



# Accelerating the Internet of Things in the UK

Using Policy to Support Practice

Salil Gunashekar, Anton Spisak, Kevin Dean,  
Nathan Ryan, Louise Lepetit, Paul Cornish

For more information on this publication, visit [www.rand.org/t/rr1492](http://www.rand.org/t/rr1492)

This research was commissioned by IoTUK and BCS, The Chartered Institute for IT

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© Copyright 2016 RAND Corporation

RAND® is a registered trademark.

RAND Europe is a not-for-profit organisation whose mission is to help improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

**Limited Print and Electronic Distribution Rights**

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit [www.rand.org/pubs/permissions.html](http://www.rand.org/pubs/permissions.html).

Support RAND  
Make a tax-deductible charitable contribution at  
[www.rand.org/giving/contribute](http://www.rand.org/giving/contribute)

[www.rand.org](http://www.rand.org)  
[www.randeurope.org](http://www.randeurope.org)

# Preface

---

The enormous growth in the number of Internet-connected ‘things’ around the world today has resulted in the Internet of Things (IoT) emerging as a critical area of interest to policymakers. Many countries, including the United Kingdom (UK), now regard the IoT as a highly significant, strategic-level infrastructure for economic growth. As a result, the IoT has been receiving considerable attention from industry, universities and government. However, to drive adoption of the IoT, it is also important to understand public attitudes to IoT applications and to identify where the public’s concerns may not be aligned with the research and business objectives of the IoT. The central aim of this study is to support a process for policy feedback that will inform the development and adoption of the IoT in the UK. We adopted a bottom-up approach that allowed us to bring together inputs from businesses and individual users of technology, enabling us to get a better idea of what is happening ‘on the ground’ in the UK. Specifically, we (i) examined the policy implications of a selection of ‘real world’ IoT case studies in the UK; (ii) surveyed a sample of informed users of technology to gauge their awareness of and views on the key policy-relevant issues related to the advancement of the IoT in the UK; and (iii) examined our findings from the case studies and the survey to generate a set of topics with supporting questions for further exploration and discussion by the policy community in the UK. While the topics for discussion and questions that follow from our findings are primarily aimed at the community of policymakers, the implications of these findings seek to provoke discussion across policy communities, including government policymakers (national and local), innovators, industry, academia and the public.

RAND Europe is a not-for-profit policy research organisation that helps to improve policy and decisionmaking in the public interest, through research and analysis.<sup>1</sup> RAND Europe’s clients include European governments, institutions, NGOs and firms with a need for rigorous, independent, multi-disciplinary analysis.

This document has been peer reviewed in accordance with RAND Europe’s quality assurance standards and as such can be portrayed as a RAND Europe document.<sup>2</sup>

For more information about RAND Europe or this document, please contact:

Dr Salil Gunashekar  
RAND Europe, Westbrook Centre,  
Milton Road, Cambridge CB4 1YG,  
United Kingdom  
Telephone: +44 (1223) 353 329  
E-mail: [sgunashe@rand.org](mailto:sgunashe@rand.org)

---

1 For more information on RAND Europe, please see <http://www.rand.org/randeuropa.html> (as of 10 March 2016)

2 For more information on RAND’s quality standards, please see <http://www.rand.org/standards.html> (as of 10 March 2016)



# Table of contents

---

<b>Preface</b>	<b>i</b>
<b>Table of contents</b>	<b>iii</b>
<b>List of figures</b>	<b>v</b>
<b>List of tables</b>	<b>vi</b>
<b>List of acronyms</b>	<b>vii</b>
<b>Executive summary</b>	<b>ix</b>
<b>Acknowledgements</b>	<b>xix</b>
<b>Chapter 1: Introduction</b>	<b>1</b>
<i>1.1 Background</i>	1
<i>1.2 Research objectives</i>	4
<i>1.3 Outline of report</i>	5
<b>Chapter 2: Study design and methods</b>	<b>7</b>
<i>2.1 Study design and scope</i>	7
<i>2.2 Description of methods</i>	7
<i>2.3 Limitations of the analysis</i>	11
<b>Chapter 3: Results from the analysis of the case studies</b>	<b>13</b>
<i>3.1 Introduction</i>	13
<i>3.2 Findings from the analysis of the case studies</i>	14
<b>Chapter 4: Results from the analysis of the survey</b>	<b>27</b>
<i>4.1 Introduction</i>	27
<i>4.2 Findings from the survey</i>	28
<b>Chapter 5: Suggested topics for policy discussion</b>	<b>39</b>
<i>5.1 Introduction</i>	39
<i>5.2 Priority topics for further consideration and key policy questions</i>	39
<b>Chapter 6: Concluding remarks</b>	<b>51</b>
<b>References</b>	<b>53</b>
<b>Appendix A: Illustrations of the IoT in action in the UK</b>	<b>57</b>
<b>Appendix B: Semi-structured protocol for case study interviews</b>	<b>61</b>
<b>Appendix C: List of case study interviewees</b>	<b>65</b>

<b>Appendix D: Survey protocol for Professional and Chartered members of BCS, The Chartered Institute for IT</b>	<b>67</b>
<b>Appendix E: Rapid policy review: Actions of the UK government related to the IoT</b>	<b>73</b>
<b>Appendix F: Relationship between the findings from the case studies and the survey, and the proposed topics for discussion by the policy community</b>	<b>77</b>

# List of figures

---

Figure 1:	Geographic locations of the nine IoT-related case studies examined in the study	xi
Figure 2:	Study phases and associated methodologies used in the research	xii
Figure 3:	Study phases and associated methodologies used in the research	8
Figure 4:	Diagram showing the steps involved in the research	12
Figure 5:	Respondents' perceptions of what represent examples of IoT applications	28
Figure 6:	Word cloud showing the most frequently occurring words in the survey responses to the question 'What do you consider to be the "best" example of an Internet of Things application?'	29
Figure 7:	Respondents' perceptions of which sectors are most likely to benefit from the IoT	30
Figure 8:	Respondents' perceptions of what are the most important benefits of the IoT	31
Figure 9:	Respondents' perceptions of what are the most important barriers to wider adoption of the IoT	32
Figure 10:	Respondents' perceptions of the security implications associated with the IoT	33
Figure 11:	Respondents' perceptions of which security threats are most likely to be associated with the IoT	33
Figure 12:	Respondents' perceptions of the privacy implications associated with the IoT	34
Figure 13:	Respondents' perceptions of the data sharing aspects of the IoT	35
Figure 14:	Respondents' perceptions of what the role of government should be in relation to the IoT	36
Figure 15:	Respondents' perceptions of the most important priorities for the government to stimulate the IoT	37
Figure 16:	Geographic locations of the nine IoT-related case studies examined in the study	60

# List of tables

---

Table 1:	Summary of the findings from the case studies and survey	xiii
Table 2:	The proposed priority topics for discussion and the associated key policy questions	xv
Table 3:	Examples of enabling factors identified by interviewees for developing and adopting IoT applications in the UK	15
Table 4:	Examples of barriers identified by interviewees to developing and adopting IoT applications in the UK	17
Table 5:	The proposed priority topics for discussion and the associated key policy questions	49
Table 6:	Summary descriptions of the nine IoT-related case studies examined in the study	57
Table 7:	List of case study interviewees	65
Table 8:	Actions of the UK government related to the IoT over the past five years	73
Table 9:	Relationship between the key findings from the case studies and the proposed priority topics for discussion by the policy community	77
Table 10:	Relationship between the key findings from the survey and the proposed priority topics for discussion by the policy community	78



# List of acronyms

AHSN NENC	Academic Health Science Network for the North East and North Cumbria
API	application program interface
BIS	Department for Business, Innovation and Skills
BSI	British Standards Institution
CMA	Competition & Markets Authority
CPNI	Centre for the Protection of National Infrastructure
DCMS	Department for Culture, Media and Sport
EPSRC	Engineering and Physical Sciences Research Council
IoT	Internet of Things
ITU	International Telecommunication Union
M2M	machine-to-machine
NHS	National Health Service
NSTAC	National Security Telecommunications Advisory Committee
R&D	research and development
RFID	radio frequency identification
ROI	return on investment
SME	small to medium-sized enterprise
TSB	Technology Strategy Board (now known as Innovate UK)
UK	United Kingdom
UKTI	UK Trade & Investment



# Executive summary

---

## Background and context

The promise of technology is as unchanging as it is alluring: to improve our lives and well-being in ways we have not yet imagined possible. The current iteration of that promise is upon us: the Internet of Things (IoT). Connecting the physical and virtual worlds underpins the ambition of the IoT. The enormous growth in the number of connected ‘things’ around the world today has resulted in the IoT emerging as a critical area of interest to policymakers. Many countries, including the United Kingdom (UK), now regard the IoT as a highly significant, even strategic-level infrastructure for economic growth. As a result, the IoT has been receiving considerable attention from industry, universities and government alike. Furthermore, consumers have a growing awareness of the connected devices and sensors that enable the IoT, mainly through domestic equipment (e.g. smart TVs and Internet-accessible home security and control systems for heating and lighting).

It is evident the IoT holds the potential for major economic opportunities across a wide variety of consumer and industrial sectors; however, there are important horizontal policy issues that affect the development and adoption of the IoT across these sectors. With a growing body of IoT projects and commercial activities in the UK, there is a need to use evidence from ‘real world’ IoT implementations to inform policy in this rapidly emerging area. Furthermore, the significance of involving consumers of technology in informing IoT policy and in decisionmaking cannot be overestimated, particularly when key decisions are to be made which touch upon such issues as privacy, security and trust. Clearly, there are numerous challenges that will require integrated and consistent policy responses across government. Indeed, the IoTUK initiative, launched in 2015 and tasked with accelerating the UK’s IoT capability, is an important step in this direction (IoTUK 2016a).

## Research objectives

Against this backdrop, the central aim of this study, which was commissioned by IoTUK and BCS, The Chartered Institute for IT (hereafter referred to as the Institute), is to support a process for policy feedback that will inform the development and adoption of the IoT in the UK. We adopted a bottom-up approach that allowed us to bring together input from businesses and individual users of technology, enabling us to get a better idea of what is happening ‘on the ground’ in the UK. Specifically, we (i) examined the policy implications of a selection of ‘real world’ IoT projects (hereafter called case studies) in the UK identified by IoTUK<sup>3</sup>; (ii) surveyed a sample of informed users of technology to gauge their awareness

---

3 The case studies we examined in the project were selected by IoTUK on the basis of research commissioned by IoTUK that looked at various examples of IoT implementations across different sectors in the UK. See, for example, IoTUK (2016b) for a summary of some of these projects. Summary descriptions of the nine case studies we examined are provided in Appendix A.

of and views on the key policy-relevant issues related to the advancement of the IoT in the UK; and (iii) examined our findings from the case studies and the survey to generate a set of topics with supporting questions for further exploration and discussion by the policy community in the UK.

## Illustrations of the IoT in action in the UK

Studying specific IoT case studies in depth offers a way to understand what is happening at the frontier of IoT industrial activity in the UK and to extrapolate the likely implications on public policy. In this study, we looked at nine ‘real world’ examples of IoT implementations that had been previously identified by IoTUK. Figure 1 presents a map of the UK with their locations. Some of the case studies we examined have more distinctly IoT-related characteristics than others (for example, in terms of breadth of connectivity and smartness); however, in general, all of them had the potential to be scaled up even further. The case studies span consumer and industrial applications across a wide range of sectors, such as healthcare, energy and environment, transport, retail, and agriculture, and all are examples of IoT-related projects that have been deployed in practice and that have measurable outputs (rather than, for example, being prototypes or demonstrators in a laboratory). In other words, they represent examples of applications that have moved from development to deployment, which allowed us to track their adoption pathways. Furthermore, the case studies have an underlying ‘public benefit’ mission attached to them. We were particularly interested in the implications of these case studies for policy, and we aimed to examine in detail the role of policy to support such projects, which could potentially stimulate the UK’s IoT landscape.

## Methodology

To gain a rounded picture of the potential policy implications of IoT developments in the UK, we adopted a mixed-methods approach to designing the study.<sup>4</sup> Broadly, we conducted the research in three distinct but overlapping phases, as illustrated in Figure 2. In Phase 1, we undertook an in-depth examination of the nine IoT case studies to extract potential policy implications of these implementations. Studying specific IoT implementations in depth offers a way to understand what is happening at the frontline of IoT activity in the UK and to extrapolate the likely implications on public policy. This phase of the study involved a focused review of background documentation associated with each case study, followed by key informant interviews with individuals closely connected to the case studies.<sup>5</sup> In Phase 2 of the study, we carried out an online survey of informed users of technology<sup>6</sup> to gauge their awareness and perceptions of key policy-relevant issues related to IoT developments in the UK.<sup>7</sup> Finally, in Phase 3 of the project, we triangulated the evidence from Phases 1 and 2 against a rapid review of current and previous UK government policy actions related to the IoT. We synthesised our findings to produce a set of wide-ranging policy-relevant topics and

4 A detailed description of the study design and methods used in the research is presented in Chapter 2.

5 The results from the analyses of the case studies are discussed in Chapter 3.

6 The survey was circulated to a random sample of 9,998 Professional and Chartered members (BCS 2016) of the Institute. We made the assumption that this group of users would have a reasonable level of understanding of technology based on their work experience and training.

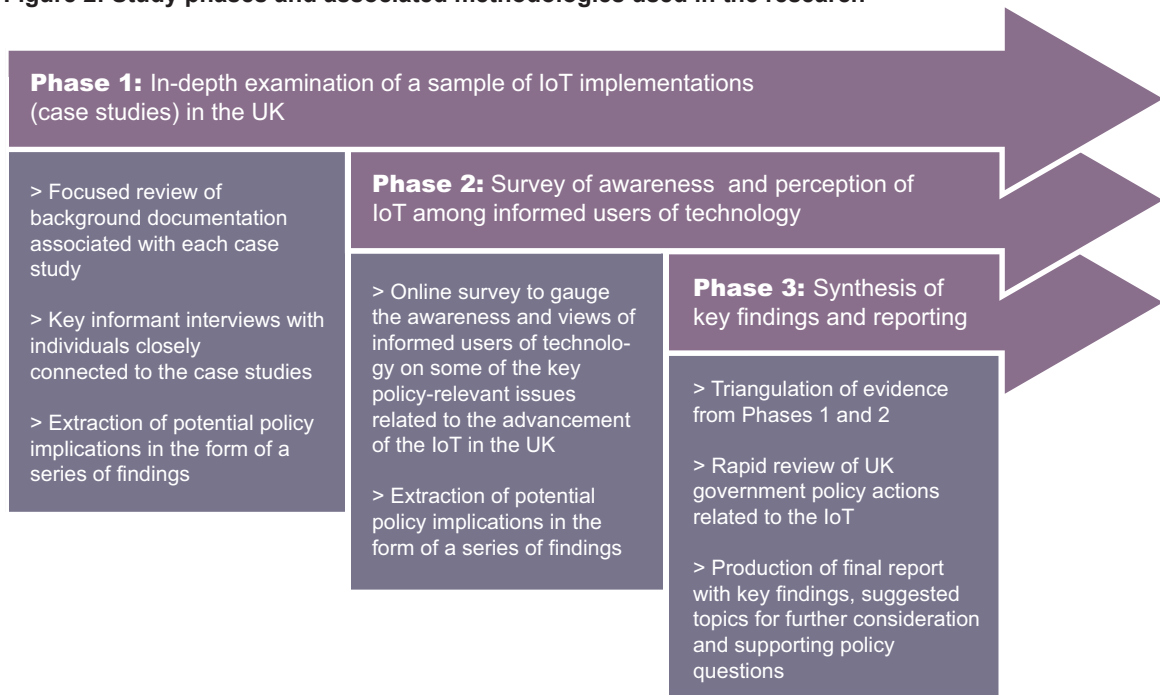
7 The results from the analyses of the survey are discussed in Chapter 4.

supporting questions for further exploration and discussion, which were aimed at provoking discussion across policy communities (including national and local government policymakers, industry, innovators, academia and the public).<sup>8</sup>

**Figure 1: Geographic locations of the nine IoT-related case studies examined in the study**



8 The synthesis of the key findings and the topics for policy discussion and supporting questions are presented in Chapter 5.

**Figure 2: Study phases and associated methodologies used in the research**

## Key findings from the analyses and suggested topics for policy discussion

The key findings from the analyses of the case studies of IoT implementations and the online survey of informed users of technology are presented in Table 1.

The development and adoption of the IoT presents a number of promising opportunities. However, the insights from the analysis of the case studies show several important and challenging research and policy questions arising from the understanding of how IoT-related projects become adopted by the market. Furthermore, the results of the survey clearly demonstrate that it is crucial to take into account the views and opinions of citizens on the key policy-relevant issues regarding the development of the IoT.

By synthesising the findings from the case studies and the survey, we generated a set of policy-relevant priority topics for further exploration and discussion. The topics for discussion we have proposed are grouped into four sets of policy objectives pertaining to the IoT in the UK. These are themes for action aimed at (i) supporting research and innovation in the IoT ecosystem; (ii) stimulating demand for the IoT to be adopted more widely by using IoT solutions in the delivery of public services; (iii) strengthening infrastructure and framework conditions for the development and adoption of the IoT as a systemic innovation; and (iv) mitigating the risks of a pervasive IoT. These themes were triangulated against a rapid review of IoT-related policy actions in the UK over the past five years and represent clustered policy measures or actions that share a common objective.

**Table 1: Summary of findings from the case studies and the survey**

Findings from the case studies of IoT implementations
<ul style="list-style-type: none"> <li>• Non-technical factors are critical to developing and adopting the IoT (e.g. collaborative networks, organisational capabilities and culture, and citizen engagement).</li> <li>• The challenges in developing the IoT market and accelerating its growth are immense, with market uptake and business model–related factors highlighted as the foremost issues.</li> <li>• Demonstrating sustainable business models with a solid return on investment is critical in order to progress the IoT market.</li> <li>• The public sector as a strategic purchaser could accelerate the uptake of IoT technologies, though to do so it will need to ensure that the small and medium enterprises (SMEs) leading IoT markets can participate and are assessed appropriately in procurement processes.</li> <li>• Creating both trust and confidence in the security of data and processes enabled by the IoT is not always aligned with businesses' objectives to innovate and deliver value.</li> <li>• Clear, unambiguous and standardised processes for personal data governance are considered to be prerequisites for linking up systems and for making them interoperable and trustworthy.</li> <li>• IoT innovators' perceptions are mixed over the ability and level of impact of public policy to drive and accelerate the IoT market.</li> </ul>
Findings from the survey of informed users of technology
<ul style="list-style-type: none"> <li>• IoT applications are perceived to range across both consumer and industrial applications, with transport and logistics, energy and environment, home, and healthcare viewed as the most likely sectors to benefit from the IoT.</li> <li>• Increased environmental sustainability and improved efficiencies for organisations are seen to be the most significant benefits of the IoT.</li> <li>• Security vulnerabilities and privacy concerns are overwhelmingly perceived to be the most important barriers to the wider adoption of the IoT.</li> <li>• The IoT is perceived to exacerbate existing security challenges. The misuse of personal data and undermining of the integrity of business networks are seen to be the most likely security challenges associated with the IoT.</li> <li>• Privacy vulnerabilities pose a significant concern to users of IoT applications. More transparency among organisations collecting and using data, as well as increased user control and digital literacy, are perceived as key priorities to enable trust and confidence in data sharing and governance.</li> <li>• There is a perception that the public sector could play a stronger role in accelerating the uptake of the IoT in the UK, but that it should put citizens at the forefront of these efforts. The priorities for support are seen to be in ensuring interoperability, investing in people (e.g. through skills, training or education), and fostering multistakeholder collaborations (e.g. among businesses, universities and government), and less so in creating new business opportunities through public spending.</li> </ul>

Within each topic for discussion, we have articulated a series of corresponding key policy questions. These questions are wide ranging and horizontally apply across different sectors and industries. The required responses to these questions are unlikely to be achieved by public policy or industry alone; instead, it may require an active, multi-stakeholder approach. While the questions that follow from our findings are primarily aimed at the community of policymakers, the implications of these findings, which are deliberately formulated as questions, seek to provoke discussion across policy communities, including government

policymakers (national and local), innovators, industry, academia and the public. In Table 2, we present a summary of each of the proposed priority topics for consideration clustered by the policy objectives, along with the supporting policy questions.<sup>9</sup>

## Limitations of the analysis



There are a few caveats that should be kept in mind when interpreting the analyses presented in this report. First, it is important to note that this report is not an evaluation of the nature, impact or achievement of the nine case studies. Rather, we have used the information gathered from a rapid assessment of nine exemplar IoT-related projects in the UK to extract broader policy implications. Although the case studies we investigated cover a broad range of sectors and industries and include both consumer and industrial applications, they are not fully representative of the breadth and scope of IoT-related work in the UK. Therefore, any generalisation of the findings of our study should be undertaken with care. Second, the data we collected on the case studies using the background documentation and interviews were mostly based on self-reported information, and it was beyond the scope of this study to independently verify all the information. Third, a divergence of views on IoT developments in the UK was expressed across all the interviews. In our analysis, we have attempted, as best as possible, to articulate the majority opinions expressed across the sample of interviewees. Finally, we intentionally surveyed a random sample of the Institute's Professional and Chartered members, using this group as a proxy for informed users of technology. However, we note that a small percentage of respondents claimed that they had no personal or professional experience with the IoT.

---

9 In Appendix F, we present a summary of the findings from the analyses of the case studies and the survey and visually indicate how each of the findings link to the proposed priority topics for consideration.



**Table 2: The proposed priority topics for discussion and the associated key policy questions**

Policy objectives	Priority topics for consideration	Key policy questions
 <p><b>Supporting research and innovation in the IoT ecosystem</b></p>	<p>The need to focus on non-technical factors that drive adoption</p> <p>The need for knowledge from previous IoT projects to be shared, helping researchers and businesses avoid reinventing the wheel</p>	<ul style="list-style-type: none"> <li>• How can policy provide or incentivise more investment in non-technical factors for newly created IoT-related innovations?</li> <li>• How can sector-specific public investment initiatives work together to ensure that tested technologies are applied to new contexts and that system-wide effects are realised?</li> <li>• What steps can be taken by the policy community to create opportunities for effective collaborative networks involving citizens, industry, academia and government?</li> <li>• What can be done to infuse and sustain a culture of collaboration among the different stakeholders in the IoT ecosystem?</li> <li>• How can the policy community help to develop and sustain a workforce of sufficient critical mass and with the appropriate technical and commercial skills?</li> </ul> <ul style="list-style-type: none"> <li>• How can the public sector and industry systematically recognise IoT-related projects and capture the lessons learnt from implemented projects, starting with those that have been funded by government?</li> <li>• What are the ways to disseminate this evidence in a transparent and accessible manner to the various stakeholders in the emerging IoT marketplace?</li> <li>• How can the policy community systematically map the IoT ecosystem in 'real time' to anticipate and identify areas for public and private research and innovation investment more strategically?</li> <li>• What incentives can be created for industry to share the lessons of IoT implementations?</li> </ul>
 <p><b>Stimulating demand for the IoT to be adopted more widely</b></p>	<p>The opportunities to use IoT technologies in the delivery of public services and to help spur greater market demand</p>	<ul style="list-style-type: none"> <li>• How can public authorities identify areas where IoT with system-level benefits might be applied rather than an established solution?</li> <li>• How can the policy community capture evidence of the effectiveness and impact of local authorities' procuring of new IoT technologies at the project and system levels?</li> <li>• What are the challenges faced by procurement authorities in purchasing IoT technologies with limited evidence of benefits, and how can these challenges be recognised in the process?</li> <li>• How can public authorities ensure that the procurement processes for IoT technologies balance recognition of innovative, new-to-market SME suppliers with well-established players?</li> <li>• Could the supplier selection criteria be revised to reflect the potential of using the IoT in the delivery of public services?</li> <li>• How can the project-specific and system-level benefits be adequately valued and measured in a business case used by public authorities?</li> <li>• How can the policy community support the use of IoT technologies for infrastructure projects?</li> </ul>

Policy objectives	Priority topics for consideration	Key policy questions
 <p><b>Strengthening infrastructure and framework conditions for the development and adoption of the IoT as a systemic innovation</b></p>	<p>Sustaining structural change and benefit through interoperability and information sharing across applications</p>	<ul style="list-style-type: none"> <li>• What can the policy community do to help to accelerate the development of interoperable standards in IoT nationally and internationally?</li> <li>• How can publicly funded smart city and large-scale demonstrator projects support the drive towards common standards?</li> <li>• How can public procurement processes support the use of open IoT-enabling standards and interfaces in order to gain critical mass?</li> </ul>
	<p>Supporting the use of integrated IoT infrastructure across sectoral boundaries to help scalability of individual technologies</p>	<ul style="list-style-type: none"> <li>• Is there a need to raise awareness among public authorities as to the wider, system-level benefits that could potentially be accrued by leveraging IoT technologies as systemic innovations in public infrastructure projects?</li> <li>• How can the policy community support integrated, interoperable IoT infrastructure solutions rather than the continued deployment of individual technologies?</li> <li>• How can public authorities frame their requirements to encourage IoT standards-compliant devices and services?</li> <li>• How can the policy community support standards compliance as a prerequisite for procurement against public sector funding?</li> </ul>
 <p><b>Mitigating the risks of a pervasive IoT</b></p>	<p>Supporting a trusted, people-centric IoT ecosystem</p>	<ul style="list-style-type: none"> <li>• How can the policy community help industry balance economic objectives with creating an IoT ecosystem that is more open, trustworthy and inclusive?</li> <li>• How can the recognised processes for certifying devices be adapted to deal with the specific trust challenges posed by the IoT, including consent and information governance?</li> <li>• How can the policy community encourage industry to be open about information governance processes and the reporting of incidents?</li> <li>• How can the policy community incentivise industry to adopt people-centric design and development?</li> <li>• How can the policy community catalyse better ‘social contracts’ between individuals and organisations (including government) as the boundaries between the private and public spheres of personal data are progressively blurred?</li> <li>• What steps can be taken to raise cyber awareness and educate citizens about the potential benefits and risks associated with the IoT?</li> </ul>
	<p>Addressing concerns about the risks of IoT technologies to critical national infrastructure</p>	<ul style="list-style-type: none"> <li>• What can the policy community do to support the systematic assessment of risks associated with innovative IoT technologies and their deployment in public infrastructure?</li> <li>• How can current contingency plans be enhanced to identify and manage security risks associated with a growing and pervasive IoT?</li> </ul>

## Concluding remarks

We have closely examined the public policy implications of real IoT implementations and user perspectives to provide input to a feedback loop for the whole IoT policy community. We hope that using this bottom-up approach to engage with and examine the role of two key groups of stakeholders in the IoT ecosystem – businesses and individual users of technology – has generated deeper insight for the policy feedback loop. We also propose that the method we deployed in this study can be used in the future to provide a continuous feedback mechanism on how the impact of IoT-related policy is progressing in the UK – for instance, by using the survey generated for this report again, comparatively, in the future.

