohler FREng, Director, Centre for Telecommunications Research, King's College London

Dr Lina Huertas, Head of Technology Strategy for Digital Manufacturing, Manufacturing Technology Centre

Professor Adam Joinson, Professor of Information Systems, School of Management, University of Bath

Professor Derek McAuley, Professor of Digital Economy, School of Computer Science, University of Nottingham

Professor Sir John V McCanny CBE FREng FRS, Regius Professor Emeritus, Electronics and Computer Engineering, Queen's University Belfast

Professor Martyn Thomas CBE FREng, IT Livery Company Professor of Information Technology, Gresham College

Cheryl W, Research & Innovation, GCHQ

References and endnotes

1 'Public space' describes places that are open and accessible to the public such as streets, motorways, city squares and other pedestrian areas, parks and neighbourhood spaces. Public space IoT applications include smart cities and intelligent mobility.

2 'Internet of Things Cybersecurity Improvement Act of 2017'

3 The Global Conference on Cyberspace (GCCS) is referred to as the London Process because it was launched in London in 2011. GCCS aims to establish internationally agreed 'rules of the road' for behaviour in cyberspace, and to create a dialogue between governments, civil society and industry on how to implement them.

4 Department for Business, Energy and Industrial Strategy (November 2017), *Industrial strategy: building a Britain fit for the future*, www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future

5 Department for Business, Energy and Industrial Strategy (October 2017), *Made Smarter*, www.gov.uk/government/publications/made-smarter-review

6 National Infrastructure Commission (December 2017), *Data for the public good*, www.nic.org.uk/publications/data-public-good

7 Hall, W. and Pesenti, J. (October 2017), *Growing the artificial intelligence industry in the UK*, www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

8 SIG Robotics and autonomous systems (July 2014), *RAS 2020, Robotics and autonomous systems*, connect.innovateuk.org/documents/2903012/16074728/RAS%20UK%20Strategy

9 Infrastructure and Projects Authority (March 2016), *National Infrastructure Delivery Plan 2016–2021*, www.gov.uk/government/publications/national-infrastructure-delivery-plan-2016-to-2021

10 These could include the Digital Catapult, the High Value Manufacturing Catapult, the Energy Systems Catapult, the Transport Systems Catapult, the Satellite applications Catapult and/or the Future Cities Catapult.

11 Industrial strategy White Paper, www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future

12 Digital Skills Partnership is a government-led initiative involving business, charities and voluntary organisations to facilitate coordination between digital skills programmes, including the sharing of knowledge and best practice.

13 Department for Digital, Culture, Media and Sport and The Rt Hon Karen Bradley MP (March 2017), *UK Digital Strategy*, www.gov.uk/government/publications/uk-digital-strategy

14 For example, the Engineering Council's *Guidance on Security* advocates a security-minded approach, www.engc.org.uk/security

15 The Article 29 Data Protection Working Party has developed guidelines in relation to GDPR. It closed a consultation on guidelines on consent in January 2018, ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

16 Royal Academy of Engineering and Engineering the Future (April 2017), *Engineering an economy that works for all Engineering the Future*, www.raeng.org.uk/publications/responses/engineering-an-economy-that-works-for-all

17 Government Office for Science (December 2014), *Internet of things: making the most of the second digital revolution*, www.gov.uk/government/publications/internet-of-things-blackett-review

18 Royal Academy of Engineering (2018), *Cyber safety and resilience: strengthening the foundations of the modern economy*.

19a An 'embedded system' is a specialized computer system that is part of a larger system, device or machine.

19b This definition was informed by the following paper: Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (forthcoming). *The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape*. In R. Ellis & V. Mohan (Eds.), Cybersecurity Governance. Wiley.

20 World Economic Forum (January 2015), *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*, www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

21 World Economic Forum (January 2015), *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*, www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

22 European Commission (2014), *Definition of a research and innovation policy leveraging cloud computing and IoT combination*, Final report: a study prepared for the European Commission DG Communications Networks, Content & Technology.

23 McKinsey, *Creating a successful Internet of Things data marketplace*, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace

24 For example, Databox: EPSRC Project on privacy-aware personal data platform, www.databoxproject.uk/about/; for example, Hub-of-all-things, hubofallthings.com

25 Wired Insights, *IoT won't work without artificial intelligence*, www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence

26 For example, kickstarter www.kickstarter.com or indigogo www.indiegogo.com

27 Telit www.telit.com

28 Teezle www.teezle.com

29 European Commission (2014), *Definition of a research and innovation policy leveraging cloud computing and IoT combination*, Final report: a study prepared for the European Commission DG Communications Networks, Content & Technology.

30 Government Office for Science (December 2014), *Internet of things: making the most of the second digital revolution*, www.gov.uk/government/publications/internet-of-things-blackett-review

31 Department for Digital, Culture, Media and Sport and The Rt Hon Karen Bradley MP (March 2017), *UK Digital Strategy*, www.gov.uk/government/publications/uk-digital-strategy

32 In addition to assets, technology, processes and organisation, people also generate data through consumer IoT devices and through their digital footprints more broadly.

33 HM Government (November 2017), *Industrial Strategy: Building a Britain fit for the future*, www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future

34 National Infrastructure Commission (December 2017), *Data for the public good*, www.nic.org.uk/publications/data-public-good

35 This follows the government's invitation to sectors to produce a clear proposal for boosting the productivity of their sector: *Industrial Strategy Green Paper* (January 2017), www.gov.uk/government/consultations/building-our-industrial-strategy

36 BEIS (October 2017), *Made Smarter*, www.gov.uk/government/publications/made-smarter-review

37 *Artificial Intelligence Sector Deal* in HM Treasury

38 SIG Robotics and autonomous systems, (July 2014), *RAS 2020, Robotics and autonomous systems*, connect.innovateuk.org/documents/2903012/16074728/RAS%20UK%20Strategy

39 European Commission (2014), *Definition of a research and innovation policy leveraging cloud computing and IoT combination*, Final report: a study prepared for the European Commission DG Communications Networks, Content & Technology.

40 European Commission (April 2016), *Advancing the Internet of Things in Europe*, Staff working document, SWD(2016) 110 final.

41 European Commission – Justice and fundamental rights, *Data protection in the EU*, https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-protection-eu_en

42 European Commission – Digital single market policies, *The Directive on security of network and information systems (NIS Directive)*, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

43 European Commission (2014), *Definition of a research and innovation policy leveraging cloud computing and IoT combination*, Final report: a study prepared for the European Commission DG Communications Networks, Content & Technology.

44 Consumer IoT could outpace industrial IoT – Gartner and Tech Insider agree on unit forecasts but disagree about buyers (June 2017). Agreement on the huge number of units/devices, but disagreement about where they will go. www.networkworld.com/article/3200134/internet-of-things/consumer-iot-could-outpace-industrial-iot.html

45 www.iotforall.com/consumer-iot-vs-industrial-iot

46 For example, a SCADA system. Supervisory control and data acquisition is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery.

47 See Section 6.2 The decision to process locally or centrally, Royal Academy of Engineering and the Institution of Engineering and Technology (IET) (November 2015), *Connecting data: driving productivity and innovation*, www.raeng.org.uk/publications/reports/connecting-data-driving-productivity

48 Manchester Cityverve is one example of a smart city application, cityverve.org.uk/platform-of-platforms

49 www.iotforall.com/consumer-iot-vs-industrial-iot

50 LPWAN is Low Powered Wide Area Network, NB-IoT Narrowband-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology.

51 Bluetooth will be an important communications technology for wearable products connecting to the internet via smartphones in many cases.

52 Consumer IoT vs. Industrial IoT – What are the Differences? (July 2017) 'From a development and commercial rollout standpoint, they increasingly appear to be parallel ecosystems with significant overlap but also marked differences, players, and innovations'. www.iotforall.com/consumer-iot-vs-industrial-iot

53 www.iotforall.com/consumer-iot-vs-industrial-iot/

54 Operational technology is the hardware and software that controls physical systems.

55 A CE mark is a European certification mark, http://ec.europa.eu/growth/single-market/ce-marking/

56 Department for Transport (February 2017), Vehicle Technology and Aviation Bill, www.gov.uk/government/collections/vehicle-technology-and-aviation-bill

57 Brass, I. qtd in *Royal Society Conference Report, The Internet of Things: Opportunities and Threats*, p. 12, Publication available: royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf

58 Brass, I., Tanczer, L., Carr, M., Elsden, M. and J. Blackstock (2017), *IoT Security - A Review of the Regulatory and Standards Landscape*. The Royal Society, The Internet of Things: Opportunities and Threats. Video available: www.youtube.com/watch?v=3uh1UHsNmek

59 This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted on 16 September 2014, ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

60 A full list of guidelines issued by Article 29 Working Party is available here: ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

61 Internet of Things Cybersecurity Improvement Act of 2017. This US bill aims to 'provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes'. www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

62 Thomas, L.D.W. and Leiponen, A. (2016), Big data commercialization, *IEEE Engineering Management Review*, 44, December 2016.