The IoT is a rapidly evolving area that has implications for a wide range of industry sectors and stakeholders. Its development holds great promise to deliver socio-economic benefits, and there is a clear case for businesses and the public sector to harness the opportunities made possible by the features of IoT technology – sensing, connectivity, feedback and collaborative processes – both locally and at the system level. The UK government has already recognised the importance of the IoT to its own performance, to that of UK industry, and as a growth market for innovative UK technology companies, especially the small to medium-sized enterprises (SMEs). In creating IoTUK, it has committed significant investment to the IoT, making IoTUK a dedicated resource that can support the delivery of government policy and catalyse markets.

Moreover, the role of citizens cannot be overemphasised in debates about the future of the IoT. The explicit inclusion of the public as stakeholders in the IoT ecosystem is imperative if a reliable, open and trustworthy IoT landscape is to be established. In particular, citizens need to have a good understanding of the benefits and risks associated with the IoT. Crucial questions raised in this study relate to how the UK can most effectively enable the deployment of IoT products and services to foster business opportunities while creating public trust and confidence in the principles by which the IoT is governed.

Our analysis indicates that some of the key questions relate to the ways in which government, in particular, can encourage and shape the IoT marketplace, as well as to the timing and consequences of such initiatives. The IoT is, potentially, a pervasive innovation that is developing rapidly. While much is known about the IoT, it would be too soon to describe it as a mature and stable innovation, for all its significance. The moment is right, therefore, for the policy community to address underlying questions and concerns and to shape the development of the IoT in light of both business needs and informed public preferences. The first steps in this direction might involve addressing the questions raised concerning setting the right framework conditions that ensure long-term growth for the IoT, as well as recognising and understanding the nature of the IoT as a systemic innovation requiring funding, standards, evidence and trust.



# Acknowledgements

---

We have been able to carry out this study because of the support of a number of people. First, we are grateful to BCS, The Chartered Institute for IT, and IoTUK, who commissioned the project, and in particular to the following individuals, who provided invaluable support and feedback throughout: Karen Tuck (BCS, The Chartered Institute for IT), David Evans (BCS, The Chartered Institute for IT), Roger Marshall (BCS, The Chartered Institute for IT), Jon Jeffery (BCS, The Chartered Institute for IT), George Georgiou (BCS, The Chartered Institute for IT), David Dowe (IoTUK), Jessica Rushworth (DCMS on secondment to the Digital Catapult), and Derek McAuley (The University of Nottingham). We would like to thank the individuals and organisations who kindly agreed to be interviewed as part of this study and the many Professional and Chartered members of BCS, The Chartered Institute for IT, who gave up their time to complete the survey. We very much appreciate the helpful and timely comments of our quality assurance reviewers, Stuart Parris and Susanne Sondergaard. We would like to thank Molly Morgan Jones for her helpful insights and advice throughout the project. We are also grateful to Jessica Plumridge, who designed and laid out the report. Finally, we would like to thank Suzanne Needs for copy editing the text.



# Chapter 1: Introduction

## 1.1 Background

The promise of technology is as unchanging as it is alluring: to improve our lives and well-being in ways we have not yet imagined possible. The current iteration of that promise is upon us, in the form of the Internet of Things (IoT). Connecting the physical and virtual worlds is what underpins the ambition of the IoT. The IoT can be regarded as an extension of today's Internet, consisting of 'a pervasive and self-organising network of connected, identifiable and addressable physical objects<sup>10</sup>... [that use] embedded chips and microprocessors' (Schindler et al. 2013).<sup>11</sup> The value of the IoT can only be truly recognised if different applications and devices work together seamlessly across and within different sectors, creating system-wide effects and enabling new capabilities and processes. Various estimates foresee that the number of connected devices could grow to between 20 and 100 billion by 2020, with the forecasted global economic value added ranging between \$1.9 to \$14.4 trillion by 2020 (Government Office for Science 2014).

Realising the potential benefits to the economy, many countries, including the UK, now regard the IoT as a highly significant, strategic-level infrastructure for economic growth (Government Office for Science 2014). As a result, the IoT has been receiving considerable attention from industry, universities and government. In the UK, the Government Office of Science published a comprehensive review of the IoT in 2014, and it followed this by creating a national programme of coordinated activities to support the growth of the IoT, IoTUK.<sup>12</sup> Yet, despite its enormous economic possibilities, many important questions remain as to how to harness the system-wide benefits of the IoT. It is crucial to understand the factors that can enable researcher and developer communities to bring new IoT applications to market and to understand the system-level implications of those products and services when they become adopted more widely. Furthermore, with consumers' growing awareness of the connected devices and sensors that enable the IoT, mainly through domestic equipment (e.g. smart TVs, Internet-accessible home security and control systems for heating and lighting), it is important to take into account their attitudes and concerns to understand how it affects the adoption of the IoT more widely. Moreover, there are also questions for individual users of technology concerning, for example, the privacy and security of their data, and implications for the security of infrastructure and the resilience of systems. As the IoT penetrates ever further into everyday objects and its rate of adoption increases, there are pressing challenges for, and possible threats to, businesses, governments, cities and communities that will need to be addressed.

---

10 In this report, we use the words 'objects', 'devices' and 'things' interchangeably.

11 While the concept of IoT is based on many enabling technologies that form the backbone of this new paradigm, individual IoT applications share three defining characteristics: capturing data from the object, aggregating that information across a data network, and acting on that information (Manyika et al. 2013).

12 In Appendix E, we provide a rapid overview of IoT-related policy actions undertaken by the UK Government from 2011 to 2016.

This report presents the findings of a study that examined the public policy implications of the development of the IoT in the UK with the aim of understanding how to accelerate the adoption of IoT applications by consumers and its diffusion across the economy.

### 1.1.1 Rapid review of the IoT landscape

Digitally-enabled systems meet physical objects in this new technological paradigm. Individual IoT systems – for instance in the home or in isolated pockets of public sector operations, such as lighting or waste disposal – are generating new opportunities for users, businesses and the public sector. The discussions around IoT often revolve around its consumer applications, such as health-tracking wearables, smart home devices and thermostats. However, the IoT has seen its application in industrial contexts grow, where, for example, the use of smart grids for electricity, water and transportation networks improves infrastructure management. It can also present new opportunities to improve the efficiency and performance of public services, for instance, by constructing ‘smarter’ cities and enabling objects to become smart and Internet-enabled, thus potentially reducing costs – for example, those relating to traffic incidents, improving road traffic management, or rolling out healthcare applications (BSI 2014). Indeed, according to one estimate (Cisco Systems 2014), 25 per cent of the global market value could be realised by the public sector.

As IoT applications are adopted more widely, the benefits of the IoT have been unfolding in recent years in terms of the IoT’s capability to improve existing business processes; achieve greater productivity in current operations; or lead to new business models with new types of products, services and strategies (Manyika et al. 2015). Increased smartphone penetration, connectivity and software-driven services are giving rise to new business models in the digital economy (OECD 2015a). It is anticipated that, as the adoption of the IoT widens, businesses will shift from products to ‘outcome-based’ services and thereby not only generate new opportunities for people to upgrade their skills, but also create new types of jobs (World Economic Forum 2015).

Although such major sectors as healthcare, agriculture, retail, energy, transport and built environments (home, office and city) all stand to gain from the benefits of connected objects, large opportunities exist in combining data across different industry sectors and thus breaking down the silos of data capture and processing. The full economic potential of the IoT can be realised as individual objects connected to cyber–physical networks are linked to wider networks across the board. The collection of data and data analytics drive the behaviour of actuators and the purpose of sensor networks, thus opening new opportunities for development of technologies and their use. As noted by the OECD (2015a), the data collected from these sensor networks thus becomes an ‘infrastructural resource’. Thus, the economic value of using data from the IoT amplifies when the data can be reused on a wider scale by other applications. The opportunities that occur when an increase in usage leads to a direct increase in value for other users or an increase in value of complementary products and services are commonly referred to as ‘network effects’ (Parker and Van Alstyne 2005). These effects will be achieved when more devices are connected and when there are appropriate conditions that can facilitate the connectivity and scalability required (Van Alstyne 2014). The network effects of the IoT are key to achieving the desired, system-level benefits from the connected devices. From a policy perspective, the scalability of individual IoT-enabled technologies within the market and the use and flow of its data within and beyond industrial sectors become key policy issues.



### The IoT as a systemic innovation

Although IoT technologies frequently appear to be sophisticated product-level innovations, the impact of the IoT is really felt by an industry, community or organisation when overall IoT-enabled connectivity, communication and collaboration enables system-level change in processes, capabilities and costs. Even simple IoT products can therefore enable, and are dependent on, the systemic innovation nature of the IoT. Systemic innovation generally represents a concept that describes fundamental changes in social dimensions (e.g. values, attitudes, and regulations), technical dimensions (e.g. infrastructure, technology, tools, and processes) and, importantly, the relation between these dimensions (TNO 2014). In this way, achieving systemic innovation requires not only technological innovation but also complementary changes in organisations and institutions to implement them, as well acceptance by consumers/citizens. Improved governance mechanisms are needed to facilitate system innovations, especially because such innovations take time and sustained commitment from stakeholders (OECD 2015c). For example, the IoT not only requires different technical capabilities but also potential changes in consumer practices, infrastructure, skills, and culture.<sup>13</sup>

Despite those systemic opportunities, the expected rapid adoption and diffusion of IoT technologies have not yet taken place, and their benefits have not been fully maximised (Hwang et al. 2015). The existing literature has considered numerous technical, financial, security, privacy and regulatory challenges as key elements for adoption of IoT applications by users and its diffusion throughout the economy. However, these issues are different for businesses, consumers and policymakers. As the recent survey of global businesses by the World Economic Forum (2015) showed, almost two-thirds of businesses view lack of interoperability and security as the two biggest hurdles. Other barriers include the lack of clearly defined return on investment (ROI), inadequate business models able to achieve profitability, and incompatibility of technologies with legacy equipment. Adopting the IoT will require changes in business models and organisational processes. Bi et al. (2014) describe the key features of the future enterprises having adopted the IoT, such as decentralised decisionmaking, a flat and dynamic organisation able to deal with massive data, an increasingly heterogeneous environment and resources, and the ability to adapt to real-time changes and to reconfigure capabilities. Manyika et al. (2013) emphasise the challenges for companies, notably in terms of decisionmaking processes and skills upgrade.

The adoption of the IoT is likely to be triggered by the public perception and views of the benefits and risks, which are important factors for the adoption of emerging technologies (Hall and Martin 2005). Citizens might not be sufficiently informed to be able to weigh up the risks and benefits. As more devices are connected to the Internet, the risks individuals face online are extended to the collective risks borne by employers, the industry environment, public sector organisations and nations (Manyika et al. 2013). Some of these challenges relate to security and data privacy, especially as it relates to unintended data amalgamation,

13 Systemic innovations are generally complex to fund (requiring large investments up-front before benefits are evidenced), to implement (requiring coordination of standards, service levels and costs across organisation boundaries), and to measure in terms of benefits (e.g. benefits may only accrue when IoT systems are at large scale, pervasive and connected, making the measurement of individual investments complex or even impossible). Analogies are the rail network, motorway network and national telecommunications infrastructure, enabling completely new capabilities but requiring significant investment before generating large-scale benefits. Given those challenges, the literature on systemic innovation has shown that government policy has a crucial role to play and requires a 'horizontal' policy approach (OECD 2015c), addressing cross-sectoral issues that potentially inhibit the development and adoption of the IoT.

unconsented data collection and amalgamation and cyber-risk, as complex, organised attacks on systems are foreseeable (BCS 2013). It has been argued that the IoT should be thought of as the ‘Internet of Trust’, as trust will be fundamental to enhancing the user experience and addressing key legal challenges, such as user privacy (OECD 2015b).

The increasing mobile access to the Internet and the growth of the smartphone market are likely to create a large consumer demand for the IoT (Schindler et al. 2014). In addition, some advances allow for an improvement in the effectiveness of the IoT and a reduction in costs. Factors often mentioned as enabling a wider adoption of the IoT include the falling prices and improved performance of sensors, wider network availability and capacity, and improved capacity in data management and storage (Schindler et al. 2014; Government Office for Science 2014). This could drive a strong business case and foster the wide adoption and spread of the IoT – as well as a growth in business models based on the IoT – the more the technology matures and costs fall.

## 1.2 Research objectives

It is evident the IoT holds the potential for major economic opportunities across a wide variety of consumer and industrial sectors; however, there are important horizontal policy issues that affect the development and adoption of the IoT across these sectors. With a growing body of IoT projects and commercial activities in the UK, there is a need to use evidence from ‘real world’ IoT implementations to inform policy in this rapidly emerging area. Furthermore, the significance of involving consumers of technology in informing IoT policy and decisionmaking cannot be overestimated, particularly when key decisions are to be made which touch upon such issues as privacy, security and trust. Clearly, there are numerous challenges that will require integrated and consistent policy responses across government. The IoTUK initiative launched in 2015 is an important step in this direction (IoTUK 2016a).

### ***‘Convening and amplifying the UK’s IoT industry to help business and economic growth’***

Currently a three-year programme running until 2018 that involves a £32m investment from the UK government, IoTUK is an overarching national programme of activities that seeks to accelerate the UK’s proficiency within the IoT domain (IoTUK 2016a). Driven by the Digital Catapult and the Future Cities Catapult, IoTUK specifically aims to hasten the adoption of IoT technologies across the business and public sectors. At a broader level, the initiative is targeting the advancement of the UK as a global leader in IoT ‘to ensure that foreign companies and investors understand the investable work being done in the UK’ (IoTUK 2016c).

The central aim of this study, which was commissioned by IoTUK and BCS, The Chartered Institute for IT (hereafter referred to as the Institute<sup>14</sup>), is to support a process for policy feedback that will inform the development and adoption of the IoT in the UK. We adopted a bottom-up approach that allowed us to bring together input from businesses and individual users of technology, enabling us to get a better idea of what is happening ‘on the ground’ in the UK. Specifically, we (i) examined the policy implications of a selection of ‘real world’

14 The Institute’s involvement with the study aligns with its mission to ‘make IT good for society’.

IoT projects (hereafter called case studies) in the UK identified by IoTUK;<sup>15</sup> (ii) surveyed a sample of informed users of technology to gauge their awareness of and views on the key policy-relevant issues related to the advancement of the IoT in the UK; and (iii) examined our findings from the case studies and the survey to generate a set of topics with supporting questions for further exploration and discussion by the policy community in the UK.

### 1.3 Outline of report

The study design and methods used in the research are presented in Chapter 2. We also list some important limitations that should be taken into account when interpreting the analysis. The key findings from the analyses of the IoT case studies are discussed in detail in Chapter 3, and the results of the online survey are presented in Chapter 4. Chapter 5 provides a synthesis of the key insights from the analyses of the case studies and the survey and discusses our findings in relation to the UK's governmental policy towards IoT. Specifically, we examine our findings to propose a set of policy-relevant priority topics for further exploration and discussion, and within each of these topics, we articulate a series of corresponding key policy questions. We end by providing some concluding remarks in Chapter 6. The appendices present further information, such as the summary descriptions of the case studies (Appendix A), protocols used for the interviews (Appendix B) and the survey (Appendix D), and the list of case study interviewees (Appendix C). In Appendix E, we provide the results of a rapid review of IoT-related policy actions undertaken by the UK government over the past five years. In Appendix F, we show the links between the findings from the case studies and survey, and the proposed topics for policy discussion.

---

15 The case studies we examined in the project were selected by IoTUK on the basis of research commissioned by IoTUK that looked at various examples of IoT implementations across different sectors in the UK. See, for example, IoTUK (2016b) for a summary of some of these projects. Summary descriptions of the nine case studies we examined are provided in Appendix A.



# Chapter 2: Study design and methods

## 2.1 Study design and scope

To gain a rounded picture of the potential policy implications of IoT developments in the UK, we adopted a mixed-methods approach to designing the study. Broadly, we conducted the research in three distinct but overlapping phases, as illustrated in Figure 3. In Phase 1, we undertook an in-depth examination of the nine IoT case studies to extract potential policy implications of these implementations.<sup>16</sup> Studying specific IoT implementations in depth offers a way to understand what is happening at the frontline of IoT activity in the UK and to extrapolate the likely implications on public policy. This phase of the study involved a focussed review of background documentation associated with each case study, followed by key informant interviews with individuals closely connected to the case studies.<sup>17</sup> In Phase 2 of the study, we carried out an online survey of informed users of technology to gauge their awareness and perceptions of key policy-relevant issues related to IoT developments in the UK.<sup>18</sup> Finally, in Phase 3 of the project, we triangulated the evidence from Phases 1 and 2 against a rapid review of current and previous UK government policy actions related to the IoT. We synthesised our findings to produce a set of wide-ranging policy-relevant topics and supporting questions for further exploration and discussion, which were aimed at provoking discussion across policy communities (including national and local government policymakers, industry, innovators, academia and the public).<sup>19</sup> Each of the methods employed is discussed in more detail in the following sections.

## 2.2 Description of methods

### 2.2.1 Focused review of background documentation for each case study

As noted above and in Chapter 1, to carry out the first stage of research (Phase 1), we conducted a focused review of background documentation associated with the nine IoT-related implementations. Summary descriptions of the case studies are provided in Appendix A. The case studies were identified by IoTUK from a larger pool of extensive case studies on the basis of research previously commissioned by IoTUK that looked at a series of examples of ‘real life’ implementations of the IoT in the UK across different sectors and industries.<sup>20</sup>

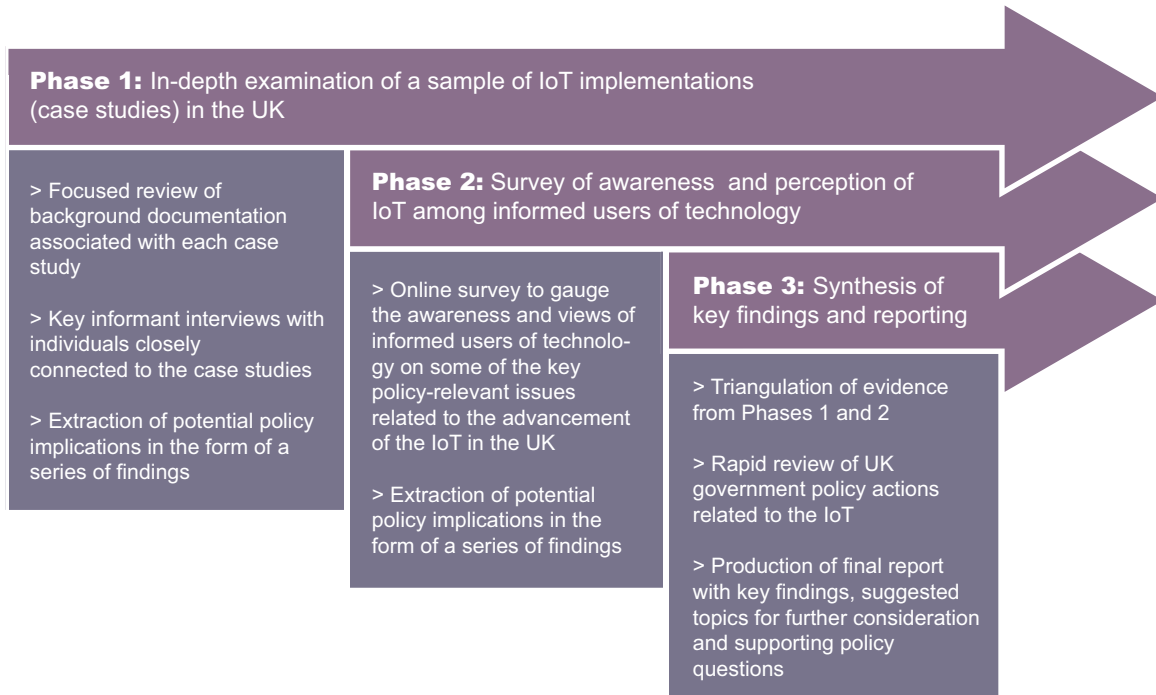
16 Summary descriptions of the nine case studies we examined are provided in Appendix A.

17 The results from the analyses of the case studies are discussed in Chapter 3.

18 The results from the analyses of the survey are discussed in Chapter 4.

19 The synthesis of the key findings and the topics for policy discussion and supporting questions are presented in Chapter 5.

20 For a summary description of some of these projects, see IoTUK (2016b).

**Figure 3: Study phases and associated methodologies used in the research**

The primary source of data underpinning this element of the research was an internal report prepared for IoTUK consisting of a series of case studies. Where possible, we also assimilated information in our analysis from other sources, such as project webpages.<sup>21</sup>

Some of the case studies we examined have more distinctly IoT-related characteristics than others (for example, in terms of breadth of connectivity and smartness); however, in general, all of them had the potential to be scaled up even further. The case studies span consumer and industrial applications across a wide range of sectors, such as healthcare, energy and environment, transport, retail, and agriculture, and all are examples of IoT-related projects that have been deployed in practice and that have measurable outputs (rather than, for example, being prototypes or demonstrators in a laboratory). In other words, they represent examples of applications that have moved from development to deployment, which allowed us to track their adoption pathways. Furthermore, the case studies have an underlying ‘public benefit’ mission attached to them. We were particularly interested in the implications of these case studies for policy, and we aimed to examine in detail the role of policy to support such projects, which could potentially stimulate the UK’s IoT landscape.

The data from the rapid review of the case studies were analysed to extract several high-level policy themes as well as potential policy-related subtopics to investigate during the interview stage of the research that immediately followed. Broadly, for each case study, the policy themes and subtopics covered the following main elements: (i) project characteristics (e.g. standards, governance, security protection); (ii) market value proposition (e.g. demand-side articulation of need, business model, financing, sustainability); (iii) framework conditions (e.g.

21 See, for example, Breathe Heathrow (2016), Bristol is Open (2016), and Silent Herdsman (2016).

regulation and liability, skills, education); and (iv) current and potential societal implications (e.g. inclusiveness, ethical issues, trust, privacy, security). This information was aggregated in a policy theme matrix. The high-level policy themes were informed to a degree by previous IoT policy research studies<sup>22</sup> but were enriched using specific information from the case study background documentation. This bottom-up approach of capturing policy themes, and in particular subthemes (e.g. supply and demand factors, public/private financing, business model, government support), to investigate further in the interviews was by default 'grounded' in reality, reflecting the experiences of a sample of IoT projects that have been deployed in practice in the UK.