63 European Commission (January 2017), *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy*, SWD (2017) 2 final.

64 For example, this happened in the competition between VHS and Betamax standards.

65 An ethical standard is a set of standard principles and/or procedures that encourage values such as trust and fairness.

66 GMP Swann (2010), *The Economics of Standardization: an update*, Report for the UK Department of Business, Innovation and Skills (BIS).

67 Royal Academy of Engineering and IET (2015), *Connecting data: driving productivity and innovation*, www.raeng.org.uk/publications/reports/connecting-data-driving-productivity

68 The IIC Industrial Security Framework, available here: http://www.iiconsortium.org/wc-security.htm

69 Brass,I., Tanczer, L., Carr, M., Elsden M., and J. Blackstock (2017) *IoT Security: Standards and Guidelines Landscape Mapping*, Report submitted to the Expert Advisory Group of the UK Government Department for Digital, Culture, Media and Sport. Publication available upon request.

70 openconnectivity.org/certification/ocf-certification

71 www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/IoT-Assurance-Services

72 eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

73 A reference architecture provides a template solution for architecture for a particular domain. It also provides a common vocabulary with which to discuss implementation.

74 Carr, M. 2016. 'Public Private Partnerships in National Cybersecurity Strategies'. *International Affairs*. 92(1).

75 Toni Erskine and Madeline Carr. 2016. 'Beyond "Quasi-Norms": The Challenges and Potential of Engaging with Norms in Cyberspace' in *International Cyber Norms: Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Roigas (eds). Tallinn: NATO CCD COE Publications.

76 The Global Conference on Cyberspace (GCCS) is referred to as the London Process because it was launched in London in 2011. GCCS aims to establish internationally agreed 'rules of the road' for behaviour in cyberspace, and to create a dialogue between governments, civil society and industry on how to implement them.

77 Tanczer, L., Yahya, F., Brass, I., Elsden, M., Blackstock, J., & Carr, M., (2017). *International Developments on the Security of the Internet of Things*. PETRAS IoT Hub, Department for Digital, Culture, Media and Sport (DCMS): London.

78 A systems approach will help to identify the roles of the various systems and the interdependencies between them. An integrated high-level perspective will be needed, alongside a recognition that each part of the system must have local autonomy to function effectively. Such an approach will also help to gather a wide range of perspectives from stakeholders to build a common purpose.

79 Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (forthcoming). The United Kingdom's Emerging Internet of Things (IoT) Policy and Legislative Landscape. In: R., Ellis & V., Mohan, *Rewired: Cybersecurity Governance*. Wiley.

80 A sunset clause is a provision of a law that will automatically be terminated after a fixed period unless it is extended by law.

81 Brass, I., Tanczer, L. M., Carr, M., & Blackstock, J. (2017). Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things? *Risk & Regulation* Magazine of the Centre for Analysis of Risk and Regulation (CARR), 33(Summer), 12–15.

82 Durrant-Whyte, H., Geraghty, R., Pujol, F. and Sellschop, R. (November 2015), *How digital innovation can improve mining productivity*, McKinsey article, www.mckinsey.com/industries/metals-and-mining/our-insights/how-digital-innovation-can-improve-mining-productivity

83 Talk by Hugh Durrant-Whyte at the Royal Society conference on the Internet of Things, October 2017.

84 Royal Academy of Engineering and IET (2015), *Connecting data: driving productivity and innovation*, www.raeng.org.uk/publications/reports/connecting-data-driving-productivity

85 Accenture Report. 2015. Driving Unconventional Growth through the Industrial Internet of Things.

86 KPMG (2017), *The changing landscape of disruptive technologies, Part 2 – Innovation convergence unlocks new paradigms*, info.kpmg.us/content/dam/info/tech-innovation/disruptive-tech-2017-part2.pdf

87 McKinsey Global Report (2015), *Unlocking the potential of the internet of things*, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

88 World Economic Forum (January 2015), *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*, www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

89 The World Economic Forum suggests that in an 'outcome economy', companies will shift from competing through selling products and services, to competing on delivering measurable results important to the customer.

90 Consumers International, *Testing our trust: consumers and the Internet of Things*, 2017 Review, www.consumersinternational.org/media/154746/iot2017review-2nded.pdf

91 Breidbach, C.F. and Maglio, P.P. (2016). Technology-enabled value co-creation: An empirical analysis of actors, resources, and practices. *Industrial Marketing Management*, 56: 73-85.

92 Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7): 1645–1660.

93 Wired (October 2017), *The Little Black Box that Took Over Piracy*, www.wired.com/story/kodi-box-piracy

94 Trusted Reviews (December 2017), *The Kodi Box crackdown is doomed to fail*, www.trustedreviews.com/opinion/kodi-box-crackdown-illegal-sports-streaming-sky-bt-addons-3346917

95 Nurse, J. R., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT Professional*, 19(5), 20-26.

96 In October 2016, attackers mounted concurrent global DDoS attacks on internet services firm Dyn, using IoT devices. The attack severely impacted Dyn's clients, which include Twitter, Reddit, Spotify, SoundCloud, among others. www.ibtimes.co.uk/massive-ddos-attack-that-almost-brought-down-us-internet-how-it-happened-why-1587696

97 Grangel-González, I., Halilaj, L., Coskun, G., Auer, S., Collarana, D. and Hoffmeister, M. (2016), *Towards a Semantic Administrative Shell for Industry 4.0 Components*, 2016 IEEE Tenth International Conference on Semantic Computing (ICSC), ieeexplore.ieee.org/document/7439338

98 Mineraud, J., Mazhelis, O., Su, X., and Tarkoma, S., 2016. *A Gap Analysis of Internet-of-Things Platforms*. Computer Communications. 89(C): 5-16.

99 These include IoT-capable management tools.

100 An IoT marketplace brings together in a website information about compatible products and services from several IoT suppliers, helping suppliers to promote their products and customers to choose an IoT solution.

101 Telus IoT marketplace, https://iot.telus.com/en/business/on/

102 ThingWorx IoT marketplace, https://marketplace.thingworx.com/

103 Huth, M., et. al. 2016. 'From Risk Management to Risk Engineering: Challenges in Future ICT Systems.' In Griffor, E., ed., *Handbook of System Safety and Security*, p. 131-174.

104 Royal Academy of Engineering and IET (2015), *Connecting data: driving productivity and innovation*, www.raeng.org.uk/publications/reports/connecting-data-driving-productivity

105 Tanczer, L., Brass, I., Carr, M., Blackstock, J., 2017. Consent Workshop Report, proceedings of a workshop on IoT and Consent, jointly hosted by Pinsent Masons and PETRAS.

106 Royal Academy of Engineering and IET (2015), *Connecting data: driving productivity and innovation*, www.raeng.org.uk/publications/reports/connecting-data-driving-productivity\

107 The 'data controller' determines the purposes and means of the processing of personal data, while the 'data processor' processes personal data on behalf of the controller.

108 For example, ISO 15926: Building Smart IFCs.

109 For example, McKinsey (October 2013), *Open data: Unlocking innovation and performance with liquid information.*

110 McKinsey (October 2016), *Creating a successful Internet of Things data marketplace.*

111 Thomas, L.D.W and Leiponen, A (2016), *Big data commercialisation*, IEEE Engineering Management Review, Vol 44, Issue 2.

112 For example, Industrial Data Space, www.industrialdataspace.org/en and https://cityverve.org.uk/platform-of-platforms/

113 Aerospace journal, August 2015, *Big data in the aerospace sector*, Royal Aeronautical Society.

114 Klaschka, R. (2015), *Our buildings, our data... maybe not*, CIBSE Journal, July 2015.

115 Pinsent Masons (May 2017), *Connected and autonomous vehicles: the emerging legal challenges*, www.pinsentmasons.com/PDF/2017/Freedom-to-Succeed-AMT/Connected-autonomous-vehicles-report-2017.pdf

116 European Commission (January 2017), *The free flow of data and emerging issues of the European data economy*, Commission staff working document, Brussels, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy

117 The plain English version of Facebook's terms and conditions were published by the Children's Commissioner for England and TES in October 2017 to help children understand the implications of signing a contract to use the social media platforms from age 13, www.tes.com/teaching-resources/digital-citizenship

118 The UK Data Protection Bill requires the Information Commissioner to prepare an 'age-appropriate design code' for internet services, as proposed in amendments brought by Baroness Kidron (January 2018).