### **2.2.2 Key informant interviews associated with each case study**

As noted above and in Appendix A, the case studies investigated in this study are diverse and cut across a range of sectors (e.g. health, transport, agriculture, retail, energy and environment). In a sense, they are all point solutions<sup>23</sup> and exemplars of smart sensing solutions<sup>24</sup> that have the potential to be scaled up. We used the policy theme matrix from the rapid review of the background documentation (described in the previous section) as a guide to structure and develop an interview protocol (the interview protocol is included in Appendix B). The interview protocol included information about the aims of the project, a list of the questions that would be used to guide the conversation, and a note on confidentiality. The interviews, all of which were conducted by telephone, were semi-structured<sup>25</sup> and lasted between 30 minutes and one hour. The interview protocol was sent to the interviewees a few days in advance. In addition to posing the standard set of questions that was common across all interviews, we framed several project-specific questions.

Across the nine case studies, we conducted a total of 13 interviews with individuals closely associated with the projects. The complete list of interviewees is presented in Appendix C; it includes, for example, founders, CEOs, business managers, technical directors, technology providers, and city council representatives.

We were particularly interested in the implications for public policy, and we therefore aimed to examine in detail the role of policy in supporting such projects, a role which could potentially stimulate the UK's IoT landscape. More specifically, we used the interviews to construct 'user stories', in order to better understand the case studies and to extract the potential implications of these projects for governmental policies directly or indirectly targeting the IoT, including (but not limited to) industrial policy, digital security policy and technology policy. Our interview questions broadly revolved around three main themes. The first set of questions looked at what the project had achieved to date and the key factors that enabled those achievements. We also explored the barriers to date (e.g. national or local government policy) that potentially hindered its progress. The second set of questions focused on the future ambitions of the project and related aspects (e.g. financing models and business sustainability). The final set

22 E.g. Schindler et al. (2013) and Government Office for Science (2014).

23 As currently funded and implemented, they have a relatively narrow implementation scope and scale.

24 With varying levels of context awareness built into them.

25 By carrying out the interviews using a semi-structured format, we were keen to elicit comparable responses across the interviewees to common questions in the protocol while also encouraging interviewees to provide additional contextual information which could help us extract potential policy implications.



of questions attempted to identify some of the key barriers that could potentially hinder those ambitions and what policymakers could do to address them (e.g. what specific policy steps could be taken to help with future ambitions, expansion, etc.). The results of the interview analyses are discussed in Chapter 3. To protect the anonymity of the interviewees, the analysis presented in the report does not make any specific references either to individuals or to the nine case studies.

### **2.2.3 Online survey of awareness and perception of the IoT among informed users of technology**

The second phase of the study was a focussed survey to gauge the awareness and perceptions of a section of the 'public' on some of the key policy-relevant issues related to the development of the IoT in the UK. The key informant interviews informed some of the areas for further exploration in the survey. The survey protocol is presented in Appendix D. We used an online survey to ask for the views and opinions of the Institute's Professional and Chartered members (BCS 2016), using this group as a proxy for 'informed' users of technology.<sup>26</sup> The survey was sent to a random sample of 9,998 Professional and Chartered members. The survey was opened on 21 December 2015 and remained open for one month. E-mail reminders were sent out on 7 January 2016. All survey responses were aggregated into a database for further analysis.

The sample of Professional and Chartered members was asked to respond as they saw IoT developments from their own perspective and experience, and the invitation e-mail highlighted that there were no 'right' or 'wrong' answers. The survey covered several topics, including: (i) general perceptions and understanding of the IoT; (ii) perceptions of the potential benefits of and barriers to the wider adoption of the IoT; (iii) perceptions of the security, privacy, resilience and data sharing aspects of the IoT; and (iv) views on the role of government in supporting IoT developments in the UK. The survey protocol was developed by the RAND Europe study team in discussion with IoTUK and the Institute and was administered by the Institute using the Snap Surveys platform. The results of the survey are presented in Chapter 4.

### **2.2.4 Rapid review of UK Government's policy actions related to the IoT**

In the final phase of the study, we linked the collated evidence from Phases 1 and 2 to the UK's governmental policy on IoT over the last five years. To do this, we 'mapped' the IoT policy landscape by carrying out a rapid review of current and previous governmental activity in the area of IoT (the results of this review are presented in Appendix E). The types of action included (for example) policy strategies, funding and other support mechanisms, consultations, guidance, standards information, and reviews. The review covered publicly released information and did not include the internal actions, or activities of working groups in the UK government. Pairing the evidence from our research with the review of existing policy initiatives and actions, we identified potential policy gaps that could be addressed in the future and articulated those in a set of topics for policy discussion. This is discussed further in Chapter 5.

---

26 We made the assumption that this group of users would have a reasonable level of understanding of technology based on their work experience and training.

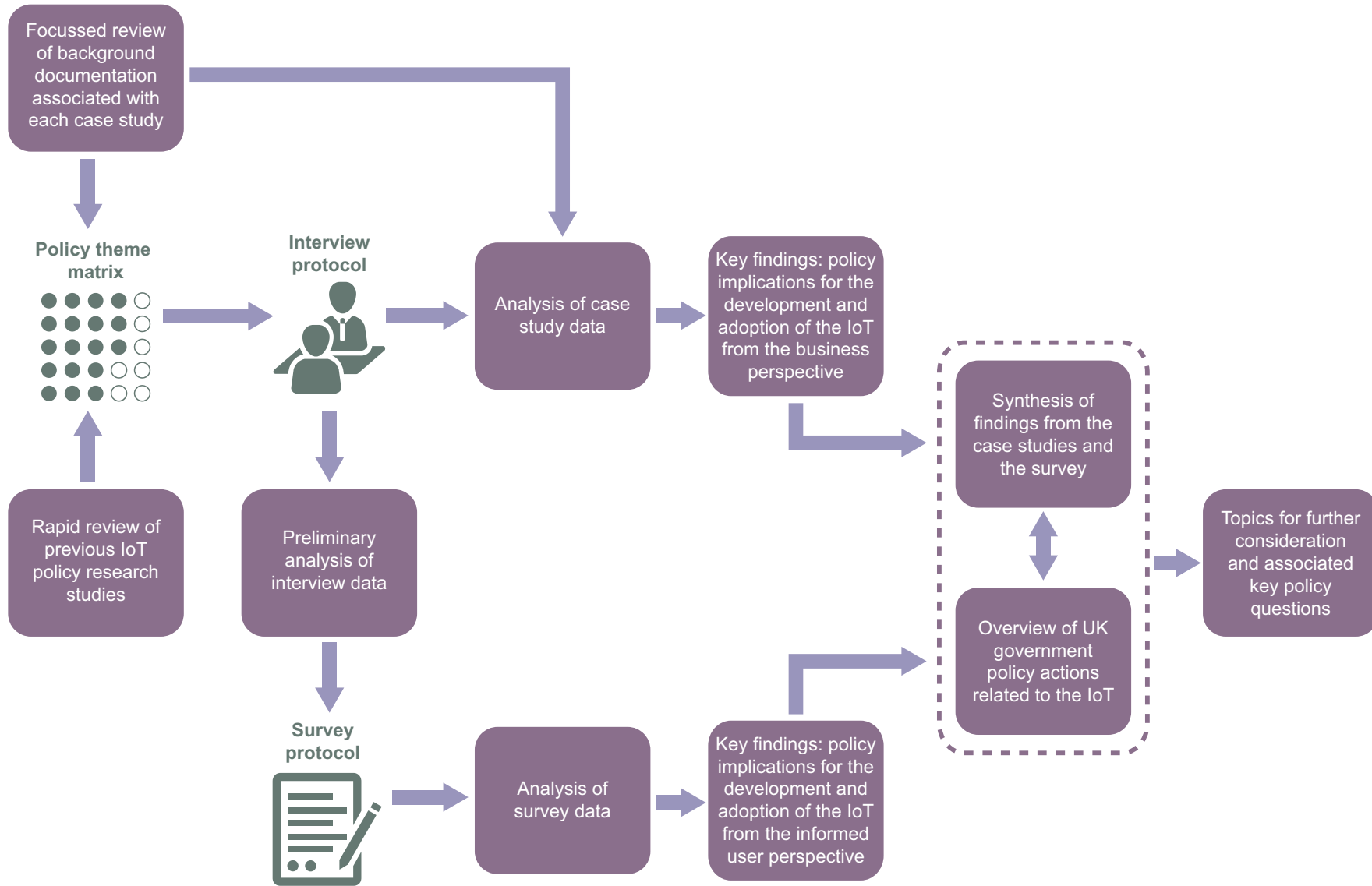


A diagram illustrating the various steps involved in the research and their interactions is shown in Figure 4.

## 2.3 Limitations of the analysis

There are a few caveats that should be kept in mind when interpreting the analyses presented in this report. First, it is important to note that this report is not an evaluation of the nature, impact or achievement of the nine case studies. Rather, we have used the information gathered from a rapid assessment of nine exemplar IoT-related projects in the UK to extract broader policy implications. Although the case studies we investigated cover a broad range of sectors and industries and include both consumer and industrial applications, they are not fully representative of the breadth and scope of IoT-related work in the UK. As a whole, these nine case studies were chosen to be illustrative rather than best-practice examples with the potential to be extensible to other applications. Therefore, any generalisation of the findings of our study should be undertaken with care. Indeed, our analysis suggests that the key insights and suggested topics for policy discussion that we have presented should be treated as exploratory; they warrant further, deeper examination. Second, the data we collected on the case studies using the background documentation and interviews were mostly based on self-reported information, and it was beyond the scope of this study to independently verify all the information. Third, the interviews were carried out using a semi-structured protocol, which resulted in some of the questions not being asked in all of the interviews. Fourth, a divergence of views on IoT developments in the UK was expressed across all the interviews. In our analysis, we have attempted, as best as possible, to articulate the majority opinions expressed across the sample of interviewees. Finally, we intentionally surveyed a random sample of the Institute's Professional and Chartered members, using this group as a proxy for informed users of technology. However, we note that a small percentage of respondents claimed that they had no personal or professional experience with the IoT.

Figure 4: Diagram showing the steps involved in the research



# Chapter 3: Results from the analysis of the case studies

## Summary of findings from the case studies of IoT implementations

1. Non-technical factors are critical to developing and adopting the IoT (e.g. collaborative networks, organisational capabilities and culture, and citizen engagement).
2. The challenges in developing the IoT market and accelerating its growth are immense, with market uptake and business model-related factors highlighted as the foremost issues.
3. Demonstrating sustainable business models with a solid return on investment is critical in order to progress the IoT market.
4. The public sector as a strategic purchaser could accelerate the uptake of IoT technologies, though in order to do so it will need to ensure that the small and medium enterprises (SMEs) leading IoT markets can participate and are assessed appropriately in procurement processes.
5. Creating both trust and confidence in the security of data and processes enabled by the IoT is not always aligned with businesses' objectives to innovate and deliver value.
6. Clear, unambiguous and standardised processes for personal data governance are considered to be prerequisites for linking up systems and for making them interoperable and trustworthy.
7. IoT innovators' perceptions are mixed over the ability and level of impact of public policy to drive and accelerate the IoT market.

## 3.1 Introduction

In this chapter, we present the results of the analysis of the case studies that was carried out in Phase 1 of the study (Figure 3). As noted in Chapters 1 and 2, the case studies we have investigated represent varied examples of IoT implementations in the UK spanning, different sectors and covering both consumer and industrial applications. Nevertheless, they share a number of features. All the case studies can be viewed as point solutions with relatively narrow implementation scope as currently funded and implemented. They also have varying degrees of connectivity and context-awareness built into them. Because of these factors, these examples can be viewed as '*Intranet of Things*' implementations. Another commonality is that the case studies have been partly or fully funded by the government (central and/or local), albeit through different funding mechanisms. Perhaps the most important factor for selecting and examining the projects was that they have moved beyond the development or prototype stage to implementation and have been adopted by the market, although only at an early stage of adoption compared with the full potential of the IoT.

Analysing these case studies gives us a sense of what is happening at the frontier of the IoT sector in the UK and enables us, accordingly, to (i) examine qualitative factors that have

contributed to adopting IoT applications to the market; (ii) understand the role of public policy in shaping the development pathways of the projects; and (iii) identify a number of present and potential policy implications associated with the development and adoption of the projects. Thus, the analysis of the case studies addressed questions such as: What is happening ‘on the ground’ with respect to firms operating in the IoT space? What are the key factors that helped IoT products and services to be developed and adopted by the market? What are the barriers to their development and deployment? What could be done to stimulate further development of the IoT in the UK? What is holding back the development of the IoT in the UK? And can a seemingly fragmented IoT landscape in the UK evolve into a scalable and extensible IoT ecosystem?

This chapter outlines findings from the synthesis of the in-depth interviews and background documentation associated with the case studies (carried out in Phase 1 of the study, as shown in Figure 3). The implications of those insights for policy, as well as the potential opportunities and challenges, are discussed in Chapter 5.

## 3.2 Findings from the analysis of the case studies

On the basis of the analyses of the interview data and the background documentation associated with the case studies, we present a series of findings that warrant further investigation.



### **Finding 1: Non-technical factors are critical to developing and adopting the IoT.**

In examining the case studies, we aimed to understand common characteristics that helped the case studies reach the implementation stage. This is crucial to extrapolating the factors and practices that could be used to inform appropriate policy support mechanisms for both the development and the adoption of the IoT. It has been characteristic of all the case studies that they have reached the deployment stage where their products or services have been implemented in practice and where the evidence of their impact could be generated. All the case studies explicitly aimed to build on their user cases by deploying their products or services on a wider scale, either by growing their market segment or, in the case of public infrastructure projects, reaching wider populations. Interviewees identified a number of enabling factors as important to developing and adopting the IoT case studies (Table 3).

**Table 3: Examples of enabling factors identified by interviewees for developing and adopting IoT applications in the UK**

Examples of enabling factors identified by interviewees	
Financing and business model	<ul style="list-style-type: none"> <li>• Early-stage R&amp;D funding to support the development of new technologies</li> <li>• Late-stage funding to support commercialisation of new technologies by demonstrating a strong business case and return on investment to funders and potential buyers</li> <li>• Creating robust business cases informed by the needs of end users that highlight benefits for both IoT product innovation and system-level innovation (made possible by the connection and processes enabled by IoT products)</li> <li>• Financing public IoT infrastructure projects through joint procurement processes to share the risk and achieve the necessary scale for system-level efficiency and process change</li> </ul>
Networks	<ul style="list-style-type: none"> <li>• Collaboration between research-intensive universities and businesses that recognises the impact of the IoT at the product and system levels</li> <li>• Access to international networks and foreign markets</li> </ul>
Technology, standards and interoperability	<ul style="list-style-type: none"> <li>• Embedded sensors and control systems</li> <li>• Cloud computing</li> <li>• Machine-to-machine (M2M) communications technology</li> <li>• Standards that facilitate interoperability and security, particularly open standards (open application program interface [API])</li> <li>• Agile technology development, informed by the user needs</li> </ul>
Organisational capabilities and culture	<ul style="list-style-type: none"> <li>• Strong leadership and consistent, clearly communicated vision</li> <li>• Progressive culture within public authorities, with political ‘buy-in’ for innovative technologies and the system-level changes they support</li> <li>• Multi-disciplinary teams, with both technological and commercial experience</li> </ul>
Government support	<ul style="list-style-type: none"> <li>• Funding support to aid commercialisation of innovative technological products and services</li> <li>• Government procurement opportunities to help innovators of IoT technologies develop evidence-based business cases for their product or service</li> </ul>
Citizen involvement	<ul style="list-style-type: none"> <li>• Engagement of citizens in the planning and design of IoT products and services</li> </ul>

Source: RAND Europe interviews

One of the most notable points was the availability of appropriate financing mechanisms and business cases to develop the IoT product and subsequently commercialise it. For some projects, early-stage government funding, particularly from such sources as Innovate UK, provided them with the means to bring new technologies closer to the market. As reported by one interviewee, this funding also provided an added value beyond the funding gains. And it also signalled the credibility of ‘unproved’ technology to potential customers.



*It was the combination of funding and credibility of being an Innovate UK-funded project, partly funded by the government. It was the name that mattered, too.*

It was also observed that government procurement opportunities played an important role in bringing the technology to the market. In response to the need to reduce the increasing costs and manage an ever-increasing demand on public services or infrastructure, public authorities procuring new technologies is seen as one way of managing increasing demand on public services or infrastructure. Interviewees noted that, in general, the public authorities with whom they had been working had strong leadership and management, with progressive vision and the *'political buy-in'* that set out the right conditions for procuring and testing new technologies to support the delivery of public services. In examining larger public infrastructure projects, we observed that some projects used a joint-procurement process<sup>27</sup> in order to manage risks and deploy the IoT product or service at a wider, integrated, system-level scale than an individual locality.

Aside from factors related to financing, interviews identified that access to networks was key to the implementation of the projects and their subsequent market roll-out. In particular, for a number of case studies, proximity to research-intensive universities was an important source of subject-specific technical expertise and international networks. Multidisciplinary teams with a combination of strong technological as well as commercial experience were expressed as an important factor that helped them move from development to deployment.

The studied projects were underpinned by available technologies, including embedded sensors and control systems, cloud computing and machine-to-machine communications technologies.<sup>28</sup> Yet, it was reiterated by a number of interviewees that technological development was directly informed by user needs. In this regard, several interviewees emphasised the value of involving citizens in designing 'user-driven' IoT solutions, which would enable products and services to be more 'easily' adopted by the market.



*Our product started with a problem and then we looked at how technology can address this problem.*

Some interviewees noted that having an agile approach<sup>29</sup> to technological development was a vital ingredient for creating prototypes that could be piloted with a sample of users and to building customer-centric products and services that could be swiftly and effectively adopted by the market.



*Development of the IoT should involve people who are actually affected by the technology.*

- 
- 27 Joint procurement represents an effort by multiple public authorities to collectively procure certain goods or services and manage the assets. In practical terms, it requires the synchronisation of multiple procurement processes, objectives and visions.
- 28 The concepts of IoT and M2M technologies are often conflated. M2M communications refers to technology that allows for the automatic exchange of data or information from one device to another through wired and wireless communications links. M2M communications could be considered to be an integral part of the IoT and in this context refers to enabling the transfer of data from sensors and devices in a network.
- 29 Agile or lean technological development is characterised by tightly integrated processes of user–producer interaction in rapid product development and highly flexible production.



**Finding 2: The challenges in developing the IoT market and accelerating its growth are immense, with market uptake and business model-related factors highlighted as the foremost issues.**

In developing and implementing products, the case studies have faced a wide range of challenges, some of which were sector- or context-specific, while others could be seen to exist more widely across the IoT industry. Table 4 presents the most significant barriers identified by interviewees to developing new IoT products and services and their subsequent adoption by the market. Some of the barriers were also mentioned in relation to their current ambitions to scale up their products or services and achieve more sustainable business growth.

**Table 4: Examples of barriers identified by interviewees to developing and adopting IoT applications in the UK**

Examples of barriers identified by interviewees	
Market uptake and business models	<ul style="list-style-type: none"> <li>• Lack of proven business models and user cases to demonstrate the return on investment value for customers</li> <li>• Projects not self-characterised as 'IoT-related', leading to diffuse and unconnected learning, evidence and business case development</li> <li>• Difficulties in articulating, developing and proving an appropriate business case for investment in new IoT applications</li> <li>• Inadequate confidence of potential buyers to purchase new IoT applications</li> </ul>
Integration	<ul style="list-style-type: none"> <li>• Incompatibility of new systems to integrate with legacy systems, hindering the possibilities for achieving scale</li> </ul>
Privacy and security	<ul style="list-style-type: none"> <li>• Consumer concerns about privacy and security and demands for accountability and governance</li> </ul>
Skills	<ul style="list-style-type: none"> <li>• Lack of commercial skills to help new products to market</li> </ul>
Regulation	<ul style="list-style-type: none"> <li>• Outdated or non-existent regulatory framework for large-scale IoT-powered infrastructure</li> </ul>

Source: RAND Europe interviews

The vision of the IoT is that a greater value can be generated when devices and objectives are connected in order to enable new capabilities and processes that allow more efficient use of resources, for instance. From the case studies, it emerged that one of the most overwhelming barriers to wider adoption of the IoT by the market was the difficulty in generating an adequate demand for their point applications, despite the availability of innovative technologies. Interviewees suggested that there remains a caution for 'buyers' to purchase technologies with unproven and/or high-risk return on investment. This caution amplified when large-scale of uptake is required, either pervasively or in a single organisation. It therefore seems that the lack of market readiness and confidence to invest in and purchase new IoT applications represents the biggest barrier to commercialising their products and services.



*At the very technical level, we could scale and deploy sensors very quickly. We have the capabilities to do that. But the scalability comes from their [customers'] understanding and knowledge.*



It was evident that the supply-side availability of technologies was an enabling factor to developing an IoT ecosystem. From the case studies, it would appear that the barrier to diffusing new technologies is more a reflection of the demand-side failure in the IoT market.



*There are a lot of people now developing solutions and eager to implement them, but there is a caution on the side of the buyers.*

As the majority of interviewees reiterated, the lack of confidence in the demand side of the market stems from difficulties in developing a *'solid and sustainable business model'* and building a business case for investors and potential customers that could adequately demonstrate return on investment. Some interviewees pointed out that initially they had focused more on technological development, without fully understanding and testing the business model accompanying the technologies. In addition, a number of case studies did not self-characterise their projects as 'IoT-related', did not have access to information about similar IoT applications implemented in other contexts, and thus were not able to explore emerging business models in the IoT industry.

Related to the inability to find the appropriate business model was the concern of several technology developers that the difficulties in commercialising their technologies can be partially attributable to the lack of commercial skills and business expertise. A number of interviewees mentioned that investing in people with technical skills is inevitably necessary, but that their project did not adequately invest in the commercial skills their technologies required in order to be commercialised.

Another set of barriers relates to integrating new IoT products with existing and previous-generation equipment and infrastructure. To achieve the full potential of their connectedness, devices must be connected to the cloud, allowing for the flow and sharing of data across organisational boundaries and thus opening up new business opportunities (Borgia 2014). This inevitably includes the integration with many existing and legacy systems. In this regard, some interviewees noted that incompatibility was an issue and that it was often difficult to integrate their products with existing infrastructure. As many legacy systems, especially those used in industrial applications, tend to have long life spans, it became *'economically infeasible for [their] customers to invest into [their] products'*. As a result, they had to rethink the pathways to commercialisation.



*Competing systems are healthy; however, there is a need to make them a bit more compatible than they are at the moment.*

In a minority of the case studies, the issues related to privacy and security were identified as barriers to market adoption of their solutions. Interviewees were well aware that privacy breaches and security vulnerabilities can impede trust of prospective buyers of their products and that therefore the potential consequences are much broader than any current challenges. In addition, some interviewees emphasised that the inability to exchange knowledge and practice, and not being able to network with other similar initiatives, posed a challenge. As would be expected, some interviewees also reported a variety of implementation problems



of both a technical and a non-technical nature; however, these were largely context- and/or industry-specific.



**Finding 3: Demonstrating sustainable business models with a solid return on investment is critical in order to progress the IoT market.**

Many interviewees emphasised that developing new connected products and services is not as challenging as being able to commercialise those products and services in the market. As mentioned previously, it emerged that at the core of this problem are the difficulties in building and communicating a solid, sustainable financial case for ROI for potential customers of IoT products and services, with benefits and costs clear beyond the stage of 'project' funding. For businesses, this creates difficulties in attracting investors with more realistic expectations about return on investment and potential customers.



*One of the challenges for the global sector is a lack of really robust user cases with a solid return on investment which you can point to. To date, there has been too much focus, certainly in recent years, on proving technology in the pilots, while, actually, we know that technology works, but what we need to be doing is proving the model.*

In this regard, a specific set of challenges is faced by public sector organisations introducing new technologies, such as IoT, in the delivery of public services. One difficulty relates to getting the initial buy-in and justifying the public investment, yet the challenges are amplified by the uncertainty of ROI that IoT technologies present. In the majority of the case studies we investigated, public authorities had undertaken a cost–benefit assessment to demonstrate the potential ROI. It was evident that most public authorities procured those technologies in response to the need to reduce costs in the short term or manage ever-increasing demand on public services in the medium to long term.

Despite being implemented, the majority of case studies are searching for the right model to ensure the sustainability of their projects. The majority indicated that they were on track to deliver return on investment over the next few years but noted that the expectations of their investors would be met at later stages of the project than initially anticipated. For some interviewees, unrealistic expectations of investors fuel a sense of frustration and pressure. This suggests a misalignment between private investors expecting early, technologically based high returns from breakthrough products and system-level process change yielding significant system-wide benefits – but with associated time implications.