119 A recent study of travellers' attitudes to intelligent mobility by the Transport Systems Catapult found that 57% of respondents would not mind sharing their personal data to get a better service.

120 The Hub-of-All-Things, http://hubofallthings.com

121 Databox project is developing a privacy-aware data analytics platform to collate, curate, and mediate access to personal data, www.databoxproject.uk

122 Digital Prosumer is developing a platform that allows individuals to take control of the monetisation of their personal data, www.digitalprosumer.co.uk

123 European Commission Horizon 2020, Responsible Research and Innovation, https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

124 ORBIT: The Observatory for Responsible Research and Innovation in ICT, https://www.orbit-rri.org/about-rri/

125 HM Government (November 2017), *Industrial Strategy: Building a Britain fit for the future*, www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future

126 Royal Society (November 2017), *After the reboot: computing education in UK schools*, https://royalsociety.org/~/media/policy/projects/computing-education/computing-education-report.pdf

127 The development of the revised computing curriculum was initiated in September 2012: Royal Academy of Engineering, *DfE invite BCS and RAEng to co-ordinate the revised programmes of study for ICT*, www.raeng.org.uk/news/news-releases/2012/September/dfe-invite-bcs-and-raeng-to-co-ordinate-for-ict

128 Royal Academy of Engineering and Engineering the Future (April 2017), *Engineering an economy that works for all: Industrial Strategy Green Paper response*, www.raeng.org.uk/publications/responses/engineering-an-economy-that-works-for-all

129 www.ucl.ac.uk/ucl-east/academic_vision/the-shared-vision

130 The Cybersecurity Body of Knowledge is a comprehensive Body of Knowledge to inform and underpin education and professional training for the cybersecurity sector, www.cybok.org

131 Science and Technology Committee. (2016). *Digital skills crisis: Second Report of Session 2016–17* (No. HC 270) (pp. 1–51). London: House of Commons. Retrieved from: https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf

132 Luis Martínez-Cantos, J., 2017. *Digital skills gaps: A pending subject for gender digital inclusion in the European Union*. Eur. J. Commun. 267323117718464. doi:10.1177/0267323117718464

Guardian, 2016. 'Gender gap in UK degree subjects doubles in eight years', Ucas study finds. *Guardian*, www.theguardian.com/education/2016/jan/05/gender-gap-uk-degree-subjects-doubles-eight-years-ucas-study

Weingarten, E., Garcia, M.E., 2015. *Decrypting the Cybersecurity Gender Gap*. New America, Washington D.C.

Vitores, A., Gil-Juárez, A., 2016. 'The trouble with "women in computing": a critical examination of the deployment of research on the gender gap in computer science'. *J. Gend. Stud.* 25, 666–680.

133 In relation to individuals, cyber hygiene describes the measures that individuals need to take to maintain their online safety.

134 For example, in the case of Zigbee, a wireless technology developed as an open global standard.

135 Sohrabi Safa, N.S. and Maple, C. (2016), Human errors in the information security realm – and how to fix them, Computer Fraud & Security, Volume 2016, Issue 9, Pages 17-20.

136 For example: Adams, A. and Sasse, M.A (1999), Users are not the enemy, *Communications of the ACM* 42.12 (1999): 40-46.

137 Craggs, B. and Rashid, A. (2017), *Smart cyber-physical systems: Beyond usable security to security ergonomics by design*, Software Engineering for Smart Cyber-Physical Systems Workshop at International Conference on Software Engineering 2017: 22-25.

138 For example, HFACS, the 'human factors analysis and classification system', is a tool used in engineering applications to understanding why and how a security event occurred, and the corresponding human and environmental causal factors. HFACS applied to cybersecurity would provide a means of ensuring that a more optimised set of design principles could be applied to future implementations of IoT, as long as an adequate definition of security for IoT is developed.

139 S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi, The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game, *IEEE Transactions on Software Engineering* (Accepted to Appear), 2018.

140 A. Zanutto, B. Shreeve, K. Follis, J. S. Busby, and A. Rashid, The shadow warriors: In the no man's land between industrial control systems and enterprise IT systems, in Workshop on Security Information Workers, Thirteenth Symposium on Usable Privacy and Security, SOUPS, 2017.

141 Firmware is the set of instructions set of instructions programmed on a hardware device.

142 A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

143 A system has integrity if its intended functions are being performed without degradation or being impaired by other changes or disruptions.

144 Why Johnny doesn't write secure software?: Secure software development by the masses, www.writingsecuresoftware.org This project investigates the security behaviours and decision-making processes of those involved in software development.

145 Nurse, J. R., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. *IT Professional*, 19(5), 20-26.

146 Kleinhans, J. P. (2017). *Internet of Insecure Things. Can Security Assessment Cure Market Failures?* Berlin: Stiftung Neue Verantwortung, www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

147 'Graceful degradation' refers to the ability of a system to maintain limited functionality even when a large portion of it has been destroyed or rendered inoperative, thus preventing catastrophic failure.

148 HM Government (August 2017), *The key principles of vehicle cybersecurity for connected and automated vehicles*, Principle 5.2, www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

149 Nurse, J.R.C., Creese, S. and De Roure, D. (2017), Security risk assessment in Internet of Things systems, *IT Professional*, Volume 19, Issue 5.

150 IT systems are associated with high-level management and resource planning for large organisations, while operations technology systems are those that monitor and control field devices and processes.

151 BEIS (October 2017), *Made Smarter* review, www.gov.uk/government/publications/made-smarter-review

152 For example, Apple's new iWatch 3 has an enhanced heart feature. Startups such as CloudTag are targeting the NHS via medical-grade consumer devices aimed at the health, wellbeing and fitness markets, www.cloudtag.com

153 For example, pacemakers, neuro-stimulators, drug delivery systems and on- and in-body systems of medical devices.

154 Military bases and patrol routes were found to be identifiable based on public data shared by Strava, a social network for athletes. *Wired* (January 2018), The Strava heat map and the end of secrets, www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy

155 GSMA, (2016), *IoT Security Guidelines Overview Document. Version 1.1* (pp. 1–42). unknown: GSM Association, www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf

156 Department for Transport and Maritime and Coastguard Agency (August 2016), *Ports and port systems: cybersecurity code of practice*, www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice

157 HM Government (August 2017), *The key principles of cybersecurity for connected and automated vehicles*.

158 Department for Business, Energy and Industrial Strategy (April 2014), *Cyber Essentials Scheme*, www.gov.uk/government/publications/cyber-essentials-scheme-overview

159 'Cyber hygiene' describes the range of activities undertaken to keep an organisation or function safe and secure, comprising policies and procedures, training and skills development and technology. They are used in combination to ensure that risks are minimised.

160 For example, National Cyber Security Centre risk management collection (August 2016), www.ncsc.gov.uk/guidance/risk-management-collection

161 At present software is presumed to be working correctly in the event of an incident, with the onus on the user, rather than the manufacturer, to prove that it was at fault.

162 For example, ISO/IEC 27000 is part of a growing family of ISO/IEC information security management systems (ISMS) standards.

163 NCSC Cloud security collection (August 2016), www.ncsc.gov.uk/guidance/cloud-security-collection

164 Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (forthcoming). The United Kingdom's Emerging Internet of Things (IoT) Policy and Legislative Landscape. In: R., Ellis & V., Mohan, Rewired: Cybersecurity Governance. Wiley.

165 Urquhart, L. and McAuley, D. (May 2017), *Cybersecurity Implications of the Industrial Internet of Things*, TILTing Perspectives 2017: Regulating a Connected World, Tilburg, Netherlands, 17-19 May 2017. Available at SSRN: https://ssrn.com/abstract=2971991

166 HM Government (August 2017), *The key principles of vehicle cybersecurity for connected and automated vehicles*, Principle 1.4: 'All new designs embrace Security by Design. Secure design principles are followed in developing a secure ITS/CAV System, and all aspects of security (physical, personnel and cyber) are integrated into the product & service development process.' www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

167 National Cyber Security Centre, Secure by default, www.ncsc.gov.uk/articles/secure-default

168 Marsh on behalf of the UK Government (2015), *UK cybersecurity: the role of insurance in managing and mitigating the risk*, https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

169 Tanczer, L., Brass I., Carr M., & Blackstock J. (forthcoming). The Internet's Fire Brigade: Incident Response Teams Collaboration Practices as a Form of Science Diplomacy in Cybersecurity. *Global Policy Journal*. CSIRTs are teams responsible for receiving, reviewing, and responding to computer security incidents and focus on the security of computer systems and/or networks that make up the infrastructure of an organisation. CSIRTs operate for a defined constituency including a variety of entities such as governments, corporations, and educational institutions. PSIRTs are teams within corporate organisations that carry out similar functions to CSIRTs but focus primarily on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products, offerings, solutions, components and/or services that an organisation produces and/or sells.