For most interviewees, policy intervention played an important role in overcoming these barriers. For some of the interviewees, this uncertainty was partly mitigated by late-stage government funding to support commercialisation of their products and services, which allowed them to build sustainable business cases. For others, the strategic use of procurement markets by the public sector enabled them to enter the market and build successful user cases for other buyers, which is illustrative of the public sector funding systemic innovations.



**Finding 4: The public sector as a strategic purchaser could accelerate the uptake of IoT technologies, though in order to do so it will need to ensure that the SMEs leading IoT markets are assessed appropriately in procurement processes.**

From the case studies in our sample, it was evident that the public sector often acts as an important purchaser of 'IoT-related' products and services. As a result of this, the government has the opportunity to encourage adoption of IoT technologies by commissioning new products and services. A number of case studies involved local authorities commissioning new technologies in response to budgetary pressures on local government to deliver 'more for less'. Commissioning of technologies can therefore be seen as a response to managing public services rather than an explicit need to increase demand for innovation. As a result of purchasing innovative and new technologies, policymakers can help individual innovations improve their capacity to be adopted more widely. Nevertheless, the technology providers were able to diffuse their existing products, for which there had been an apparent lack of demand in the market. The view that the government can lead by example was also captured by a number of interviewees.



*The government has a tremendous 'nudge power' through its procurement process and the money it spends. It would be a combination of leading by example, actually doing this internally within the government departments rather than trying to persuade the rest of the world to buy. They are trying to convince about exports of the UK capabilities, and yet we are not doing it ourselves at home.*

Although the procurement markets can represent an important force for diffusing new technologies to the market, there remain important barriers to commissioning new technologies for local government. At the core of those challenges is, as mentioned previously, the lack of capacity of public authorities to build a robust business case for a new technology-driven product or service which could clearly demonstrate a return on investment. In this process bidders often have to include a cost-benefit analysis as part of the tendering processes to demonstrate value for money and, importantly, potential improved efficiency and cost savings for local authorities. However, there are obvious difficulties for businesses with new technologies to demonstrate the return on investment when no robust use cases have been collected (Heher 2006). One case study demonstrated that a joint procurement process could allow councils to negotiate a lower price and spread the risk, especially when the investment concerns larger infrastructure projects.

We observed that, as a consequence of those procurement processes, many commissioned technological products or services were provided by well-established technology businesses that had (i) the resources to participate in the procurement processes, (ii) an adequate track record in delivering similar services, and (iii) the business capacity to respond to the sales requirements of public procurement. These factors, however, are particularly difficult for SMEs with innovative IoT products, for whom taking part in the procurement processes requires significant investment costs. As noted by one interviewee, lengthy business cycles set out by procurement processes and significant up-front investment with uncertainty means that they are disincentivised to provide services for public sector. As a result, young businesses with innovative products thus become overshadowed by larger players.



*Without spending a penny more than they already are, the government could leverage the UK capability by simply asking them how do you make use of the most cutting-edge technology and smart city thinking?*

While the procurement markets seem as an important force for commissioning new technologies, our interviewees suggested that such processes are not currently suitable for stimulating the development or prototyping of new technologies, but, rather, for creating opportunities for diffusion of existing and proven IoT products and services in the new contexts and/or sectors.

The evidence from large public infrastructure projects suggests there is an opportunity for public-private partnerships to purchase technologies that require higher investment. One case study showed that matching public funding with private sector funding provides the opportunity to de-risk the uncertainty of public investment and ensure longer-term sustainability of the project. The evidence suggests, however, that these partnerships require well-established and productive relationships between public and private actors.

Part of the reason why this made it difficult to procure technologies in the public sector is that it was also generally difficult to find people in the public sector with the vision and willingness to take on risks. It was also observed that demand was sometimes hampered by poor user perception of the added value of IoT solutions or by media reputation.



**Finding 5: Creating both trust and confidence in the security of data and processes enabled by the IoT is not always aligned with businesses' objectives to innovate and deliver value.**

As the number of devices connected to cyber-physical systems continues to rise, the scale of potential security risks from IoT is expected to significantly increase cybersecurity vulnerabilities and provide new opportunities for abuse (QinetiQ 2015). In the analysis of the case studies, we understood the issue of security to be under more competing tensions than may have seemed to be the case at the outset. We observed that views on the nature and severity of security challenges differ across the case studies and that these relatively 'soft' political requirements are not always aligned with the requirements of businesses.

The case study interviewees broadly agreed that ensuring security was a potential challenge within their own applications as well as the wider IoT sector. The security and protection of IoT-related applications and the data they generate is necessary to ensure the trust of potential buyers and the wider public in IoT environments. Addressing security concerns was viewed as key to fuelling more trust in purchasing IoT solutions and thus unlocking new business opportunities and protecting the users of IoT products and services.



*Security is an issue we agonise over.*

Other respondents felt that they were employing the ‘*best available security practices*’ and that the associated cyber-risks related to their individual solutions were ‘*negligible*’. The majority of them reiterated their reliance upon other vendors and firms, who, in their view, were practicing ‘*good*’ cybersecurity procedures. Some interviewees, who appreciated the risks associated with their IoT solution, nevertheless felt that current security concerns are mostly in reaction to events (e.g. cyber attacks) that are unavoidable and that good practice arises from capturing lessons post-incident and communicating them back to the security sector. In these cases, interviewees felt that an excessive focus on security considerations detracted from realising potential business opportunities and technological innovation. The impression was that while security was a concern, it was secondary to delivering business objectives.



*The question about getting any guidance on countering cyber-risks suggests that there is somebody to come and advise us – I wouldn’t be entirely sure who that is.*

We also examined the security risks related to public infrastructure IoT projects, where the potential vulnerabilities exacerbate as they impact on the safety or the provision of essential services to citizens and communities. Broadly speaking, the interviewees associated with these case studies did not view the scale of present or potential security risks as very significant. Some interviewees noted that they mitigated their security risks during the procurement phase and selected suppliers who had strong security credentials and whose solutions were ‘*secure by design*’. Others, however, mentioned that systems are susceptible to physical destruction or sabotage given the challenge of engineering small, secure, Internet-connected devices. The same interviewees noted the susceptibility of IoT solutions to the jamming of radio signals.

Finally, the majority of interviewees generally thought of their application as being ‘disconnected’ from the wider network. They had not considered how the security implications would become much more critical once their applications scaled up, that is, when their local technology solutions became connected to the wider network of objects that is the future scope of the IoT.



**Finding 6: Clear, unambiguous and standardised processes for personal data governance are considered to be prerequisites for linking up systems and for making them interoperable and trustworthy.**

It was evident across the majority of case studies that data governance was vital for successful IoT implementations, in particular for linking up different systems and making them interoperable. However, there is a need to understand how citizens – both as producers of data underpinning the IoT and as end users of IoT applications – respond to new IoT applications, as their concerns could limit their uptake of IoT applications.



*The world is moving in the way we treat people’s data as private or not private.*

When asked about the privacy implications of their connected consumer and industrial products, several interviewees recognised the necessity to make a trade-off between the benefits potentially arising from tailored, personalised services and the risks associated with collecting and sharing personal data. Despite the benefits that businesses saw from collecting and sharing personal data, it became clear in a number of interviews that they lacked some consideration for how citizens would respond to the use of their personal data by connected products and services. As shown by a recent survey, a high proportion of consumers believe that the benefits of sharing personal data are solely for an organisation's economic gain (Digital Catapult 2015).<sup>30</sup>



*Brands will have to be honest and open with people about what data they are collecting, and how and why.*

In some technology areas, developers used anonymised data to ensure as far as possible that a data holder's private data is not re-identified. Most solutions were 'opt in' by default, and users had to 'switch off' or 'opt out' if they did not want their personal information collected. In contrast, some interviewees noted a misperception that existed of IoT solutions as being '*privacy-intruding*', claiming that the IoT sector might have an '*image problem*' more generally. In the case of larger systemic IoT applications, technology providers noted that they did not encounter any privacy breaches, such as intrusive exposure of behavioural patterns or profiling, and rarely considered potential wider privacy implications when developing and implementing their solutions.



*People will willingly give up personal data if they understand why it's being collected and what the benefit to them is.*

Across the case studies we saw an ad hoc approach when it came to data governance and data protection. It emerged that businesses were creating their own data governance structures to suit their needs. Some businesses became '*owners*' of data, others saw themselves in some way as having '*licensed access*' to data, while others were mere '*conduits*' for data flows. It was noted by some that data governance was not a '*technical question*' but rather an '*ethical question*' about who should own users' personal data. In these cases, data ethics and privacy concerns were placed at the centre of the IoT solution, as the businesses were more concerned about the users and their rights to opt out of digital tracking and the deletion of personal data than about the commodification of personal data. Others indicated that data governance questions tend to be answered '*legally*' and are not necessarily informed by good practice. They felt motivated by compliance with common industry standards about the protection of personal data and its legal implications, rather than placing the individual at the centre of their decisionmaking process. In general, however, clearly defined data governance procedures were seen as the key to joining up systems, facilitating seamless interoperability, and, consequently, enabling successful IoT implementations.

30 In the same survey, over 60 per cent of consumers felt uncomfortable sharing personal data, with 14 per cent refusing to share any personal data at all (Digital Catapult 2015).



**Finding 7: IoT innovators' perceptions are mixed over the ability and level of impact of public policy to drive and accelerate the IoT market.**

When asked about the role that public policy could and should play in developing and adopting the IoT in the UK, there were generally mixed responses concerning the expected support from local or central government. In general, interviewees noted the need for government to provide better targeted funding instruments for stimulating the UK IoT market, particularly in relation to late-stage technological development and commercialisation.<sup>31</sup> Others saw the role of public policy in 'softer' ways, such as knowledge/practice exchange or raising market awareness. There were also views that the '*interference*' of government in private markets can stifle innovation rather than support it. One interviewee observed, for example, that by favouring certain businesses over others, the government sets inadequate framework conditions for developing and adopting the IoT in the UK.



*The whole thing is happening and emerging organically all around us.*

Public funding for the projects was generally acknowledged as an important component of government support to the IoT. When discussing the available funding mechanisms to support the IoT sector in the UK, reactions differed as to the effectiveness of support from Innovate UK. There was agreement among some recipients of Innovate UK grants that government support had been '*instrumental*' in commercialising their solution. But others were not convinced by the support offered to IoT demonstrators. Broadly speaking, it was also acknowledged that there should more funding and grant opportunities to support the commercialisation of early-stage IoT products and services, particularly funds that cover not only capital costs but also investment in human capital, commercial skills for IoT, and knowledge exchange.

There was also a wider agreement that central government should have a mandate for setting appropriate standards to help the flow of data across connected objects and devices, which is seen as a key enabler in building focus and critical mass in the emerging stages of creating sustainable and scalable IoT networks.<sup>32</sup> It was noted that while the British Standards Institution (BSI) has started '*good work*' around smart cities (BSI 2014), it is important not to tackle those issues within a narrow UK context, but to pursue a broader vision at the European Union and international levels.

Another significant opportunity for government was in relation to the ability of public bodies (particularly local authorities) to identify the opportunities for the applications of IoT-enabled technologies solutions and to build a better business case around them. One suggestion was

31 All the case studies we examined were either fully or partly government-funded. However, there is a mix of government mechanisms through which they were funded. Some case studies were provided funding by Innovate UK in order to commercialise those products. Others were fully or partly financed by local authorities. In other cases, funding was provided by individual central government departments, such as the Department of Transport or the Department of Health.

32 For example, in the particular context of the health sector, Denmark mandated in 2013 that all 'personal connected health' devices and services should comply with the Continua Health Alliance's guidelines for interoperability (ehealthnews 2013).



for government to make available a set of 'toolkits' for local councils to work out business benefits. One interviewee referred to an example in the USA, where an information pack was made available to local authorities to develop the business case for the development and procurement of local street lighting systems. Another opportunity related to the creation of appropriate conditions for SMEs to enter the government procurement markets so that they could compete against larger players in the procurement markets.

Other interviewees argued that central government could support industry with 'softer' interventions. This included suggestions to create centres of excellence outside London to demonstrate the full capability of the IoT, rather than invest in a larger number of smaller demonstrators. It was proposed that '*successful*' projects could disseminate the lessons learnt across the market, for example, through IoTUK. Others suggested that more guidance is needed for the investment community, to make sure it understands the potential return on investment for new technologies, such as IoT, and that it does not set unrealistic expectations that become a hindrance to small-company growth. It was also suggested by some interviewees that government could harness the growing UK capability in IoT by encouraging and facilitating new exporting opportunities through, for example, UK Trade & Investment (UKTI). It was noted that the opportunities by UKTI should be open to larger businesses as well as SMEs. In this regard, a number of interviewees highlighted significant interest in their products and services from foreign markets. One interviewee in particular noted that late-stage government funding from Innovate UK was an important element that allowed the company to gain traction in international markets. This suggests there are opportunities for the UK to export IoT-related technologies to international markets and to help establish the UK as a '*stronger player in the IoT sector globally*'.



*New exporting opportunities came directly out of this project, using the same concept and technology in Europe and the Middle East.*





# Chapter 4: Results from the analysis of the survey

## Summary of findings from the survey of informed users of technology

1. IoT applications are perceived to range across both consumer and industrial applications, with transport and logistics, energy and environment, home, and healthcare viewed as the most likely sectors to benefit from the IoT.
2. Increased environmental sustainability and improved efficiencies for organisations are seen to be the most significant benefits of the IoT.
3. Security vulnerabilities and privacy concerns are overwhelmingly perceived to be the most important barriers to the wider adoption of the IoT.
4. The IoT is perceived to exacerbate existing security challenges. The misuse of personal data and undermining of the integrity of business networks are seen to be the most likely security challenges associated with the IoT.
5. Privacy vulnerabilities pose a significant concern to users of IoT applications. More transparency among organisations collecting and using data, as well as increased user control and digital literacy, are perceived as key priorities to enable trust and confidence in data sharing and governance.
6. There is a perception that the public sector could play a stronger role in accelerating the uptake of the IoT in the UK, but that it should put citizens at the forefront of these efforts. The priorities for support are seen to be in ensuring interoperability, investing in people (e.g. through skills, training or education), and fostering multistakeholder collaborations (e.g. among businesses, universities and government), and less so in creating new business opportunities through public spending.

## 4.1 Introduction

This chapter presents the results of the analysis of the online survey that was carried out in Phase 2 of the study (Figure 3). To complement the insights we obtained from analysing ‘real life’ IoT implementations in the UK, in Phase 2 of the study we conducted a focussed opinion survey of informed users of technology.<sup>33</sup> The survey was circulated to a random sample of 9,998 Professional and Chartered members (BCS 2016) of the Institute to solicit their knowledge of and opinions about IoT developments in the UK. In total, 467 responses were collected, between 21 December 2015 and 21 January 2016. The survey was designed to collect data on the perceptions, awareness and understanding of the IoT from the perspective of informed users of technology. The full survey protocol can be found in Appendix D. The survey helped us gain a sense of what one sector of public opinion thinks about key issues,

33 When asked about their personal or professional experience with IoT, approximately 60 per cent of respondents self-characterised as ‘end users/consumers’, 34 per cent as ‘technology developers’, 21 per cent as ‘commercial/business support’, and 16 per cent as ‘researchers’. Only 15 per cent of respondents stated they had no previous experience with the IoT.

such as the applicability of the IoT to specific sectors, the benefits and risks of using IoT-related products and services, and the role of government in supporting the IoT as a strategic industry in the UK. This chapter describes the findings of the survey specifically, presenting some detailed descriptive statistics.

## 4.2 Findings from the survey

Below we present a series of findings for policy from the analysis of the survey data.

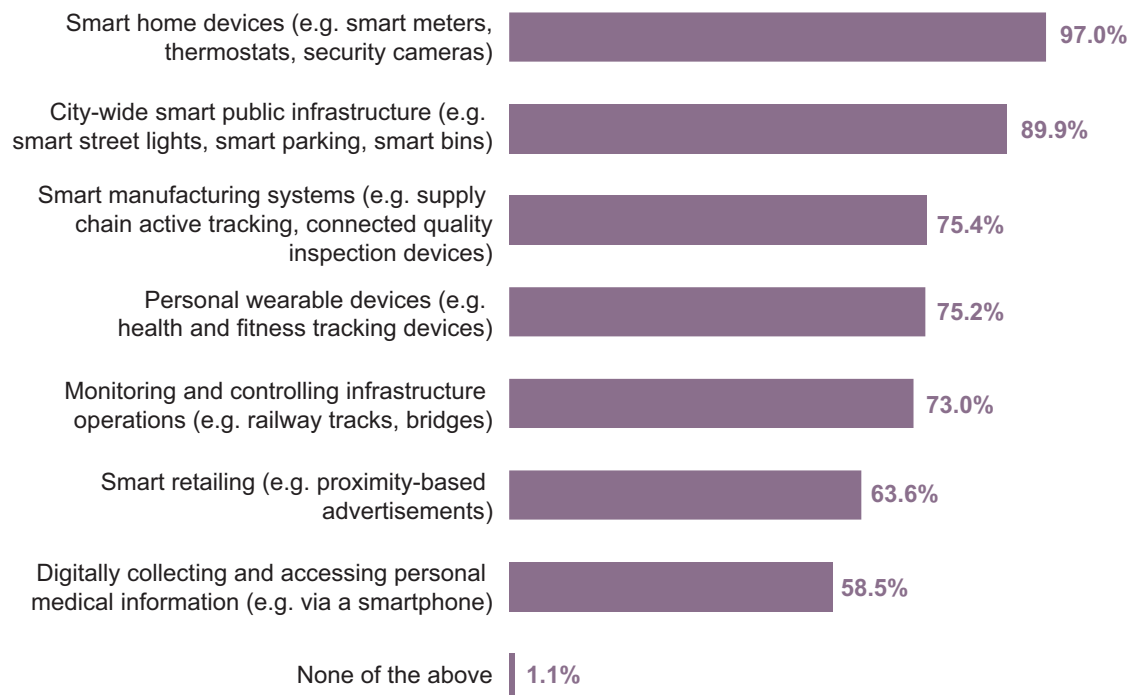


**Finding 1: IoT applications are perceived to range across both consumer and industrial applications, with transport and logistics, energy and environment, home, and healthcare viewed as the most likely sectors to benefit from the IoT.**

Respondents were presented with different examples of IoT applications across a range of sectors and industries and were asked to select the applications they most closely associate with the IoT. The results are shown in Figure 5. For all the examples presented, the majority of respondents agreed that they represented examples of IoT applications, though to varying degrees of agreement. Notably, almost all respondents (97 per cent) associated smart home applications, such as smart meters, thermostats and security cameras, with the IoT. Approximately 90 per cent related city-wide smart public infrastructure with the IoT, which includes such examples as smart street lighting and smart parking. About three quarters of respondents considered smart manufacturing systems (e.g. supply chain active tracking), personal wearable devices (e.g. health and fitness tracking devices) and infrastructure monitoring and controlling devices (e.g. for railway tracks and bridges) to be associated with IoT applications.

**Figure 5: Respondents' perceptions of what represent examples of IoT applications**

**Question: Which of the following do you agree represent examples of Internet of Things applications?**



Respondents were also asked to suggest what they considered from their own perspective to be the 'best' example of an IoT application. A word cloud that depicts the most frequently occurring words within the responses to this question is shown in Figure 6.<sup>34</sup> This only provides a visual complement, but it highlights the diversity of perceptions while also reiterating the distribution of responses highlighted in Figure 5 (i.e. the majority opinion viewed 'smart-X' applications as examples of the IoT).

Figure 6: Word cloud showing the most frequently occurring words in the survey responses to the question 'What do you consider to be the "best" example of an Internet of Things application?'

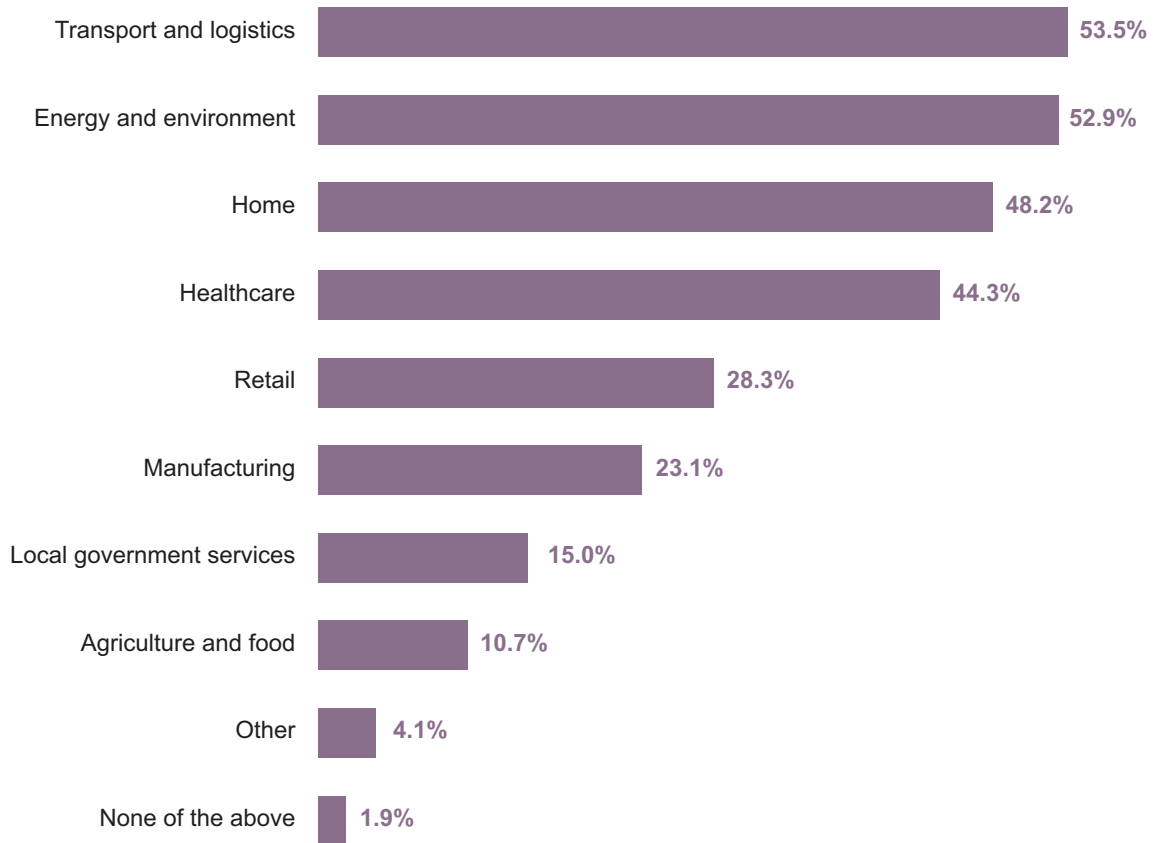


As illustrated in Figure 7, the majority of respondents viewed transport and logistics (54 per cent) and energy and environment (53 per cent) as the broad sectors that are most likely to benefit from the development of the IoT; 48 per cent and 44 per cent of respondents, respectively, identified home and healthcare as other key sectors. In contrast, only approximately one in ten respondents considered the agriculture and food sector to be most likely to benefit from the IoT.

34 The responses to the open survey question (What do you consider to be the 'best' example of an Internet of Things application?) were input to an online word cloud-generating software (Jason Davies 2016). The more times a word appears in the survey responses, the bigger the word is in the resulting word cloud.