170 Royal Academy of Engineering (2018), *A safe and resilient future: strengthening the systems that support the modern economy*.

171 For example, Facebook has published its terms and conditions in a form that makes them accessible to children, www.tes.com/teaching-resources/digital-citizenship

172 Lindley, J.G., Coulton, P. & Sturdee, M. (2017), *Implications for Adoption*. in CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, New York, CHI 2017, Denver, United States, 6-11 May. DOI: 10.1145/3025453.3025742

173 Rogers, Everett (16 August 2003). *Diffusion of Innovations, 5th Edition*. Simon and Schuster. ISBN 978-0-7432-5823-4

174 Williams, R., Stewart, J. and Slack, R., 2005. *Social learning in technological innovation: Experimenting with information and communication technologies*. Edward Elgar Publishing.

175 Voß, A., Procter, R. and Williams, R., 2000, December. Innovation in Use: Interleaving day-to-day operation and systems development. In *Proceedings of the Participatory Design Conference* (pp. 192-201).

176 ZDNet (April 2015), *Internet of Things devices lack fundamental security, study finds*, www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds

177 Deontological or duty-based ethics concern what people do, not the consequences of their actions.

178 For example, Engineering Council and the Royal Academy of Engineering (July 2017), *Statement of ethical principles for the engineering profession*, www.raeng.org.uk/publications/reports/statement-of-ethical-principles

179 'Entitlement management' is used to execute fine-grained control of access to data, devices and services.

180 A data subject is the person about whom personal data is being collected, processed and stored.

181 Homomorphic encryption carries out computations on data while the data stays encrypted.

182 Multi-party computation allows different parties to carry out a joint computation and maintains the privacy of the inputs they provide.

183 Differential privacy analyses aggregated data while keeping individuals' data private.

184 Amazon Echo View is a voice-activated smart speaker system with Bluetooth and Wi-Fi connectivity.

185 Kodi boxes are set-top streaming devices. If installed with a Kodi app, they can illegally stream subscription content.

186 For example, the Databox project and the Hub-of-all-things project are exploring this.

187 Department for Digital, Culture, Media and Sport (7 August 2017), *A new data protection bill: our planned reforms, Statement of intent*, https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

188 The BIM Common Data Environment is the single source of information used to collect, manage and disseminate documentation, the graphical model and non-graphical data for the whole project team.

189 The experience regarding BIM is that several common data environment (CDE) suppliers are offering shared repositories for storage of project or asset information that are cloud-based, often located offshore and with a number of tiers of contract between the CDE service provider delivering a software as a service product and the actual hosting company.

190 Tanczer, L., Carr, M., Brass, I., and Blackstock, J. (2017). *White Paper: Consent and its implication for the Internet of Things*. PETRAS IoT Hub, Pinsent Masons: London.

191 Tanczer, L., Carr, M., Brass, I., & Blackstock, J. (2017). *White Paper: Consent and its implication for the Internet of Things*. PETRAS IoT Hub, Pinsent Masons: London.

192 'Informed consent' means that individuals have given their consent to the processing of their data with a clear understanding of how it will be used, and the implications and consequences of giving it. Draft guidance from the Information Commissioner's Office indicates that consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity, and be requested in understandable terms. Information Commissioner's Office Consultation (March 2017), *GDPR consent guidance*, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/

193 'Data minimisation' means that the minimum amount of personal data is held to fulfil a specific purpose, and no more than that.

194 Royal Academy of Engineering and Engineering the Future (April 2017), *Engineering an economy that works for all*, www.raeng.org.uk/publications/responses/engineering-an-economy-that-works-for-all

195 *Wired* (October 2017), *The Little Black Box that Took Over Piracy*, www.wired.com/story/kodi-box-piracy

ROYAL ACADEMY OF **ENGINEERING**

Royal Academy of Engineering

As the UK's national academy for engineering, we bring together the most successful and talented engineers for a shared purpose: to advance and promote excellence in engineering.