**Figure 7: Respondents' perceptions of which sectors are most likely to benefit from the IoT**

**Question: Which three of the following sectors do you think are most likely to benefit from the Internet of Things?**

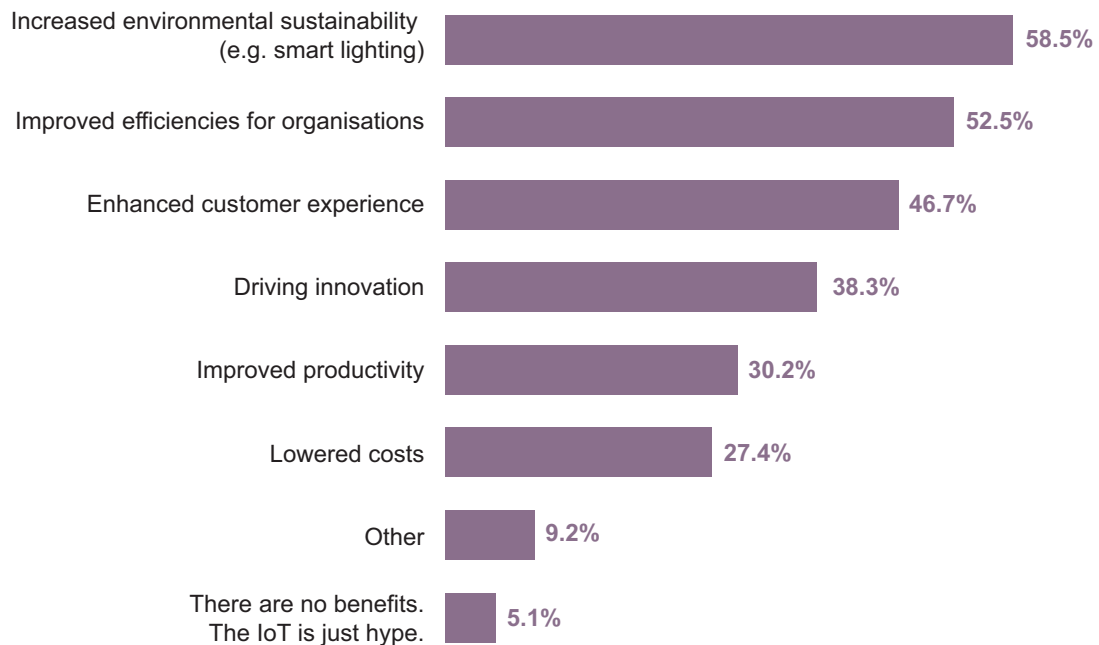


**Finding 2: Increased environmental sustainability and improved efficiencies for organisations are seen to be the most significant benefits of the IoT.**

Respondents were asked to identify what they considered to be the three most important benefits of the IoT. Several perceived benefits were identified across the sample of respondents. The results (Figure 8) show that increased environmental sustainability is perceived to be the most important benefit of the IoT (59 per cent of respondents), followed by improved efficiencies for organisations (53 per cent) and enhanced customer experience (47 per cent). Slightly more than one third of respondents (38 per cent) recognised that driving innovation was another key benefit of the IoT. Improving productivity and lowering costs were recognised as benefits by around one in three respondents. Finally, approximately 5 per cent of respondents responded that the IoT is just 'hype' and that there were no benefits associated with it.

**Figure 8: Respondents' perceptions of what are the most important benefits of the IoT**

**Question: What do you think are the three most important benefits of the Internet of Things?**

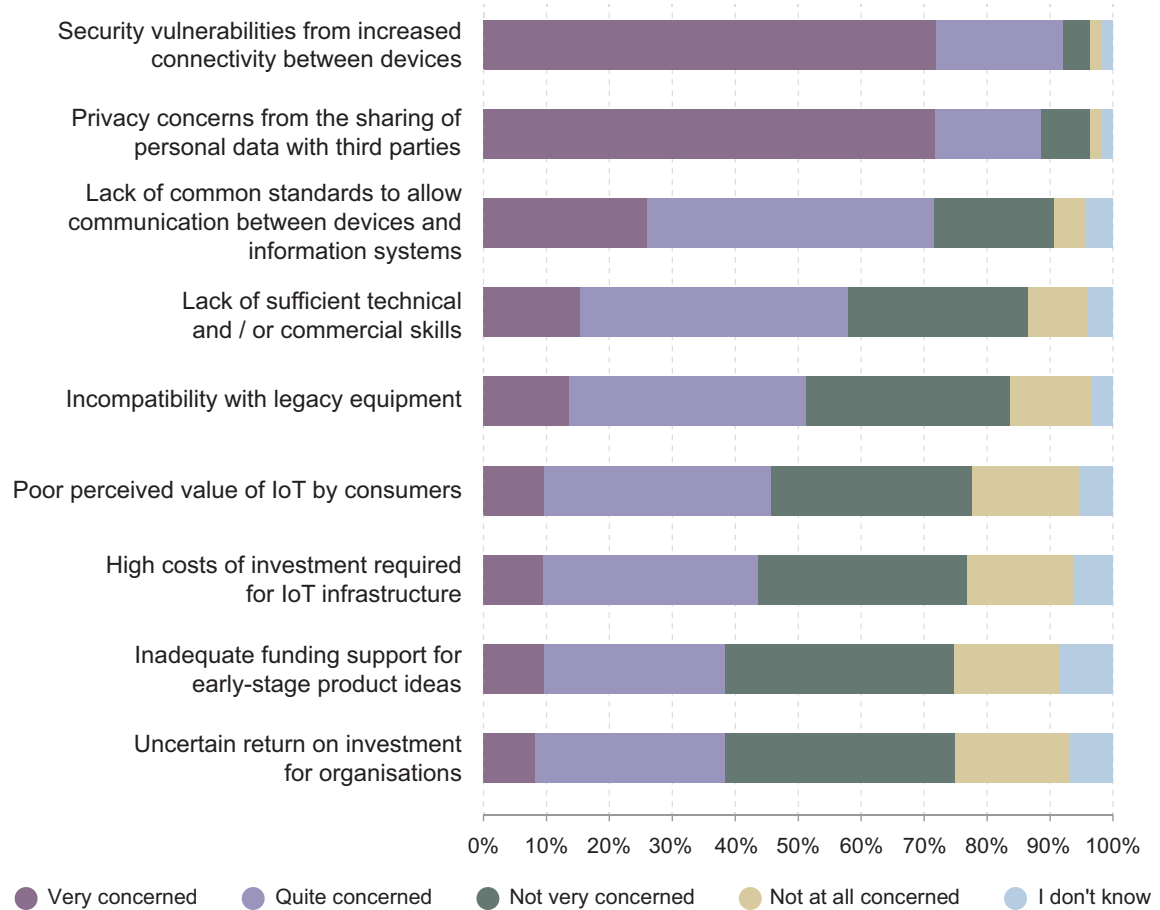


**Finding 3: Security vulnerabilities and privacy concerns are overwhelmingly perceived to be the most important barriers to the wider adoption of the IoT.**

Respondents were also asked to identify and characterise their level of concern about possible barriers to the wider adoption of the IoT in the UK. As shown in Figure 9, respondents highlighted security vulnerabilities and privacy concerns as the two most important barriers. Specifically, more than 92 per cent of respondents were quite concerned or very concerned about security vulnerabilities potentially arising from increased connectivity between devices. Similarly, almost 89 per cent of respondents were quite or very engaged with privacy concerns associated with the sharing of personal data with third parties. A large proportion of respondents (72 per cent) were also concerned about the lack of common standards to allow devices and information systems to communicate with each other in the IoT ecosystem. In addition, the lack of sufficient technical and commercial skills and incompatibility of IoT products with legacy systems were identified by the majority of respondents (58 per cent and 51 per cent, respectively) as potential barriers to the wider adoption of the IoT. In contrast, the majority of respondents were not concerned about possible barriers related to the uncertain return on investment for organisations investing in IoT (55 per cent), inadequate funding support for early-stage IoT product ideas (53 per cent), and the high costs of investment required for IoT infrastructure (50 per cent).

**Figure 9: Respondents’ perceptions of what are the most important barriers to wider adoption of the IoT**

**Question: From your own experience, how concerned are you about the following barriers to the wider adoption of the Internet of Things?**

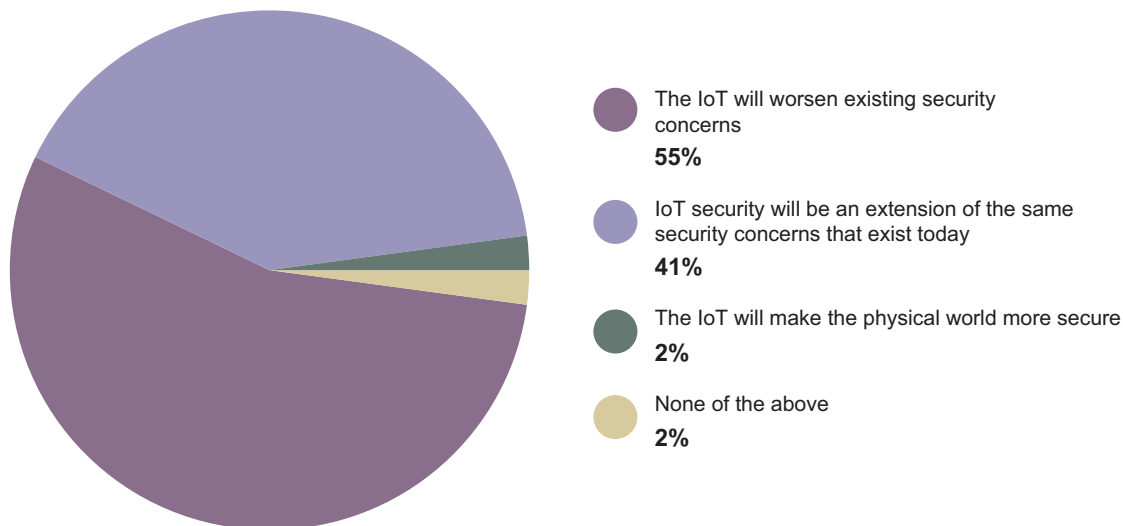


**Finding 4: The IoT is perceived to exacerbate existing security challenges. The misuse of personal data and undermining of the integrity of business networks are seen to be the most likely security challenges associated with the IoT.**

Respondents were asked about their opinions and views on the security, privacy and data sharing aspects of the IoT. Mirroring the views expressed around barriers to the wider adoption of the IoT, in the context of the potential security issues involved (Figure 10), there was an overwhelming agreement (96 per cent) that the IoT will exacerbate existing security challenges; however, there was variation in the level of perceived severity. A slight majority (55 per cent) felt that the IoT will worsen existing security concerns, while 41 per cent of respondents observed that the security challenges created by the IoT will be merely an extension of the same security concerns that exist today. Only 2 per cent of respondents thought that the IoT will make the physical world more secure.

**Figure 10: Respondents' perceptions of the security implications associated with the IoT**

Question: Which of the following statements regarding Internet of Things security do you agree with most?



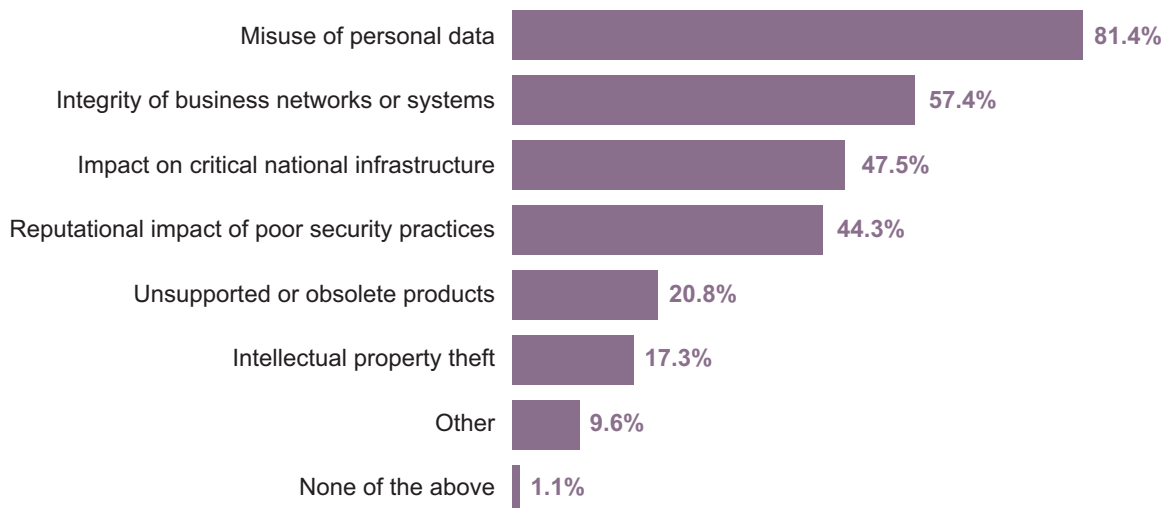
When asked about the nature of the security threats most likely to be associated with the IoT (Figure 11), the two most prominent factors that respondents recognised were the misuse of personal data (81 per cent of respondents) and the implications for the integrity of business networks and systems (57 per cent). The potential impact on critical national infrastructure (48 per cent) and reputational impact of poor security practices for organisations (44 per cent) were two other noteworthy security challenges identified by respondents.



*Every IoT device is potentially hackable. For medical appliances, this could be extremely dangerous. There are so many unknown consequences at this point.*

**Figure 11: Respondents' perceptions of which security threats are most likely to be associated with the IoT**

Question: What do you think are the three most likely security threats associated with the Internet of Things?





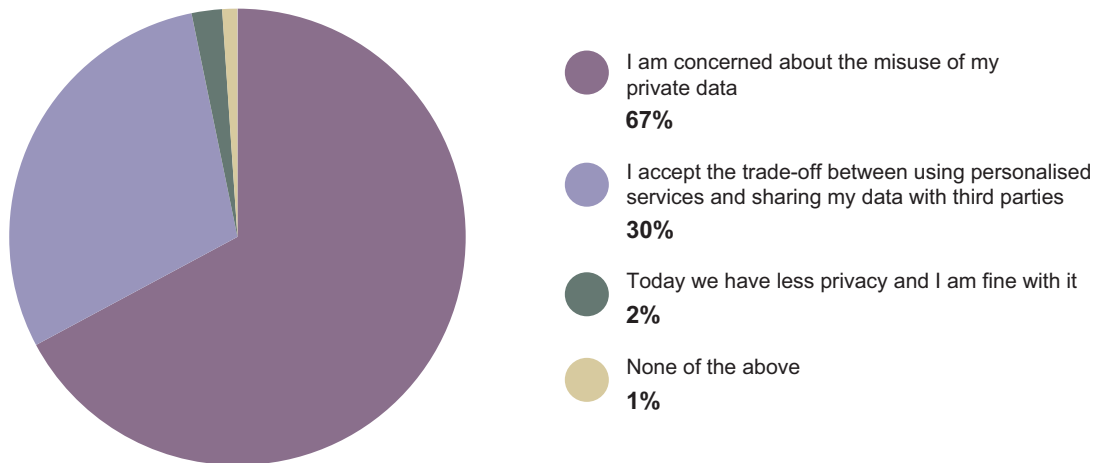


**Finding 5: Privacy vulnerabilities pose a significant concern to users of IoT applications. More transparency among organisations collecting and using data, as well as increased user control and digital literacy, are perceived as key priorities to enable trust and confidence in data sharing and governance.**

With regard to the privacy aspects of the IoT (Figure 12), the majority of respondents (67 per cent) reported that they were concerned about the possible misuse of their private data. Around 30 per cent of respondents accepted the trade-off between using personalised services that IoT products offer and sharing their personal data with third parties for any perceived benefits. Only a very small minority of respondents (2 per cent) stated that they were ‘fine’ with reduced levels of privacy potentially associated with the IoT.

**Figure 12: Respondents’ perceptions of the privacy implications associated with the IoT**

**Question: Which of the following statements regarding Internet of Things privacy do you agree with most?**



Respondents were asked about their views in relation to the data sharing aspects of the IoT. The results are presented in Figure 13. Almost everyone agreed that transparency should be the priority for organisations working in IoT-related areas. Specifically, 99 per cent of respondents agreed or strongly agreed that organisations collecting personal data should be transparent about their use of the data. Similarly, the majority of respondents agreed or strongly agreed that users should be in control of their personal data at all times (88 per cent) and that consumers should be more digitally literate to recognise the potential risks and benefits of data sharing (90 per cent). In light of these views, most respondents (92 per cent) agreed or strongly agreed that policymakers need to re-examine data protection and liability policies.

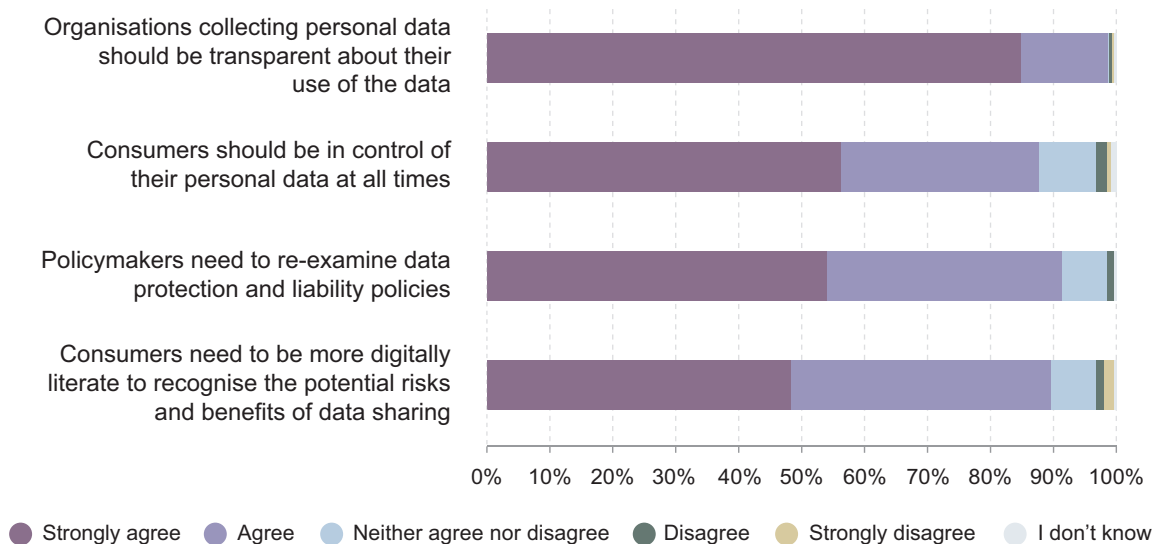


*A threat of the IoT is associated with the collection of unregulated data which on its own is probably not an issue, but when triangulated with other data presents security and privacy issues for individuals and organisations.*



**Figure 13: Respondents' perceptions of the data sharing aspects of the IoT**

**Question: To what extent do you agree or disagree with these statements related to the data-sharing aspects of the Internet of Things?**



**Finding 6:** There is a perception that the public sector could play a stronger role in accelerating the uptake of the IoT in the UK, but that it should put citizens at the forefront of these efforts. The priorities for support are seen to be in ensuring interoperability, investing in people, and fostering multistakeholder collaborations, and less so in creating new business opportunities through public spending.

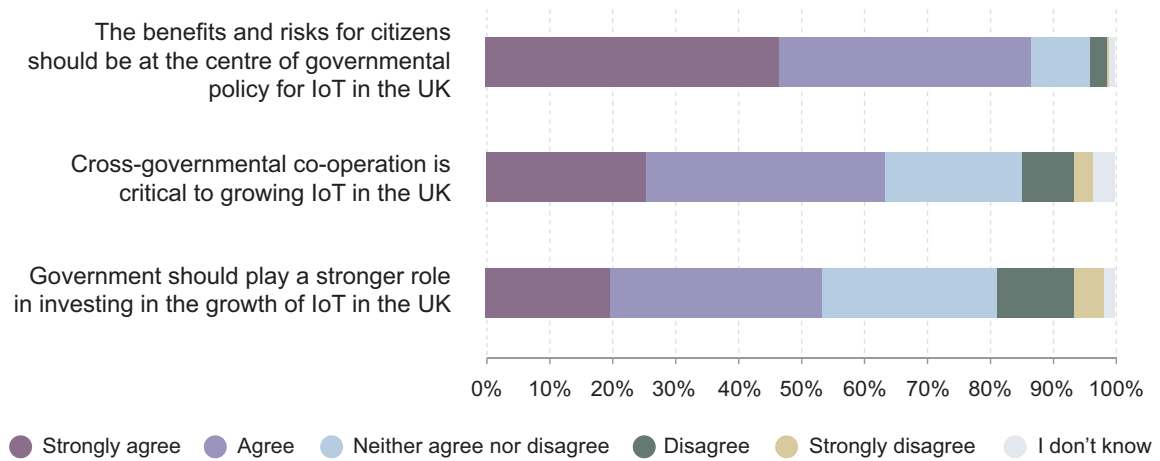
The final set of questions in the survey asked respondents for their views on the role of government in supporting the development of the IoT in the UK. The majority of respondents felt that there was scope for government intervention (Figure 14). Specifically, 53 per cent of respondents agreed or strongly agreed that the UK government should play a greater role in investing in the growth of the IoT in the UK. Only around 17 per cent of respondents disagreed or strongly disagreed that the government should play a stronger role in investing in this area. Moreover, a large majority of respondents (87 per cent) agreed that government policy for IoT should mainly revolve around assessing the benefits and risks of the IoT for its citizens. Regarding cross-governmental co-operation, most respondents (64 per cent) agreed or strongly agreed that co-operation between different government departments and agencies is critical to growing the IoT in the UK.



*The government should be putting the interests of citizens (especially the more vulnerable) above those of corporations, and above personal profit and advancement.*

**Figure 14: Respondents' perceptions of what the role of government should be in relation to the IoT**

**Question: To what extent do you agree or disagree with the following statements about the role of government?**



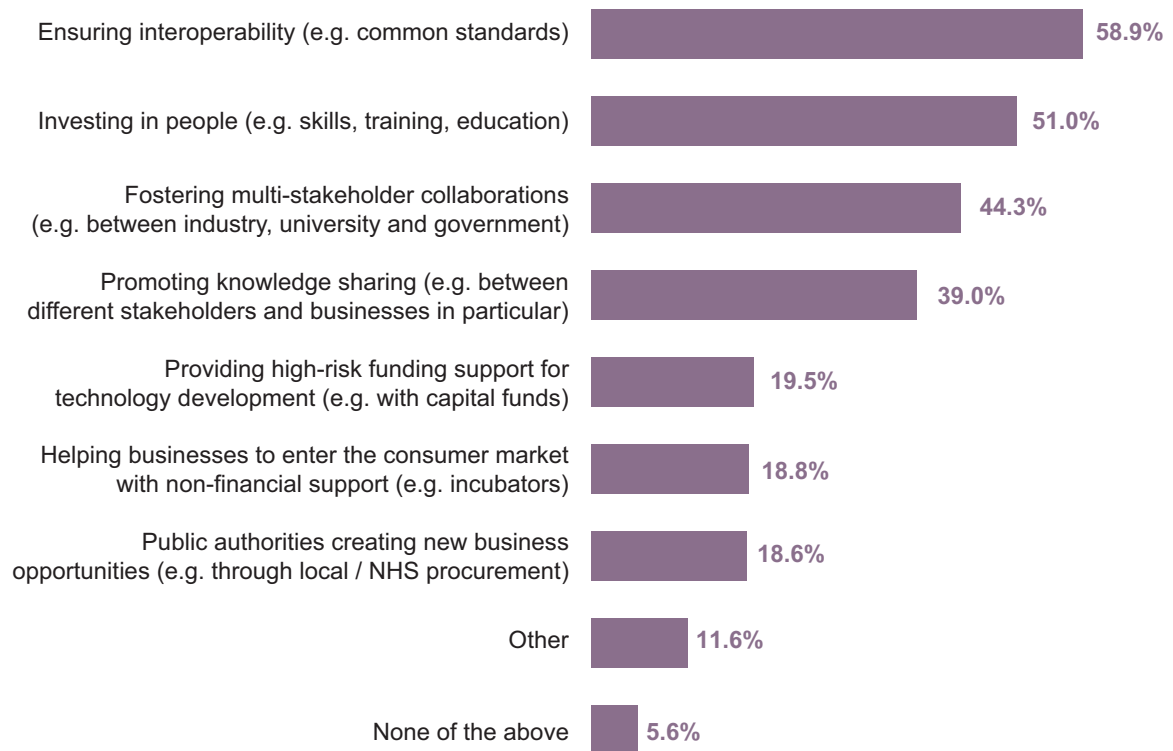
Respondents were also asked to identify what they thought should be the three most important priorities for the government to stimulate the IoT landscape in the UK. The survey results are presented in Figure 15. The most frequently selected option, identified by the majority of respondents (59 per cent), was that the government should consider interoperability and commonality of standards as a priority. Approximately 51 per cent of respondents felt that the government should be investing in people, for example, through skills, training or education. This suggests that for the majority of respondents the framework conditions for the development and diffusion of the IoT are more important than sector-specific interventions or investment. Other significant priorities identified by respondents included fostering multi-stakeholder collaboration between different actors in the IoT industry (e.g. among businesses, research and government) (44 per cent) and promoting knowledge sharing between those actors (39 per cent). Among the less significant priorities identified by respondents were three interventions which can best be described as direct interventions to support the IoT industry, namely, providing high-risk funding support for IoT technology development (20 per cent), helping businesses enter consumer markets with non-financial support mechanisms (19 per cent), and enabling public authorities to create new business opportunities, for example, through their procurement markets (19 per cent). A number of respondents noted in the 'Other' priorities option that the government should play a central role in creating and maintaining the conditions and standards for protecting personal data and privacy, and mitigating the wider security concerns arising from a rapidly evolving IoT landscape.



*The government should be regulating the security and privacy landscape, so that we can maximise benefits and minimise abuse.*

**Figure 15: Respondents' perceptions of the most important priorities for the government to stimulate the IoT**

**Question: What do you think should be the three most important priorities for the government to stimulate the IoT landscape in the UK?**





# Chapter 5: Suggested topics for policy discussion

## 5.1 Introduction

The development and adoption of the IoT presents a number of promising opportunities. However, as the insights from the analysis of the case studies (Chapter 3) show, several important and challenging policy questions arise from the understanding of how IoT-related projects become adopted by the market. Furthermore, as the results of the survey (Chapter 4) have clearly demonstrated, it is crucial to take into account the views and opinions of citizens on the key policy-relevant issues regarding the development of the IoT. In this chapter, we examine our findings to generate a set of policy-relevant priority topics for further exploration and discussion. Within each topic for discussion, we have articulated a series of corresponding key policy questions. These questions are wide ranging and horizontally apply across different sectors and industries. The required responses to these questions are unlikely to be achieved by public policy or industry alone; instead, it may require an active, multi-stakeholder approach. While the questions that follow from our findings are primarily aimed at the community of policymakers, the implications of these findings, which are deliberately formulated as questions, seek to provoke discussion across policy communities, including government policymakers (national and local), innovators, industry, academia and the public.

The topics for discussion we have proposed are grouped into four sets of policy objectives pertaining to IoT in the UK. These are themes for action aimed at (i) supporting research and innovation in the IoT ecosystem; (ii) stimulating demand for the IoT to be adopted more widely by using IoT solutions in the delivery of public services; (iii) strengthening infrastructure and framework conditions for the development and adoption of the IoT as a systemic innovation; and (iv) mitigating the risks of a pervasive IoT. These themes were triangulated against a rapid review of IoT-related policy actions in the UK over the past five years and represent clustered policy measures or actions that share a common objective (see Appendix E for the results of the rapid policy review). Our specific focus was to identify policy objectives and associated priority topics that could maximise the strategic value of the IoT in supporting system-level change in processes, rather than individual point or local innovations involving connected sensing technology. Each of these policy objectives is discussed in turn below in relation to the main insights emerging from the analysis of the case studies and the survey.

## 5.2 Priority topics for further consideration and key policy questions

### 5.2.1 Supporting research and innovation in the IoT ecosystem

As the IoT has become an important strategic area for the public sector in the UK, supporting the IoT as a key area of research and innovation has been the central focus

of governmental efforts to accelerate the IoT in the UK.<sup>35</sup> The majority of IoT-related interventions over the past five years suggest that current and previous governmental efforts have largely concentrated on the technological components of the IoT to catalyse the wider IoT environment, such as developing various types of prototypes and pilots. In addition, our analysis also demonstrated that local authorities are increasingly investing in products and services that have IoT capabilities through their procurement markets. This evidence suggests that public investment indirectly related to IoT is more wide ranging than specific IoT-type sponsorship initiated and led by the central government. Often, investment in IoT technologies is not explicitly oriented towards the more general concept of the IoT and its potential for system-wide change, but is described more narrowly in terms of ‘smart cities’ and various other domain-specific ‘smart-X’ technologies.

In the current context, our case studies suggest that the availability of new technologies is becoming less of a problem than the economic incentives to invest in and purchase new IoT solutions. While better funding support towards late-stage technological development and product commercialisation was a key concern for some of the case study interviewees, it became evident that the technology is the ‘*easy part*’ – for them, the challenges were more focused around finding the ‘*right people to do the job*’ and demonstrating ‘*viable business cases*’.

Aside from research and innovation funding support, there was strong evidence from interviews that it is important for public policy to support the IoT in ‘softer’ ways, such as stimulating collaborations, knowledge or practice exchange, or raising market awareness. The case studies have clearly demonstrated that multi-agency collaborations, particularly partnerships among universities, industry, local government, and local factors (such as progressive and forward-thinking councils) can be critical to developing and commercialising new IoT applications. The surveyed users also recognised the view that policy could play a major role in creating strong framework conditions to allow the IoT to grow and diffuse across the economy. For example, the majority of respondents felt that an important priority for the government should be investment in ‘people’ (i.e. skills, training and education of the workforce). Echoing the views of some of the case study interviewees, a large proportion of respondents also noted that the government should be fostering multi-stakeholder collaborations.

It was suggested by a number of interviewees that the intensity of current governmental activity at the central and local government levels means that there may be a vast amount of hidden knowledge across different levels of government-funded IoT projects. They suggested that their projects would have greatly benefitted from access to experiences and good practices from other government-funded IoT projects. In this regard, the survey respondents also highlighted the importance of promoting knowledge sharing among different actors. The implication of having inadequate access to information means that the ongoing efforts might lead to duplication of efforts in research and innovation in the IoT space. With this

---

35 In 2013, the UK government recognised the strategic importance of IoT for its economic opportunities and recognised it as one of the ‘great technologies’ that could propel the UK to future growth (UK Government 2014). The Technology Strategy Board (now known as Innovate UK) had already started work focused on IoT around mid-2011, when it supported the UK community of researchers and innovators in the IoT ecosystem with an investment of £4m into 8 business-led IoT demonstrators (Innovate UK 2013). This was followed by a number of investments to the Future Cities Demonstrator programme; Milton Keynes Demonstrator; and, most recently, a strategic £32m investment to set up a dedicated national programme of IoT-related activities, called IoTUK (IoTUK 2016a).

in mind, several important issues arise about the extent to which policy could play a key role in disseminating knowledge and information across the IoT market (for example, by providing signals to the market about ‘what works’ and ‘what doesn’t work’ for the successful development and deployment of IoT solutions).

**Priority topic for consideration 1:** *The need to focus on non-technical factors that drive adoption.*

**Key policy questions:**

- How can policy provide or incentivise more investment in non-technical factors for newly created IoT-related innovations?
- How can sector-specific public investment initiatives work together to ensure that tested technologies are applied to new contexts and that system-wide effects are realised?
- How can the policy community create opportunities for effective collaborative networks involving citizens, industry, academia and government?
- What can be done to infuse and sustain a culture of collaboration among the different stakeholders in the IoT ecosystem?
- How can the policy community help to develop and sustain a workforce of sufficient critical mass and with the appropriate technical and commercial skills?

**Priority topic for consideration 2:** *The need for knowledge from previous IoT projects to be shared, helping researchers and businesses avoid reinventing the wheel.*

**Key policy questions:**

- How can the public sector and industry systematically recognise IoT-related projects and capture the lessons learnt from implemented projects, starting with those that have been funded by government?
- What are the ways to disseminate this evidence in a transparent and accessible manner to the various stakeholders in the emerging IoT marketplace?
- How can the policy community systematically map the IoT ecosystem in ‘real time’ to anticipate and identify areas for public and private research and innovation investment more strategically?
- What incentives can be created for the industry to share the lessons of IoT implementations?

## 5.2.2 Stimulating demand for the IoT to be adopted more widely

In the case studies it became evident that public authorities are increasingly purchasing smart technologies for the delivery of public services and infrastructure. In doing so, they help spur greater demand for innovation.<sup>36</sup> While the drivers behind commissioning new technologies seem to include the need to reduce costs in the context of flat and declining

36 There is wide literature on different ways the public sector uses procurement to spur demand for innovation (Edler and Georghiou 2007). Public authorities typically purchase goods and service to deliver public services and create and manage public infrastructure. In pursuing those objectives, they often procure innovative technologies, which normally takes forms of either general procurement when innovation becomes an additional criterion in the call for tender and tender documents and is mostly coordinated by central government, or strategic procurement when the demand use for specific technologies is encouraged promoted in order to stimulate the market and is might not be mostly not coordinated centrally.

budgetary resources and manage increasing demand on public services in the long term, there is generally a lack of systematic understanding of the incentives that drive public authorities to commission those technologies, as well as the barriers they face in purchasing them. Our data indicates that there are considerable barriers for public authorities to build a robust business case for IoT solutions before they can justify public support and use their procurement processes to offer the same opportunities for innovators through, for example, lack of previous track record of implementation. Various interviewees suggested that more could be done increase the capabilities of local authorities for prototyping and initial implementation.

In addition, it is necessary to better understand what kind of procurement processes are best suited for purchasing IoT technologies to be used in larger public infrastructure projects. One interviewee, for example, highlighted that a joint procurement process enabled councils to negotiate lower prices, thus spreading the associated risk when addressing the investment concerns around a large infrastructure project. However, public authorities may not always realise that there is a possibility to apply these latest technologies more widely in public infrastructure projects. A 'value for money' criterion is often the key deciding factor when commissioning public infrastructure projects, with decision making only marginally accounting for the innovation of proposed solutions and the potential to support broader, more radical and disruptive process change.

To achieve wider system-level benefits, public authorities may need to develop stronger capabilities in identifying the 'challenge areas' in which IoT technologies can be applied, how they measure the prospective ROI, what project-level and system-level ROI are delivered, and what are the lessons learnt that could inform similar initiatives across the country.

The challenges of public authorities procuring new technologies were reflected in the views of businesses. For example, it was observed from the case studies that the nature of procurement markets, which tends to favour well-established providers with adequate track record and value for money, creates obvious challenges for those competing for public contracts. This can in some cases be favourable for technologies which are translated into a new context and thus could help their diffusion of IoT applications. However, as noted by some interviewees, the nature of the procurement markets is generally not suitable for smaller industry players, particularly SMEs with innovative technological products and services who often struggle to enter public sector procurement markets and compete against larger players.

In addition, technology providers have noted that demand from public authorities helped them to build more robust use cases and demonstrate the impact of their products to the wider market. From their responses, it became clear that the full economic potential of the IoT appears to be hindered by a lack of market confidence and readiness to invest in and purchase emerging IoT solutions. Specifically, the unavailability of solid business models and user cases, as well as inadequate confidence of potential buyers, were all highlighted as barriers to that adaptation of individual IoT technologies by the market. The perceptions of technology developers suggest that the IoT market might be facing demand-side problems, where costs and barriers to diffusion of scalable products and services remain high, and that there is a potential need for industrial policy to stimulate the demand side of the IoT market more deliberately and explicitly. The evidence from local authorities procuring those technologies has shown that using government procurement markets strategically can



reduce inefficiencies and costs in the delivery of public services, as well as help spur market demand for IoT applications. This observation resonates with the governmental IoT review (Government Office for Science 2014), which recommended that the government should use informed buying power to define best practice and to commission technology that uses open standards and that is interoperable and secure.

However, the attitudes and views of surveyed end users indicate that they did not see the primary role of policy to be to help stimulate demand for IoT innovation. Approximately 40 per cent of survey respondents considered the uncertain return on investment for organisations to be a barrier to the wider adoption of the IoT,<sup>37</sup> and only about one in five respondents (19 per cent) agreed that one of the important priorities for the government should be for public authorities to create new business opportunities (for example, through procurement). Yet the evidence from the case studies shows that some IoT investments arguably have significant return on investment and lead to positive outcomes for citizens and communities. At least in this context, the public does not recognise demand-side procurement of innovative technologies as an instrument to articulate the demand for innovation, and this may lead to the challenges of public organisations to build a strong case for public support.

**Priority topic for consideration 3:** *The opportunities to use IoT technologies in the delivery of public services and to help spur greater market demand.*

**Key policy questions:**

- How can public authorities identify the areas where IoT with system-level benefits might be applied rather than an established solution?
- How can the policy community capture evidence of the effectiveness and impact of local authorities procuring new IoT technologies at the project and system levels?
- What are the challenges faced by procurement authorities in purchasing IoT technologies with limited evidence of benefits, and how can the challenges be recognised in the process?
- How can public authorities ensure that the procurement processes for IoT technologies balance recognition of innovative new-to-market SME suppliers with well-established players?
- Could the supplier selection criteria be revised to reflect the potential of using the IoT in the delivery of public services?
- How can the project-specific and system-level benefits be adequately valued and measured in a business case used by public authorities?
- How can the policy community support the use of IoT technologies for infrastructure projects?

### **5.2.3 Strengthening infrastructure and framework conditions for the development and adoption of the IoT as a systemic innovation**

As noted previously in Chapters 1 and 3, in particular from the perspective of government, the full impact of the IoT will be felt most strongly when its development facilitates system-level change in processes and costs for industry and communities. In network industries such as the IoT, standards can facilitate the formation of an installed base of users, thereby easing

37 Compared with around 90 per cent who were more concerned about the security and privacy issues related to the IoT.

the emergence of technological platforms based on independently supplied but interoperable components due to common technical standards (Van Alstyne 2014). In order to harness the benefits of the network effects of the IoT, standards harmonisation is an important element of achieving interoperability and taking advantage of the system-wide benefits offered by the IoT. Indeed, there is widespread evidence that standardisation generally helps to create critical mass, making it possible to start the exploitation of economies of scale in the formative stages of a market. For example, standards can focus demand for innovations that might otherwise be spread over many technical solutions and might therefore lead to high fragmentation and insufficient critical mass, thus hindering the diffusion of innovation in the economy (Blind 2013).<sup>38</sup> As the case studies illustrate, the sensor and IoT device marketplace is very broad and diverse, and hence there is a risk that the lack of policy intervention would leave standards disharmonised or slow to emerge, or that early major industrial suppliers would dominate with their versions of standards or even with their proprietary communications and connectivity technologies.

In the survey, when respondents were asked about what they perceived to be the important priorities for the government to stimulate the IoT landscape, the majority (59 per cent) noted that the government should play a role in ensuring interoperability through common standards. Similarly, with regard to perceptions of the most important barriers to the wider adoption of the IoT, the majority of respondents (72 per cent) were predominantly concerned about the lack of common standards that would allow devices and information systems to communicate with each other in an IoT ecosystem. In addition, almost 60 per cent of respondents were concerned about the incompatibility of IoT products with legacy systems. Scalability and network benefits of individual technologies are difficult to achieve in the absence of integrated IoT infrastructure solutions across sectoral applications.<sup>39</sup>

Despite there being a case to be made for intervention, policies to support standardisation for IoT are not straightforward. As the government review on IoT showed, the UK cannot unilaterally adopt a standard and '*hope for global consensus*' (Government Office for Science 2014). In light of this observation, the review noted that the government needs to '*use expert commissioning to encourage participants in demonstrator programmes to develop standards that facilitate interoperable and secure systems*' and '*take a proactive role in driving harmonisation of standards internationally*' (Government Office for Science 2014).<sup>40</sup> There

38 There are various international examples where standard harmonisation facilitated interoperability to achieve network effects. For example, in the health domain, there are good indications of what can be achieved with bold policy decisions. Interoperability for telehealth (home monitoring) devices has been a difficult subject for many years, until the emergence of the Continua Alliance (Continua Alliance 2016). Even then, the pace and authority of the emerging Continua standards was relatively slow, until governments started to specify its use in procurements. Denmark in particular led the way with its decision in 2012 to prefer procurement devices for telehealth that were Continua compliant. By 2018, both Norway and Denmark are expected to require Continua compliance for all procured devices.

39 In the UK, for example, the Hypercat Consortium is working towards developing a new standard for secure and interoperable IoT implementations (Hypercat 2016). Hypercat is a consortium of companies, higher educational and research institutions, and local authorities in the UK.

40 The British Standards Institution (BSI) has done some work on standard frameworks for smart cities (BSI 2016). Internationally, the Global Standards Initiative on IoT is promoting a unified approach within the International Telecommunication Union (ITU) Telecommunication Standardization Sector (known as ITU-T) for developing technical standards, and it has created ITU-T Y.2060 to clarify the IoT concept, its scope and its characteristics (ITU 2016). Other initiatives include the IEEE Standards Association's IoT Related Standards, Open Interconnect Consortium, AllSeen Alliance, and IPSO Alliance (Schindler et al. 2014).

remains a strong need to consider the government's available 'levers' in using its intent to prefer, and require compliance with standards across specific IoT domains. Such statements in policy will give all suppliers the incentives to develop their products and services knowing that a market exists for devices with those standards built in. And for the public sector, adherence to the use of standards-compliant devices will mean greater choice and a better market dynamic.

As some of the case studies showed, open standards facilitate interoperability, and there is an appetite from the industry that the government should continue to seek to promote open standards in procured IoT projects, where possible. Because open standardisation processes allow for standards to reflect user needs and therefore promote the diffusion of new products by early adopters (Blind 2013), promoting open standards would mean supporting the creation of IoT products and services that respond more directly to the needs and aspirations of citizens as their primary users.

It became evident in the case studies that the projects had clear ambitions to scale up their individual point solutions and that most of them had 'roadmaps' for future growth. The opportunities to scale up were seen to exist, for example, in improving their capability and increasing their capacity to connect their devices with others, which in turn allows for the creation of new capabilities and the potential to unlock the 'network effects' of the wider IoT network. Businesses largely saw the role of government being to create amenable framework conditions that could help their products and services be scaled up through appropriate infrastructure that connects their solutions to the wider network of devices. More specifically, this included facilitating the creation of interoperable standards, as well as mechanisms to help build public trust in the IoT market.

**Priority topic for consideration 4:** *Sustaining structural change and benefit through interoperability and information sharing across applications.*

**Key policy questions:**

- How can the policy community help to accelerate the development of interoperable standards in IoT nationally and internationally?
- How can publicly funded smart city and large-scale demonstrator projects support the drive towards common standards?
- How can public procurement processes support the use of open IoT-enabling standards and interfaces to gain the critical mass?

**Priority topic for consideration 5:** *Supporting the use of integrated IoT infrastructure across sectoral boundaries to help scalability of individual technologies.*

**Key policy questions:**

- Is there a need to raise awareness among public authorities as to the wider system-level benefits that could potentially be accrued by leveraging IoT technologies as systemic innovations in public infrastructure projects?
- How can the policy community support integrated, interoperable IoT infrastructure solutions rather than continued deployment of individual technologies?
- How can public authorities frame their requirements to encourage IoT standards-compliant devices and services?
- How can the policy community support standards compliance as a pre-requisite for procurement against public sector funding?

## 5.2.4 Mitigating the risks of a pervasive IoT

While public policy efforts to create an IoT ecosystem in the UK have explicitly aimed to harness the enormous potential economic opportunities associated with the development and adoption of the IoT, concerns about present and potential negative externalities for society have not been a significant part of these efforts. Based on the evidence from this study, in order to mitigate public lack of trust in the IoT, there must be insurance against the risks posed by the pervasiveness and scale of the IoT phenomenon. There is a strong case for public policy developments to ensure that the risks of connected devices are assessed and addressed, particularly when they become connected to wider networks. In our survey, informed users of technology clearly expressed that the government should continue to invest in advancing the IoT in the UK. However, crucially, the survey results suggested that government policy for IoT should primarily revolve around assessing the benefits and risks of the IoT for its citizens. Respondents expressed significant levels of concern about privacy, security and data-related issues in IoT-enabled systems. For as long as IoT projects and devices are still relatively isolated in their implementation, such concerns are valid but are restricted to risks that are bounded. However, as the pervasive nature of IoT technology expands and system-level changes are enabled, the risks associated with issues such as security and privacy will grow exponentially. It is also true that no IoT system can ever be completely secure or private yet remain operational; there will always be risks of data exposure and cyber attack inherent in the IoT.<sup>41</sup>

From the perspective of businesses, fulfilling the economic potential of the IoT is a pressing concern, whether they are agile start-ups or large firms. For informed users of technology, however, at least based on the results of our survey, economic factors do not appear to be primary concerns. Perhaps for end users, security vulnerabilities and concerns related to

41 There is an analogy in the use of data collected and used to deliver healthcare, and in health research. Over the past 20 years, the increasing number of systems used in healthcare has led to concerns over privacy and security. The policy response has been to develop increasingly strong measures to assess and protect health data, largely through the use of information governance processes, including a standard Information Governance Toolkit (HSCIC 2016). Ever more rapid progress in the network effect of information in health has led some governments (that of Sweden, for example, Läkemedelsverket Medical Products Agency [2016]) to start to consider regulating health information systems as tightly as medical devices.

privacy and data governance are, not unreasonably, perceived to be the most critical barriers to the wider adoption of the IoT. There is seemingly a fundamental dichotomy between addressing business concerns, on the one hand, and the apprehensions perceived by the 'public', on the other. Therefore, the development of the IoT has direct implications for the relationship between citizens (as 'users' of technology) and businesses (as 'providers' of technology).

It is clear that more needs to be done in the context of sharing data in an increasingly connected world, particularly in relation to IoT applications that collect personal data and in relation to the transparency of its collection, storage and use. There is a case to be made for information governance to be at the heart of creating trust in the IoT. As is clear from the responses to our survey, the misuse of personal data is a prominent concern for the public, and there is an expectation from individuals that organisations should become more transparent about the way they collect and use data. When individuals effectively lose control and awareness of how their data is being used, this leads to erosion in trust and a diminishing acceptance of the merits of the IoT. Indeed, the survey results highlight that there is a strong perception that consumers should be in control of their personal data at all times, signalling a distinctive move towards individuals themselves acting as their own 'data controllers'. The lack of trust in IoT-enabled devices and systems may restrict their adoption by some sectors of the population. For others, adoption without understanding the associated risks may increase vulnerabilities. The key to resolving the apparent misalignment of incentives between businesses and end users could be to find mechanisms for creating trust in devices, services and organisations.

Our survey results also highlighted the strong view that consumers should be more digitally literate in order to be able to recognise the potential risks and benefits of data sharing. The opportunity thus exists to develop and implement tools to 'educate' consumers about understanding and interacting with new technologies, specifically with such topics as security and privacy considerations and data sharing. It is also worth reiterating that several case study interviewees underlined the importance of involving citizens in helping to design 'user-driven' IoT solutions to facilitate faster adoption by the market.

Cybersecurity risks are being addressed continuously by industry and government bodies. Our survey revealed concerns over the impact of potential security vulnerabilities on critical national infrastructure. Several case study interviewees articulated clear ambitions to scale up their solutions by connecting to the wider network of objects in order to enable new capabilities. As such, the potential cyber vulnerabilities are likely to affect the resilience of networks and systems underpinning the IoT networks. The growing adoption of the IoT necessitates paying greater attention to the potential impact of the system-wide impact of the IoT (rather than individual IoT deployments) on the critical national infrastructure. In the USA, the National Security Telecommunications Advisory Committee (NSTAC) issued a report examining the cybersecurity implications of the IoT within the context of national security and emergency preparedness. As this report concludes, critical infrastructure IoT devices are increasingly automated and adaptive, collecting data from the systems they control and then acting on that data; failure of some of these systems would have profound national impacts (NSTAC 2014). These impacts could be in the economic realm, such as lost productivity and damage to the national economy, or in the public safety realm, including kinetic damage or, in extreme cases, potentially catastrophic failure of machinery or infrastructure. Managing IoT

risks could be a reasonably discrete aspect of critical national infrastructure management. In the UK, there are actions being taken on critical national infrastructure, but the diffused nature of IoT connections makes such actions in relation to the IoT complex. To date, to the best of our knowledge, the UK government has not conducted any comprehensive assessment of present and potential cyber-risks and security vulnerabilities from the pervasiveness and connectivity of IoT devices as they become diffused throughout the economy.

**Priority topic for consideration 6:** *Supporting a trusted, people-centric IoT ecosystem.*

**Key policy questions:**

- How can the policy community help industry balance economic objectives with creating an IoT ecosystem that is more open, trustworthy and inclusive?
- How can the recognised processes for certifying devices be adapted to deal with the specific trust challenges posed by the IoT, including consent and information governance?
- Can the policy community encourage industry to be open about information governance processes and reporting of incidents?
- How can the policy community incentivise industry to adopt people-centric design and development?
- How can the policy community catalyse better 'social contracts' between individuals and organisations (including government) as the private and public spheres of personal data are progressively blurred?
- What steps can be taken to raise cyber awareness and educate citizens about the potential benefits and risks associated with the IoT?

**Priority topic for consideration 7:** *Addressing concerns about the risks of IoT technologies to critical national infrastructure.*



**Key policy questions:**

- How can the policy community support the systematic assessment of risks associated with innovative IoT technologies and their deployment in public infrastructure?
- How can current contingency plans be enhanced to identify and manage security risks associated with a growing and pervasive IoT?

In Table 5, we present a summary of each of the proposed priority topics for consideration clustered by the policy objectives, along with the supporting policy questions. In Appendix F, we present a summary of the findings from the analyses of the case studies and the survey, and visually indicate how each of the findings link to the proposed priority topics for consideration.