We have four strategic challenges:

Make the UK the leading nation for engineering innovation

Supporting the development of successful engineering innovation and businesses in the UK in order to create wealth, employment and benefit for the nation.

Address the engineering skills crisis

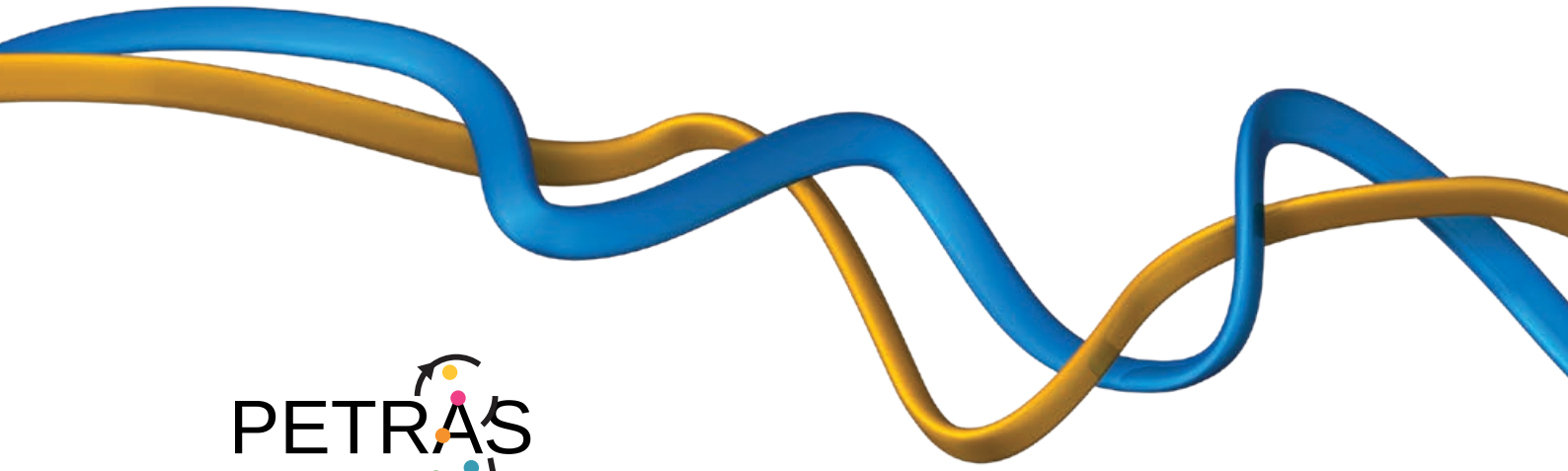
Meeting the UK's needs by inspiring a generation of young people from all backgrounds and equipping them with the high quality skills they need for a rewarding career in engineering.

Position engineering at the heart of society

Improving public awareness and recognition of the crucial role of engineers everywhere.

Lead the profession

Harnessing the expertise, energy and capacity of the profession to provide strategic direction for engineering and collaborate on solutions to engineering grand challenges.



PETRAS

The **PETRAS** Cybersecurity of the Internet of Things Research Hub is funded by the Engineering and Physical Sciences Research Council (EPSRC) to explore critical issues of Privacy, Ethics, Trust, Reliability, Acceptability, and Security (PETRAS) relating to the Internet of Things (IoT). The Hub brings together nine leading UK universities, (University of Warwick, University of Oxford, Lancaster University, University of Surrey, University College London, University of Edinburgh, University of Southampton, Imperial College London, and Cardiff University)

As part of the Government-funded IoT UK research and innovation programme, the Hub is receiving £9.8m funding from the Engineering and Physical Sciences Research Council (EPSRC), which is match funded by £14m and participation from over 120 academic, industrial and public-sector partners. The hub was announced on the 6th January 2016.

The hub looks at both social and technological issues, bringing together research leaders, industry, the public and voluntary sectors. In bringing together this community, the research hub is able to gain a thorough understanding of PETRAS issues in terms of the needs and potentially conflicting interests of government, industry and academia. This enables the hub to be a leader in the development and innovation of IoT, and an authority and influencing voice in the cybersecurity of IoT.

www.petrashub.org | Twitter@PETRASiot

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG
Tel: +44 (0)20 7766 0600
www.raeng.org.uk

Registered charity number 293074