**Table 5: The proposed priority topics for discussion and the associated key policy questions**

Policy objectives	Priority topics for consideration	Key policy questions
 <p><b>Supporting research and innovation in the IoT ecosystem</b></p>	<p>The need to focus on non-technical factors that drive adoption</p> <p>The need for knowledge from previous IoT projects to be shared, helping researchers and businesses avoid reinventing the wheel</p>	<ul style="list-style-type: none"> <li>• How can policy provide or incentivise more investment in non-technical factors for newly created IoT-related innovations?</li> <li>• How can sector-specific public investment initiatives work together to ensure that tested technologies are applied to new contexts and that system-wide effects are realised?</li> <li>• What steps can be taken by the policy community to create opportunities for effective collaborative networks involving citizens, industry, academia and government?</li> <li>• What can be done to infuse and sustain a culture of collaboration among the different stakeholders in the IoT ecosystem?</li> <li>• How can the policy community help to develop and sustain a workforce of sufficient critical mass and with the appropriate technical and commercial skills?</li> </ul> <ul style="list-style-type: none"> <li>• How can the public sector and industry systematically recognise IoT-related projects and capture the lessons learnt from implemented projects, starting with those that have been funded by government?</li> <li>• What are the ways to disseminate this evidence in a transparent and accessible manner to the various stakeholders in the emerging IoT marketplace?</li> <li>• How can the policy community systematically map the IoT ecosystem in 'real time' to anticipate and identify areas for public and private research and innovation investment more strategically?</li> <li>• What incentives can be created for industry to share the lessons of IoT implementations?</li> </ul>
 <p><b>Stimulating demand for the IoT to be adopted more widely</b></p>	<p>The opportunities to use IoT technologies in the delivery of public services and to help spur greater market demand</p>	<ul style="list-style-type: none"> <li>• How can public authorities identify areas where IoT with system-level benefits might be applied rather than an established solution?</li> <li>• How can the policy community capture evidence of the effectiveness and impact of local authorities' procuring of new IoT technologies at the project and system levels?</li> <li>• What are the challenges faced by procurement authorities in purchasing IoT technologies with limited evidence of benefits, and how can these challenges be recognised in the process?</li> <li>• How can public authorities ensure that the procurement processes for IoT technologies balance recognition of innovative, new-to-market SME suppliers with well-established players?</li> <li>• Could the supplier selection criteria be revised to reflect the potential of using the IoT in the delivery of public services?</li> <li>• How can the project-specific and system-level benefits be adequately valued and measured in a business case used by public authorities?</li> <li>• How can the policy community support the use of IoT technologies for infrastructure projects?</li> </ul>

Policy objectives	Priority topics for consideration	Key policy questions
 <p><b>Strengthening infrastructure and framework conditions for the development and adoption of the IoT as a systemic innovation</b></p>	<p>Sustaining structural change and benefit through interoperability and information sharing across applications</p>	<ul style="list-style-type: none"> <li>• What can the policy community do to help to accelerate the development of interoperable standards in IoT nationally and internationally?</li> <li>• How can publicly funded smart city and large-scale demonstrator projects support the drive towards common standards?</li> <li>• How can public procurement processes support the use of open IoT-enabling standards and interfaces in order to gain critical mass?</li> </ul>
	<p>Supporting the use of integrated IoT infrastructure across sectoral boundaries to help scalability of individual technologies</p>	<ul style="list-style-type: none"> <li>• Is there a need to raise awareness among public authorities as to the wider, system-level benefits that could potentially be accrued by leveraging IoT technologies as systemic innovations in public infrastructure projects?</li> <li>• How can the policy community support integrated, interoperable IoT infrastructure solutions rather than the continued deployment of individual technologies?</li> <li>• How can public authorities frame their requirements to encourage IoT standards-compliant devices and services?</li> <li>• How can the policy community support standards compliance as a prerequisite for procurement against public sector funding?</li> </ul>
 <p><b>Mitigating the risks of a pervasive IoT</b></p>	<p>Supporting a trusted, people-centric IoT ecosystem</p>	<ul style="list-style-type: none"> <li>• How can the policy community help industry balance economic objectives with creating an IoT ecosystem that is more open, trustworthy and inclusive?</li> <li>• How can the recognised processes for certifying devices be adapted to deal with the specific trust challenges posed by the IoT, including consent and information governance?</li> <li>• How can the policy community encourage industry to be open about information governance processes and the reporting of incidents?</li> <li>• How can the policy community incentivise industry to adopt people-centric design and development?</li> <li>• How can the policy community catalyse better 'social contracts' between individuals and organisations (including government) as the boundaries between the private and public spheres of personal data are progressively blurred?</li> <li>• What steps can be taken to raise cyber awareness and educate citizens about the potential benefits and risks associated with the IoT?</li> </ul>
	<p>Addressing concerns about the risks of IoT technologies to critical national infrastructure</p>	<ul style="list-style-type: none"> <li>• What can the policy community do to support the systematic assessment of risks associated with innovative IoT technologies and their deployment in public infrastructure?</li> <li>• How can current contingency plans be enhanced to identify and manage security risks associated with a growing and pervasive IoT?</li> </ul>



# Chapter 6: Concluding remarks

---

We have closely examined the public policy implications of real IoT implementations and user perspectives to provide input to a feedback loop for the whole IoT policy community. The case studies we analysed have demonstrable outputs and tangible 'roadmaps' for the future, and are illustrative of the changes that are happening at the frontier of IoT industrial activity in the UK. Furthermore, as the IoT ecosystem continues to evolve within the UK as well as globally, citizens will be at the centre of these developments. We complemented our research on IoT case studies from the perspective of businesses with a focused opinion survey of a sample of informed users of technology in the UK. The survey shed light on how the main policy-relevant issues related to the progress of the IoT in the UK are perceived outside specific IoT projects. We hope that using this bottom-up approach to engage with and examine the role of two key groups of stakeholders in the IoT ecosystem – businesses and individual users of technology – has generated deeper insight for the policy feedback loop. We also propose that the method we deployed in this study can be used in the future to provide a continuous feedback mechanism on how the impact of IoT-related policy is progressing in the UK – for instance, by using the survey generated for this report again, comparatively, in the future.

The IoT is a rapidly evolving area that has implications for a wide range of industry sectors and stakeholders. Its development holds great promise to deliver socio-economic benefits, and there is a clear case for businesses and the public sector to harness the opportunities made possible by the features of IoT technology – sensing, connectivity, feedback and collaborative processes – both locally and at the system level. The UK government has already recognised the importance of the IoT to its own performance, to that of UK industry, and as a growth market for innovative UK technology companies, especially SMEs. In creating IoTUK, it has committed significant investment to the IoT, making IoTUK a dedicated resource that can support the delivery of government policy and catalyse markets.

The challenges of making the most of the potential of the IoT are, however, significant. There are an ever-increasing number of connected devices, communications and collaboration technologies that make use of IoT principles – often aimed at and procured by projects that are geographically, organisationally and technologically localised and which do not self-characterise as being IoT-related. Many of these projects are unaware of each other; many are supported by public investment from different sources and thus encounter policies from multiple national government departments and from local government initiatives.

Yet the success of the IoT itself ultimately depends on system-level change in processes and use of rapid feedback capabilities across boundaries to secure the full benefits on offer. An uncertain investment return on new technologies is especially challenging for systemic IoT applications that often involve the public sector and require significant up-front investment. For businesses that are keen to operate in this space, this leads to the problem of attracting investors with more realistic expectations about return on investment. For public sector organisations, the uncertainty creates difficulties in obtaining the initial buy-in and justifying the public investment.

Moreover, the role of citizens cannot be overemphasised in debates about the future of the IoT. The explicit inclusion of the public as stakeholders in the IoT ecosystem is imperative if a reliable, open and trustworthy IoT landscape is to be established. In particular, citizens need to have a good understanding of the benefits and risks associated with the IoT. Crucial questions raised in this study relate to how the UK can most effectively enable the deployment of IoT products and services to foster business opportunities while creating public trust and confidence in the principles by which the IoT is governed. The priority topics we have highlighted for further consideration represent ideas that the policy community might consider that, in our view, could help optimise the manner in which government and industry currently support IoT efforts in the UK.

Our analysis indicates that some of the key questions relate to the ways in which government, in particular, can encourage and shape the IoT marketplace, as well as to the timing and consequences of such initiatives. The IoT is a potentially pervasive innovation that is developing rapidly. While much is known about the IoT, it would be too soon to describe it as a mature and stable innovation, for all its significance. The moment is right, therefore, for the policy community to address underlying questions and concerns and to shape the development of the IoT in light of both business needs and informed public preferences. The first steps in this direction might involve addressing the questions raised concerning setting the right framework conditions that ensure long-term growth for the IoT, as well as recognising and understanding the nature of the IoT as a systemic innovation requiring funding, standards, evidence and trust.

# References

---

- BCS. 2013. *The Societal Impact of the Internet of Things*. As of 10 March 2016: <https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf>
- BCS. 2016. 'Levels of membership.' As of 11 March 2016: <http://www.bcs.org/category/5779>
- Bi, Zhuming, Li Da Xu, & Chengen Wang. 2014. 'Internet of Things for Enterprise Systems of Modern Manufacturing.' *IEEE Transactions on Industrial Informatics* 10 (2): 1537–46.
- Blind, Knut. 2013. *The Impact of Standardization and Standards on Innovation*. Published as part of the Compendium of Evidence on the Effectiveness of Innovation Policy Intervention. As of 10 March 2016: [http://www.innovation-policy.org.uk/share/14\\_The%20Impact%20of%20Standardization%20and%20Standards%20on%20Innovation.pdf](http://www.innovation-policy.org.uk/share/14_The%20Impact%20of%20Standardization%20and%20Standards%20on%20Innovation.pdf)
- Borgia, Eleonora. 2014. 'The Internet of Things Vision: Key Features, Applications and Open Issues.' *Computer Communications* 54: 1–31.
- Breathe Heathrow. 2016. 'Breathe Heathrow: Democratising air data to meet local needs.' As of 11 March 2016: <http://theodi.org/summer-showcase-breathe-heathrow>
- Bristol is Open. 2016. 'Open Programmable City Region.' As of 11 March 2016: <http://www.bristolisopen.com/>
- BSI (British Standards Institution). 2014. 'PAS 181 Smart City Framework.' As of 10 March 2016: <http://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/>
- BSI. 2016. 'Smart City Standards and Publications.' As of 10 March 2016: <http://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/>
- Cisco Systems. 2014. *The Internet of Everything: Global Public Sector Economic Analysis, Future to Life*. San Jose, CA: Cisco Systems.
- Continua Alliance. 2016. 'About Continua.' As of 10 March 2016: <http://www.continuaalliance.org/about-continua>
- Digital Catapult. 2015. *Trust in Personal Data: A UK Review*. As of 10 March 2016: <http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf>
- Edler, J., & L. Georghiou. 2007. 'Public Procurement and Innovation – Resurrecting the Demand Side.' *Research Policy* 36 (7): 949–63.

Ehealthnews. 2013. 'Denmark's New Continua-Compliant National Health IT Reference Architecture Available in English.' As of 10 March 2016: <http://www.ehealthnews.eu/industry/3638-denmarks-new-continua-compliant-national-health-it-reference-architecture-available-in-english>

Government Office for Science. 2014. *The Internet of Things: Making the Most of the Second Digital Revolution*. As of 10 March 2016: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/409774/14-1230-internet-of-things-review.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf)

Hall, Jeremy K., & Michael J.C. Martin. 2005. 'Disruptive Technologies, Stakeholders and the Innovation Value-added Chain: A Framework for Evaluating Radical Technology Development.' *R&D Management* 35 (3): 273–84.

Heher, Anthony D. 2006. 'Return on Investment in Innovation: Implications for Institutions and National Agencies.' *The Journal of Technology Transfer* 31 (4): 403–14.

Hoffman, D.L., & T.P. Novak. 2015. 'Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things.' Available at SSRN 2648786.

HSCIC (Health & Social Care Information Centre). 2016. '2016: Information Governance.' As of 10 March 2016: <http://systems.hscic.gov.uk/infogov>

Hwang, Yoon-Min, Moon Gyu Kim, & Jae-Jeung Rho. 2015. 'Understanding Internet of Things (IoT) Diffusion: Focusing on Value Configuration of RFID and Sensors in Business Cases (2008–2012).' *Information Development* 0266666915578201.

Hypercat. 2016. 'Hypercat.' As of 13 March 2016: <http://www.hypercat.io/>

Innovate UK. 2013. 'Internet of Things Ecosystem Demonstrator.' As of 10 March 2016: <https://connect.innovateuk.org/web/internet-of-things-ecosystem-demonstrator/article-view/-/blogs/the-list-of-8-internet-of-things-clusters>

IoTUK. 2016a. 'About Us.' As of 10 March 2016: <http://iotuk.org.uk/about-us/>

IoTUK. 2016b. 'Case Studies.' As of 10 March 2016: <http://iotuk.org.uk/case-studies/>

IoTUK. 2016c. 'FAQs.' As of 10 March 2016: <https://iotuk.org.uk/about-us/faqs/>

ITU (International Telecommunication Union). 2016. 'Y.2060: Overview of the Internet of Things.' As of 10 March 2016: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>

Jason Davies. 2016. 'Jason Davies Word Cloud Generator.' As of 16 February 2016: <https://www.jasondavies.com/wordcloud/>

Läkemedelsverket Medical Products Agency. 2016. 'Guidance for Qualification and Classification of Medical Information Systems.' As of 10 March 2016: <https://lakemedelsverket.se/english/All-news/NYHETER-2013/Guidance-for-qualification-and-classification-of-Medical-Information-Systems/>

Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, & Alex Marrs. 2013. 'Disruptive Technologies: Advances That Will Transform Life, Business and the Global Economy. 2013. McKinsey Global Institute.' As of 10 March 2016:

<http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies#0>

Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, & Dan Aharon. 2015. 'The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute.' As of 10 March 2016:

<http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>

NSTAC (National Security Telecommunications Advisory Committee). 2014. *NSTAC Report to the President on the Internet of Things*. As of 10 March 2016:

<https://www.dhs.gov/sites/default/files/publications/loT%20Final%20Draft%20Report%2011-2014.pdf>

OECD (Organisation for Economic Co-operation and Development). 2015a. 'Data-driven Innovation for Growth and Well-being.' As of 10 March 2016:

<http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm>

OECD. 2015b. 'Digital Economy Outlook 2015.' As of 10 March 2016:

<http://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+outlook+2015/dbdec3c6-ca38-432c-82f2-1e330d9d6a24>

OECD. 2015c. 'System Innovation: Synthesis Report.' As of 10 March 2016:

[https://www.innovationpolicyplatform.org/sites/default/files/general/SYSTEMINNOVATION\\_FINALREPORT.pdf](https://www.innovationpolicyplatform.org/sites/default/files/general/SYSTEMINNOVATION_FINALREPORT.pdf)

Parker, Geoffrey, & Marshall Van Alstyne. 2005. 'Two Sided Networks: A Theory of Information Product Design.' *Management Science* 51 (10): 1494–1504.

QinetiQ. 2015. *Emerging Technologies*. As of 10 March 2016:

[https://www.cpni.gov.uk/Documents/Publications/2015/05-June-2015-Emerging%20Technologies%202015%20-%20V2\\_PV.pdf](https://www.cpni.gov.uk/Documents/Publications/2015/05-June-2015-Emerging%20Technologies%202015%20-%20V2_PV.pdf)

Schindler, Helen Rebecca, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge, & Hans Graux. 2013. *Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things*. SMART 2012/0053. Santa Monica, CA: RAND Corporation. As of 10 March 2016:

[http://www.rand.org/pubs/research\\_reports/RR356.html](http://www.rand.org/pubs/research_reports/RR356.html)

Schindler, Helen Rebecca, Salil Gunashekar, Jonathan Cave, Jamal Shahin, Alun Rhydderch, Benjamin Cave, Catherine A. Lichten, Nicole van der Meulen, Veronika Horvath, Sonia Sousa, & Enora Robin. 2014. *Foresight Services to Support Strategic Programming within Horizon 2020*. Foresight report (D3). Santa Monica, CA: RAND Corporation. As of 10 March 2016: [http://www.rand.org/pubs/research\\_reports/RR900.html](http://www.rand.org/pubs/research_reports/RR900.html)

Silent Herdsman. 2016. 'Cattle Health Care Management System: Silent Herdsman.' As of 11 March 2016: <http://silentherdsman.com/en/technology/>

TNO. 2014. *Systemic innovation: Concepts and tools for strengthening National and European eco-policies*. As of 10 March 2016:

[https://www.tno.nl/media/3388/systemic\\_innovation\\_eco\\_policies\\_tno\\_2014\\_r10903.pdf](https://www.tno.nl/media/3388/systemic_innovation_eco_policies_tno_2014_r10903.pdf)

UK Government. 2014. 'New eight great technologies internet of things.' As of 10 March 2016:

<https://www.gov.uk/government/publications/new-eight-great-technologies-internet-of-things>

Van Alstyne, Marshall. 2014. 'The Economics of Internet of Things.' *MIT Technology Review* July/August: 3.



World Economic Forum. 2015. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*. As of 10 March 2016:

[http://www3.weforum.org/docs/WEFUSA\\_IndustrialInternet\\_Report2015.pdf](http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf)

## Appendix A: Illustrations of the IoT in action in the UK

A key objective of the study was to examine the likely policy implications of specific IoT implementations in order to get a better idea of what is happening at the frontier of IoT activity in the UK. To do this, we looked at nine ‘real world’ examples of IoT implementations (or case studies) that had been previously identified by IoTUK.<sup>42</sup> Table 6 provides short write-ups of the nine case studies, and as a visual representation, Figure 16 presents a map of the UK with their locations.

**Table 6: Summary descriptions of the nine IoT-related case studies examined in the study**

	<p><b>Connected lighting on the South Coast: Smart street lighting controlled through a central platform</b></p>
	<p>On the UK’s South Coast, there is an installation of more than 150,000 smart street lights, one of the largest installations of its kind in the UK. The councils of Southampton and Hampshire committed to building a smart street lighting network within their respective boundaries using wireless technology supplied and managed by Mayflower Complete Control. A ZigBee wireless network, developed by Mayflower and supported by its technology partner, The Technology Partnership, connects each light to a central control platform, which enables intelligent dimming to reduce power costs and real-time monitoring of power consumption. The smart street lighting has resulted in reductions in energy consumption, light pollution and carbon emissions. There is potential to link the street lights with other smart city solutions, such as environmental monitoring and data sharing with emergency services and the public. Looking to the future, Mayflower has its sights set on rolling out more of its lighting Central Management Systems in the UK, and it is looking across the Atlantic to the United States.</p>
	<p><b>Smart bins as a service: ‘BigBelly’ solar powered bins come to Nottingham</b></p>
	<p>The city of Nottingham has deployed ‘BigBelly’ bins in the city centre – a series of connected, solar-powered compactor rubbish bins. What makes this implementation an IoT solution is the ability to connect an everyday object – a bin, in this case – with a centralised computer system to achieve significant savings and efficiencies in waste management. The frequency of bin collections has reduced from 4,400 to just 260 a week, and there has been a reduction in the need for street sweeping to deal with rubbish bin overflows. The project is currently implemented with approximately 170 bins in a variety of locations around the city, which are especially positioned in areas with high foot-fall and pedestrian traffic. Extended technological features, such as WiFi and environmental monitoring sensors, have been considered. The project is self-financing through a reduction in the number of collections and vehicles needed to empty the bins. Further savings have been made through the sale of advertising space on the sides of the bins.</p>

<sup>42</sup> The case studies that we examined in the project were selected by IoTUK on the basis of research commissioned by IoTUK that looked at examples of IoT implementations across different sectors in the UK. See, for example, IoTUK (2016b) for a summary of some of these projects.





### Smart parking in Westminster: Smart parking made open for the community

Parking bay sensors have been deployed in the City of Westminster borough in central London. It is estimated that around half a million vehicles enter the City each day. To cover the total of 40,000 on-street spaces in the borough, the current project is rolling out 10,000 SmartEye sensors in fixed locations. Innocuously positioned in the road surface along the kerb-sides of busy Westminster streets, the smart parking sensors help drivers find available parking spots using an app. The data from the system is publically available and published on an open API, enabling innovative start-ups to launch their own app and compete in the digital ecosystem. The future ambitions of the project are: to roll out the SmartEye sensors and open API to other boroughs and to tile London with a holistic smart parking solution.



### Travelling in the North East: The 'Pop Card' smart ticketing and payment platform

Tyne and Wear Metro has introduced a £25m smart ticketing system to enable passengers to travel the rail network on a single card. Nexus, the public body for and implementer of the IoT solution, is one of the leading card carriers in the UK. It proved the smart card solution in a six-month pilot programme, in partnership with local councils and commercial transport authorities. The smart ticketing solution is being implemented in conjunction with the 'all change modernisation programme', worth around £350m over 11 years. More than 40 million passengers used the system in 2015. Passengers with a 'Pop Card' can top up or renew their card online. The ticketing system employs the national standard, which allows all Pop Cards to be used on buses and trains throughout the region and ultimately throughout the country.



### Opening a city: An R&D testbed in Bristol that can be used for city scale trials

Enabled by the digital infrastructure of the Bristol Is Open project, Bristol is becoming an open programmable city - an IoT 'test bed'. Working with a number of global and local technology companies, Bristol Is Open is a joint venture between the University of Bristol and Bristol City Council. It is funded through local, national and European government funds, as well as academic research and private sector funds. To bring the project to life, the technology installed in the city includes fibre buried underground, mesh networks to connect (for example) lampposts and bins, as well as a wireless 'mile' to test 4G, LTE and 5G wireless technologies. Using the Software Defined Operating System, partners are given a 'slice of the network' to work with, and they can then engineer any number of smart solutions from datasets on such areas as education, energy, finance, health and mobility.



### Advancing telehealth in the North East: Benefitting patients and families with simple telehealth solutions

The telehealth initiative in the north-east of England led by the National Health Service (NHS) and the Academic Health Science Network for the North East and North Cumbria (AHSN NENC) is a health and social care initiative using Internet-enabled technology and devices. To date, telehealth has implemented its programmes across six foundation trusts, 28 hospital departments, 12 community teams, six Clinical Commissioning Groups, 128 general practices, 4 local authorities, 2 third-sector organisations and 700 clinicians. The project is an integration of different technologies across the NHS, allowing for more joined-up and patient-centric services at a local level. The efficiencies gained by monitoring patient conditions from their own homes allow hospitals to target their increasingly scarce resources to the highest priority patients. Text messaging between patients and clinicians is one such user-facing system, whereas most efficiencies are in the digitisation and joining up of back-end services. Looking to the future, the intellectual property developed during the NHS-AHSN NENC programme is to be used in a wide-ranging development of digital health across the North, which will include a high number of 'vanguard' programmes.





### **Farm herd sensing: Connecting farmers to their herds through sensors**

Silent Herdsman began with the support of University of Strathclyde in 2005. With financial support from Scottish Enterprise, Innovate UK and private equity, more than 350 farms and countless cows have been wirelessly connected together. The research and development (R&D) has effectively led to a demand-driven solution. The smart collars placed on the cows allow farmers to accurately predict the insemination window for cows in order to maximise milk yields, as well as their grazing patterns. With test farms in the UK, the USA and Europe, Silent Herdsman offers an internationally competitive product and service. For the farmers, return on investment is typically seen within 12 to 15 months. Future ambitions include migrating services to a cloud-based management system.



### **London City Airport demonstrator: Creating a connected retail space**

London City Airport, in conjunction with Living PlanIT and Milligan, has implemented an airport-wide IoT solution to enhance passenger experience and airport management. With 4.3 million people a year passing through the airport, managing passenger flows is critically important. Living PlanIT worked closely with the Airport to create an app tailored to the user experience and passengers to shop online. A sensor network installed in the airport assisted in managing passenger flows, with the result that the rush hour peaks in the mornings and afternoons have been smoothed. Real-time analysis of passenger flows helps to shape demand and assist during heavy use. Businesses within the terminal are increasing their turnover by up to 30 per cent and demonstrating return on investment. As a result of this project, Living PlanIT has taken the IoT solution abroad to assist other airports in developing connected retail spaces.



### **Breathe Heathrow: Using open data to help the public understand air quality and noise impacts**

Heathrow is the largest airport in the UK and is a key source of air pollution in London. Breathe Heathrow is an air monitoring project conceived and implemented by IoT company OpenSensors that has been designed to help residents in the Heathrow region of London understand the air quality and noise impacts the airport has on their local areas. A network of connecting air quality and noise sensors in the gardens of volunteers uploads data on CO<sub>2</sub>, NO<sub>2</sub>, temperature, humidity and noise levels to a centralised platform, where it is stored, monitored and analysed. All residents can access, use and share these data. This 'smart city' initiative of 'democratising' data sets has empowered local communities and decisionmakers through the simple visualisation of complex datasets.

Figure 16: Geographic locations of the nine IoT-related case studies examined in the study



## Appendix B: Semi-structured protocol for case study interviews

---

### *[Introductory questions]*

- A1. What is the nature of your involvement in the project?
- A2. How long have you been involved with the project?
- A3. What is your general understanding of the Internet of Things (IoT) landscape in the UK?
- A4. Do you regard your project as being an IoT implementation? Why / why not?

### **Q1. [Current state of the project]**

Can you please tell us about the current state of the project?

#### **SQ1.1 Team make-up**

What is the make-up of the internal project team?

#### **SQ1.2 Stakeholder involvement**

Who are the different stakeholders that you interacted with when the project was being set up / implemented, and what was the nature of these interactions?

### **Q2. [Financing model]**

Could you explain the nature of your financing model? With the benefit of hindsight, has this been effective, and if so, in what way?

#### **SQ2.1 [Stakeholder expectations on the return of investment and risks]**

How successfully has the financing model met the expectations of investees and stakeholders?

Are they prepared to continue to invest in the initiative's expansion?

### **Q3. [Enabling factors]**

What do you think were the key factors that enabled you to reach the current stage in the implementation of your project?

### **Q4. [Barriers to implementation]**

What were the obstacles that you had to overcome to reach the current stage of the project?

#### **SQ4.1 Approaches to addressing barriers**

How did you (try to) manage these challenges?

Are there different barriers you see for the sector as a whole?

**Q5. [Regulation and legal aspects / policy framework conditions]**

How do you think regulatory and legal aspects have impacted on the implementation of your project? Have you thought about the potential liability or accountability implications for your project? Did you consult lawyers, for instance, to look into these potential issues?

**SQ5.1 [Market forces / competition]**

How competitive is the environment in which your project operates? How do you think it affected the progress of your project?

**Q6. [Security, privacy and resilience]**

How well does your business plan reflect the potential security issues that may arise as a result of the 'connective' nature of your project?

**SQ6.1 [Security risk management and mitigation strategy]**

Have you had advice on countering cyber-risk associated with your project? Does your project have a security risk strategy in place?

**SQ6.2 [Privacy implications for citizens and/or users]**

Does your project take into account the privacy concerns of citizens/users and try to resolve them? If so, what strategies do you use?

Have you thought about the potential ethical implications of creating these new forms of interaction with (e.g. human-machine) and between (e.g. machine-machine) 'smart' devices?

**SQ6.3 [Personal data governance]**

Does your project have a 'data governance' framework that would enable consumers to transparently authorise the conditions under which data is used and shared with others?

What kinds of data curation mechanisms are in place to ensure data quality (and inter- operability)?

From the perspective of social acceptance, have you taken into consideration the levels of 'anonymisation', 'and 'opt-outs' that would need to be permitted?

**Q7. [Setting future ambitions]**

Looking forward 3-5 years, where do you see your project in the future?

**SQ7.1 [Business sustainability]**

What would need to be the minimum level of uptake to make the project sustainable (for example, in terms of deployment)?

When will your project become cash positive?

What do you see as being some of the main opportunities you see for your company (e.g. in relation to the wider IoT environment in the country)?

**SQ7.2 ['Future-proofing']**

What are you doing in terms of future-proofing the system? [How are you addressing issues like the potential obsolescence of, for example, core infrastructure?]

**Q8. [Perceived challenges]**

What factors and/or events do you anticipate could hinder your ambitions for the future?

**Q9. [Citizen Involvement and consumer privacy implications]**

How do you intend to involve citizens/users of technology as the project goes forward? If so, what will be the nature of this involvement?

**SQ9.1 Personal data use awareness**

Are you planning to do anything around raising user awareness on how their (personal) data is being collected and used to deliver services and benefits?

**Q10. [Governmental support to enable projects to scale up]**

What would be the three most important things that central and/or local government could do for the project to meet your future ambitions?

**SQ10.1 Scope of governmental support and involvement of other stakeholders**

Looking to the future, in addition to Government support, are there other key stakeholders that would benefit the project?

**SQ10.2 Policy mix for a robust Internet of Things**

What mix of technological, legal and regulatory (and user...) interventions are needed to support the development of a robust and sustainable 'IoT future' (with particular regard to your project)?

**Wrap-up**

B1. On reflection, is there anything you would do differently with the benefit of hindsight?

B2. Is there anything else you would like to add that we have not yet discussed?

B3. Are there any other individuals connected to the project that you think we should be speaking to?



## Appendix C: List of case study interviewees

We would like to acknowledge the contributions made by the following individuals, who kindly supported the study by allowing us to interview them in connection with the different case studies.

**Table 7: List of case study interviewees**

Case study	Interviewee
Opening a city: An R&D testbed in Bristol that can be used for city scale trials	Paul Wilson, Managing Director, Bristol Is Open
Opening a city: An R&D testbed in Bristol that can be used for city scale trials	Dimitra Simeonidou, CTO, Bristol Is Open, and Professor of High Performance Networks, University of Bristol
Farm herd sensing: Connecting farmers to their herds through sensors	Ivan Andanovic, CTO and Director, Silent Herdsman, and Professor of Broadband Networks, University of Strathclyde
Smart parking in Westminster: Smart parking made open for the community	Simon Morgan, Change Officer (Parking), City Management & Communities, Westminster City Council
Smart parking in Westminster: Smart parking made open for the community	Lewis Johnson, Head of Technology EMEA, Smart Parking Technology
Connected lighting on the South Coast: Smart street lighting controlled through a central platform	Richard Sims, Business Manager, Connected Devices, The Technology Partnership
Advancing telehealth in the North East: Benefitting patients and families with simple telehealth solutions	Paul Marriott, AHSN NENC Telehealth Programme Lead, and TECS Lead Consultant NHS England Strategic Clinical Networks
Advancing telehealth in the North East: Benefitting patients and families with simple telehealth solutions	Bryn Sage, CEO, Inhealthcare Richard Quine, Product Director, Inhealthcare
Advancing telehealth in the North East: Benefitting patients and families with simple telehealth solutions	Keith Chessell, CEO, Solcom
London City Airport demonstrator: Creating a connected retail space	Dan Byles, Vice President of Corporate Development, Living PlanIT
Breathe Heathrow: Using open data to help the public understand air quality and noise impacts	Yodit Stanton, CEO and Founder, OpenSensors.io
Smart bins as a service: 'BigBelly' solar powered bins come to Nottingham	John Marsh, Locality Manager (Neighbourhood Services Directorate), Nottingham City Council
Travelling in the North East: The 'Pop Card' smart ticketing and payment platform	David Bartlett, Corporate Manager for Business Change and Technology, Nexus





## Appendix D: Survey protocol for Professional and Chartered members of BCS, The Chartered Institute for IT

This survey is part of a broader policy research study to inform the direction and policy for the development of Internet of Things in the UK. The study is being conducted by RAND Europe, a not-for-profit policy research institute, on behalf of BCS, The Chartered Institute for IT and the recently launched IoTUK programme. By taking part in this survey, your views will be helping to inform IoT policy in the UK. The findings from the study will be published in a report in March 2016.

This survey is being conducted according to the [Market Research Society Code of Conduct](#)

If you would like this survey in an alternative format please contact [customer.insight@hq.bcs.org.uk](mailto:customer.insight@hq.bcs.org.uk). Thank you for your help.

[View BCS Privacy Policy](#)

Please tell us about your general perception and understanding of the Internet of Things.

**Q1 Which of the following do you agree represent examples of Internet of Things applications?**  
(Please tick all that apply)

- Smart home devices (e.g. smart meters, thermostats, security cameras)
- Personal wearable devices (e.g. health and fitness tracking devices)
- City-wide smart public infrastructure (e.g. smart street lights, smart parking, smart bins)
- Digitally collecting and accessing personal medical information (e.g. via a smartphone)
- Smart manufacturing systems (e.g. supply chain active tracking, connected quality inspection devices)
- Monitoring and controlling infrastructure operations (e.g. railway tracks, bridges)
- Smart retailing (e.g. proximity-based advertisements)
- None of the above

**Q2 What do you consider to be the best example of an Internet of Things application? This does not have to be an example from question 1 (max. 200 characters).**

---



---

**Q3** Which three of the following sectors do you think are most likely to benefit from the Internet of Things? *(Please select up to 3 answers only)*

- Healthcare
- Transport and logistics
- Manufacturing
- Agriculture and food
- Energy and environment
- Local government services
- Retail
- Home
- Other (please specify below - max. 150 characters)
- None of the above

---

---

**Q4** What do you think are the three most important benefits of the Internet of Things? *(Please select up to 3 answers only)*

- Improved efficiencies for organisations
- Enhanced customer experience
- Lowered costs
- Improved productivity
- Driving innovation
- Increased environmental sustainability (e.g. smart lighting)
- Other (please specify below - max. 200 characters)
- There are no benefits. The IoT is just hype.

---

---

**Q5 From your own experience, how concerned are you about the following barriers to the wider adoption of the Internet of Things?**

	Very concerned	Quite concerned	Not very concerned	Not at all concerned	I don't know
Lack of common standards to allow communication between devices and information systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Incompatibility with legacy equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Inadequate funding support for early-stage product ideas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Uncertain return on investment for organisations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High costs of investment required for IoT infrastructure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor perceived value of IoT by consumers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security vulnerabilities from increased connectivity between devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Privacy concerns from the sharing of personal data with third parties	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of sufficient technical and / or commercial skills	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please tell us about your perceptions of the security, privacy and data sharing aspects of the IoT.

**Q6 Which one of the following statements regarding Internet of Things security do you agree with most? (Please tick one box only)**

- The IoT will worsen existing security concerns
- IoT security will be an extension of the same security concerns that exist today
- The IoT will make the physical world more secure
- None of the above

**Q7 What do you think are the three most likely security threats to be associated with the Internet of Things? (Please select up to 3 answers only)**

- Misuse of personal data
- Integrity of business networks or systems
- Unsupported or obsolete products
- Reputational impact of poor security practices
- Intellectual property theft
- Impact on critical national infrastructure
- Other (please specify below - max. 200 characters)
- None of the above

---



**Q11** What do you think should be the three most important priorities for the government to stimulate the IoT landscape in the UK? *(Please select up to 3 answers only)*

- Ensuring interoperability (e.g. common standards)
- Providing high-risk funding support for technology development (e.g. with capital funds)
- Helping businesses to enter the consumer market with non-financial support (e.g. incubators)
- Public authorities creating new business opportunities (e.g. through local / NHS procurement)
- Investing in people (e.g. skills, training, education)
- Fostering multi-stakeholder collaborations (e.g. between industry, university and government)
- Promoting knowledge sharing (e.g. between different stakeholders and businesses in particular)
- Other (please specify below - max. 300 characters)
- None of the above

---



---

Finally, please tell us about your experience with the Internet of Things.

**Q12** Which of the following best describes your affiliation / organisation?

- Business / industry
- University / research
- Government / public sector
- Other (please specify below - max. 50 characters)

---



---

**Q13** Which, if any, of the following choices best reflects your personal or professional experience with the Internet of Things? *(Please tick all that apply)*

- End user / consumer
- Researcher
- Technological developer (software / hardware)
- Commercial / business support
- I have no experience with the Internet of Things
- Other (please specify below - max. 100 characters)

---



---

**Q14** Please rate your level of understanding of the Internet of Things from 1 (very low) to 5 (expert)?

- 1 - very low
- 2
- 3
- 4
- 5 - expert

Thank you for your time. We appreciate your opinion.

## Appendix E: Rapid policy review: Actions of the UK government related to the IoT

Table 8 provides an overview of publicly available information regarding policy actions of the UK government (departments and executive non-departmental public bodies) explicitly related to the IoT from 2011 until present. We note that, due to the wide-ranging and cross-cutting nature of the IoT, this rapid review may not be an exhaustive list of government activity and policy in the areas indirectly related to IoT (e.g. it does not cover the policy actions related to autonomous vehicles). In addition, this review lists only the publicly released information and does not include the internal actions or activities of working groups in the UK government. The clickable links (in the 'Action' column of Table 8) direct to official documents and/or websites (as of 11 March 2016).

**Table 8: Actions of the UK government related to the IoT over the past five years**

Time frame	Type of action	Action	Agency responsible	Summary of action
2015 – present (2018)	Policy strategy	Digital Economy Strategy 2015–2018	Innovate UK	The UK government's digital economy strategy 2015–2018 shows how the government will spend £30m a year over the next 4 years to support innovative business projects in this digital area, including the IoT, and to provide core funding for the Digital Catapult centre, the Open Data Institute and Tech City UK.
2015 – present (2018)	Support instrument and funding support	IoTUK national programme	Department for Culture, Media & Sport (DCMS) (funder); Digital Catapult and Future Cities Catapult (delivery)	An integrated £32m, three-year, government programme that seeks to advance the UK's global leadership in IoT and increase the adoption of high-quality IoT technologies and services throughout businesses and the public sector.
		Including: NHS Innovation 'Test Beds'	NHS England	Announcement of first wave of NHS Test Beds, including two Internet of Things 'test beds' in the area of diabetes and dementia.
		PETRAS Internet of Things Research Hub – part of the IoTUK programme	Engineering and Physical Sciences Research Council (EPSRC)	Investment up to £9.8m over three years, from EPSRC, to support a small number of leading UK universities working coherently together as a single internationally recognised PETRAS consortium to explore critical issues in privacy, ethics, trust, reliability, acceptability and security.
		Internet of Things CityVerve Project in Manchester – part of the IoTUK programme	DCMS	Investment of £10m in Manchester for a single collaborative research and development project to demonstrate the capability of the IoT in a city region.

Time frame	Type of action	Action	Agency responsible	Summary of action
2015 – present	Funding support	Security for IoT funding	Centre for Defence Enterprise (CDE)	Funding of up to £2m is available for research projects that identify new technologies or approaches to meet security challenges associated with the IoT.
2015 – present	Funding support	R&D funding support towards R&D in protecting data in industry	Innovate UK	Investment of up to £4m in collaborative research and development (R&D) projects that 'tackle the growing risks of disruption to Internet-enabled businesses and their digital supply chains'.
2015 – present	Funding support	Launch of HyperCatCity Smart City Initiative	Innovate UK	Builds on the Hypercat investment from Innovate UK bringing together three cities (London, Bristol and Milton Keynes) and businesses in order to 'create common, secure standards and protocols to unlock the potential of the Internet of Things'.
2014 – present	Funding support	Hypercat consortium	Innovate UK	An Innovate UK-backed consortium and standard aimed at 'driving secure and interoperable IoT for industry'.
2015	Policy strategy	<i>The National Information Infrastructure (NII): Why, What and How</i>	Open Data User Group UK	The connectivity issues related to the IoT were considered in the National Information Infrastructure document.
2015	Public consultation	<i>The commercial use of consumer data: Report on the CMA's call for information</i>	Competition & Markets Authority (CMA)	The report summarises the CMA's fact-finding exercise to 'increase knowledge of and understanding about the use of consumer data in the UK economy'. It explored the data issues related to the IoT as one of the key areas in relation to 'the collection and use of consumer data, including how it may develop in the coming years'.
2015	Policy strategy	<i>The digital communications infrastructure strategy</i>	DCMS and HM Treasury	This strategy aimed at 'supporting the UK's digital communications infrastructure' discussed the broadband and digital communications infrastructure required to harness the opportunities from IoT. It also set out a number of recommendations specific to IoT.
2015	Policy priority / Announcement	<i>Collaborative Research Priorities for the Environmental Agency 2015–2019</i>	Environment Agency	The Environment Agency sets a priority to address the proposals related to the Internet of Things and environmental issues.
2015	Policy research and analysis	<i>National Strategic Assessment of Serious and Organised Crime 2015</i>	National Crime Agency	The IoT, particularly the ongoing rollout of IPv6 addresses, is considered in relation to criminal use of Internet technology in the National Strategic Assessment of Serious and Organised Crime 2015.
2015	Policy research and analysis	<i>Internet of Things and the protection of national infrastructure</i>	Centre for the Protection of National Infrastructure (CPNI) and CESG	This document discusses the implications of IoT and M2M communications in the context of the UK national infrastructure. It was conducted by QinetiQ and commissioned by CPNI with CESG in order to 'inform and to inspire a diverse audience working mainly within the UK national infrastructure'.
2014 –2015	Public consultation	<i>Promoting Investment and Innovation in the Internet of Things</i>	Ofcom	Following the Ofcom consultation with stakeholders in 2014, Ofcom has identified several priority areas to help support the growth of the IoT, including spectrum availability, data privacy, network security and resilience, and network addresses.



Time frame	Type of action	Action	Agency responsible	Summary of action
2015	Policy research and analysis	<i>Common Cyber Attacks: Reducing the Impact</i>	GCHQ and CERT-UK	Common Cyber Attacks: Reducing The Impact has been produced by CESG (the Information Security Arm of GCHQ) with CERT-UK, and is aimed at all organisations that are vulnerable to attack from the Internet. The report aims to 'help CEOs, boards, business owners and managers to understand what a common cyber attack looks like'.
2015	Toolkit/ Guidance	<i>Internet of Things: Potential risks of crime and how to prevent it</i>	Home Office	In this guidance document, the Home Office provided 'general advice to the public and businesses about some of the potential crime risks posed by the Internet of Things and the steps they can take to avoid becoming a victim of crime.'
2015	Policy research and analysis	<i>Forward Look: Smart Metering-enabled Innovation in energy management in the non-domestic sector</i>	Department for Energy and Climate Change	This research document commissioned by the Department for Energy and Climate Change represents 'the technical forward look of anticipated innovation, and product and services development in energy supply and management solutions, enabled by smart/advanced metering in the non-domestic buildings sector, looking broadly at the period up to 2020'.
2014	Toolkit/ Guidance	Smart city standards and publications	BSI	A series of standards and publications to 'help address various issues for a city to become a smart city.'
2014	Policy strategy	<i>The UK Spectrum Strategy: Delivering the Best Value from Spectrum for the UK</i>	DCMS	The strategy sets out the UK's vision for use of spectrum 'to double its annual contribution to the economy by 2025 through offering business the access it needs to innovate and grow, and everyone in the UK the services they need to live their lives to the full.'
2014	Policy priority/ Announcement	Prime Minister David Cameron's speech to the CeBIT 2014 Trade Fair in Hannover, Germany	Prime Minister's Office	Invitation for collaboration on IoT R&D between industry in the UK and Germany. Announced additional funding for IoT research in the UK. Also announced review of IoT developments in the UK by Chief Scientific Adviser.
2014	Policy research and analysis	<i>Eight Great Technologies: The Internet of Things: A patent overview</i>	Intellectual Property Office	Identifying the IoT as one of the 'Eight Great Technologies' (plus a further two) which 'will propel the UK to future growth', the Intellectual Property Office produced an analysis of the worldwide patent landscape for the IoT.
2014	Policy research and analysis	<i>The Internet of Things: Making the most of the Second Digital Revolution: A report by the UK Government Chief Scientific Adviser</i>	Government Office for Science	The Blackett review, commissioned by the Prime Minister, explored 'the opportunities and risks of the Internet of Things for the UK and how the UK can exploit the potential of the Internet of Things'. It recommended 10 actions for government to maximise the opportunities and reduce the risks of these new technologies.
2013	Policy strategy	<i>Seizing the Data Opportunity: A Strategy for UK Data Capability</i>	HM Government	The policy document presents the vision and strategy to harness the UK's data capabilities, identifying the development of the Internet of Things as the key technological vehicle to open up new data opportunities.

Time frame	Type of action	Action	Agency responsible	Summary of action
2013	Policy strategy	<i>Spectrum Strategy 2013: Connectivity, Content and Consumers: Britain's Digital Platform for Growth</i>	DCMS	The Spectrum Strategy 2013 set out strategic priorities to establish the appropriate framework conditions for the development of the IoT with 'world-class connectivity throughout the UK', 'the production of world-beating innovative content and services that originate in the UK, but that are in demand across the globe', ensuring 'consumer safety in an increasingly online world', and helping to 'keep the cost of living down by ensuring consumers have choice about the range of communications and media services available to them'.
2013 – 2015	Policy strategy	<i>Information Economy Strategy</i>	BIS	This strategy document (developed in partnership by government, industry and academia) sets out a plan for government and industry to continue to work together to promote the success of the UK information economy sector.
2012 – present	Funding support	Future Cities demonstrator programme	TSB (Technology Strategy Board, now known as Innovate UK)	The competition, launched in 2012, supported 29 cities across the UK with £50k funding to carry out a feasibility study to demonstrate how integrated city systems (including smart urban logistics, energy and business models) could improve the performance of their city. Since then it has strategically invested £33m in future cities demonstrators across Glasgow (£24m), London (£3m), Bristol (£3m) and Peterborough (£3m).
2012 – 2014	Funding support	Internet of Things Ecosystem demonstrators	TSB (now Innovate UK)	TSB invested £4m in an 'ecosystem demonstrator' competition try to 'stimulate development of an open application and services ecosystem in the Internet of Things'. TSB funded 8 business-led demonstrator projects, launched in 2013 and completed in 2014.
2011 – 2014	Support mechanism	Internet of Things Special Interest Group	TSB (now Innovate UK)	In mid-2011, TSB established a special interest group aimed at building and engaging a UK community of innovators and researchers in the IoT. The aim of the group was to take a more concerted and interdisciplinary approach to fundamental research issues in the IoT.
2011 – 2012	Funding support	Internet of Things Convergence preparatory studies	TSB (now Innovate UK)	In October 2011, the Technology Strategy Board launched a competition to fund 10 preparatory studies to develop scenarios and strategies designed to understand more clearly the route towards an open application and services marketplace for the Internet of Things. The studies ended with a showcase and dissemination event in June 2012.

## Appendix F: Relationship between the findings from the case studies and the survey, and the proposed topics for discussion by the policy community

**Table 9: Relationship between the key findings from the case studies and the proposed priority topics for discussion by the policy community**

		Priority policy topics for consideration						
		The need to focus on non-technical factors that drive adoption	The need for knowledge from previous IoT projects to be shared, helping researchers and businesses avoid reinventing the wheel	The opportunities to use IoT technologies in the delivery of public services and to help spur greater market demand	Sustaining structural change and benefit through interoperability and information sharing across applications	Supporting the use of integrated IoT infrastructure across sectoral boundaries to help scalability of individual technologies	Supporting a trusted, people-centric IoT ecosystem	Addressing concerns about the risks of IoT technologies to critical national infrastructure
Findings from the case studies of IoT implementations	Non-technical factors are critical to developing and adopting the IoT.	✓					✓	
	The challenges in developing the IoT market and accelerating its growth are immense, with market uptake and business model-related factors highlighted as the foremost issues.	✓	✓		✓			
	Demonstrating sustainable business models with a solid return on investment is critical in order to progress the IoT market.		✓	✓				
	The public sector as a strategic purchaser could accelerate the uptake of IoT technologies, though in order to do so it will need to ensure that the SMEs leading IoT markets are assessed appropriately in procurement processes.			✓				
	Creating both trust and confidence in the security of data and processes enabled by the IoT is not always aligned with businesses' objectives to innovate and deliver value.					✓	✓	✓
	Clear, unambiguous and standardised processes for personal data governance are considered to be pre-requisites for linking up systems and for making them interoperable and trustworthy.					✓		
	IoT innovators' perceptions are mixed over the ability and level of impact of public policy to drive and accelerate the IoT market.	✓				✓	✓	

**Table 10: Relationship between the key findings from the survey and the proposed priority topics for discussion by the policy community**

		Priority policy topics for consideration						
		The need to focus on non-technical factors that drive adoption	The need for knowledge from previous IoT projects to be shared, helping researchers and businesses avoid reinventing the wheel	The opportunities to use IoT technologies in the delivery of public services and to help spur greater market demand	Sustaining structural change and benefit through interoperability and information sharing across applications	Supporting the use of integrated IoT infrastructure across sectoral boundaries to help scalability of individual technologies	Supporting a trusted, people-centric IoT ecosystem	Addressing concerns about the risks of IoT technologies to critical national infrastructure
Findings from the survey of informed users of technology	IoT applications are perceived to range across both consumer and industrial applications, with transport and logistics, energy and environment, home, and healthcare viewed as the most likely sectors to benefit from the IoT.			✓				
	Increased environmental sustainability and improved efficiencies for organisations are seen to be the most significant benefits of the IoT.				✓	✓		
	Security vulnerabilities and privacy concerns are overwhelmingly perceived to be the most important barriers to the wider adoption of the IoT.						✓	✓
	The IoT is perceived to exacerbate existing security challenges. The misuse of personal data and undermining of the integrity of business networks are seen to be the most likely security challenges associated with the IoT.					✓		✓
	Privacy vulnerabilities pose a significant concern to users of IoT applications. More transparency among organisations collecting and using data, as well as increased user control and digital literacy, are perceived as key priorities to enable trust and confidence in data sharing and governance.						✓	
	From the user perspective, government could play a stronger role in growing the IoT but should put citizens at the centre of its efforts. The priorities for support are seen to be in ensuring interoperability, investing in people, and fostering multi-stakeholder collaborations, and less so in creating new business opportunities through public spending.	✓	✓		✓	✓	✓	