This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

Europe's policy options for a dynamic and trustworthy development of the Internet of Things

SMART 2012/0053

Helen Rebecca Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Jean Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge, Hans Graux

RAND EUROPE

RAND EUROPE

Europe's policy options for a dynamic and trustworthy development of the Internet of Things

SMART 2012/0053

Helen Rebecca Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Jean Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge, Hans Graux

Prepared for European Commission, DG Communications Networks, Content and Technology (CONNECT)

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

RAND Europe is an independent, not-for-profit policy research organisation that aims to improve policy and decisionmaking in the public interest through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

RAND OFFICES
SANTA MONICA, CA • WASHINGTON, DC
PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA
DOHA, QA • CAMBRIDGE, UK • BRUSSELS, BE
www.rand.org • www.rand.org/randeurope

Preface

This document provides the final report (D7) for a study aiming to assist the European Commission in devising a European policy approach to foster a dynamic and trustworthy development of the Internet of Things (IoT), which contributes to addressing Europe's key societal challenges.

The target audience of this report consists of stakeholders in the IoT and IoT-affected policy domains and sectors.

The study has been conducted by RAND Europe, in collaboration with Simon Forge (SCF Associates Ltd), Maarten Botterman (GNKS Consult), and Hans Graux (time.lex). For more information about RAND Europe and this document, please contact Helen Rebecca Schindler at:

RAND Europe Cambridge Ltd
Westbrook Centre
Milton Road, Cambridge CB4 1YG
United Kingdom
Tel: +44 1223 353 329
www.rand.org/randeurope
E-mail:schindler@rand.org

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policy and decisionmaking in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, non-governmental organisations and firms with a need for rigorous, independent, multidisciplinary analysis. This report has been peer-reviewed in accordance with RAND's quality assurance standards.

Table of contents

Figures

Tables

Abbreviations

AIDC	Automatic Identification and Data Capture
APEC	Asia-Pacific Economic Cooperation
BLAST	Bursty, Lightweight Packets, Asynchronous Command-Response, Transitional
CAGE	Commercial and Government Entity
CEN	Comité Européen de Normalisation
CEPT	Conference of Postal and Telecommunications Administrations
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Competiveness and Innovation Programme
CR	Cognitive Radio
DC IoT	Dynamic Coalition on IoT
DNS	Domain Name System
DoDAAC	Department of Defense Activity Address Code
DSSS	Direct Sequence Spread Spectrum
EC	European Commission
ECO	European Communications Office
EDI	Electronic Data Interchange
EDIFICE	The Global Network for B2B Integration in High Tech Industries
ENISA	European Network and Information Security Agency
EPC	Electronic Product Code
EPRI	Electric Power Research Institute
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission (US)
FEDMA	Federation of European Direct and interactive Marketing Associations
FHSS	Frequency-Hopping Spread Spectrum

FI-PPP	Future Internet Public–Private Partnership
FTC	Federal Trade Commission (US)
GDP	Gross Domestic Product
GS1	Global Standards One
GSMA	Groupe Speciale Mobile Association
GTIN	Global Trade Item Number
HTTP	HyperText Markup Language
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IMSI	International Mobile Subscriber Identity
INCITS	InterNational Committee for Information Technology Standards
IoE	Internet of Everything
IoT-A	IoT-Architecture Project
IPR	Intellectual Property Rights
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
ITRs	International Telecommunication Regulations
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Sector
kbps	Kilobits Per Second
LTE	Long-Term Evolution
M2M	Machine to Machine
M3N	Metropolitan Mesh Machine Network
MAC	Medium Access Control
MNO	Mobile Network Operator
NCAGE	NATO Commercial and Government Entity
NFC	Near Field Communication

NHS	National Health Service (UK)
NIC	National Intelligence Council (US)
NIST	National Institute of Standards and Technology (US)
NRA	National Regulatory Authorities
OASIS	Organization for the Advancement of Structured Information Standards
ODETTE	Organisation for Data Exchange by Tele Transmission in Europe
OECD	Organisation for Economic Cooperation and Development
ONS	Object Name Service
PCAST	Presidential Counsel of Advisors on Science and Technology
P3P	Platform for Privacy Preferences
PET	Privacy Enhancing Technology
PPP	Public–Private Partnership
R&I	Research and Innovation
R&TTE	Radio Equipment and Telecommunications Terminal Equipment
RDF	Resource Description Framework
RDI	Research, Development and Innovation
REFIT	Regulatory Fitness and Performance Programme
RSPG	Radio Spectrum Policy Group
RTD	Research and Technology Development
SAML	Security Assertion Markup Language
SECaaS	Security as a Service
SME	Small and Medium-Sized Enterprise
SRD	System Reference Document
TETRA	Terrestrial Trunked Radio
TFEU	Treaty on the Functioning of the European Union
TLD	Top-level Domain
TPLan	Test Purpose Language
ubicomp	Ubiquitous Computing
URI	Uniform Resource Indicator
UPC	Uniform Product Code
W3C	World Wide Web Consortium
WRC	World Radio Communication Conference
WRC-12	World Radio Communication Conference, 2012

WSD	White Space Devices
WSIS	World Summit on the Information Society

Abstract

The rapidly-developing Internet of Things (IoT) may challenge conventional business, market, policy and societal models. This report to the European Commission aims to inform a consistent European policy stance capable of fostering a dynamic and trustworthy IoT that meets these challenges.

The study addresses the following research question:

What can usefully be done to stimulate the development of the Internet of Things in a way that best supports Europe's policy objectives (societal impact and jobs through innovation), while respecting European values and regulations (with particular reference to ethics and data protection)?

The study builds on prior work including the six challenges (identification, privacy and data protection and security, architectures, ethics, standards and governance) identified by the European Commission's IoT Expert Group (2010-2012) and results from the 2012 public consultation on the IoT. The study was informed by a literature review, key informant interviews and an internal scenario workshop. Its findings and conclusions were extended and tested at an open stakeholder workshop. The analysis supports an initial soft law approach combining standards, monitoring, 'information remedies' and an ethical charter to facilitate IoT self-organisation and clarify the need for and nature of effective regulatory interventions.

Executive summary

The Internet of Things (IoT) is developing rapidly and may challenge conventional business, market, policy and societal models. In particular, the economic, socio-political, legal and technological governance of the internet is based on assumptions about rational choice, market forces and effective self-organisation that are most appropriate to human-controlled systems. The interacting autonomous systems of the IoT are already departing from this paradigm. This raises two complementary policy challenges: whether these departures raise any unique IoT-specific policy concerns, let alone specific problems in need of legal intervention or policy support; and whether the development of the IoT affects the rationale, impacts and/or available instruments for existing interventions ranging from regulation to development and deployment support.

A study to inform a consistent policy stance towards the IoT

This report commissioned by the European Commission aims to inform the development of a consistent European policy stance capable of fostering a dynamic and trustworthy IoT that helps meet key European challenges.

The study addresses the following research question:

What can usefully be done to stimulate the development of the Internet of Things in a way that best supports Europe's policy objectives (societal impact and jobs through innovation), while respecting European values and regulations (with particular reference to ethics and data protection)?

The study builds on European Commission work initiated in 2005, including policy discussions and recommendations including those of the European Commission's IoT Expert Group (2010-2012) in particular, the six challenges (identification, privacy and data protection and security, architectures, ethics, standards and governance) identified by that group. We also build on the results of the 2012 public consultation on the IoT conducted in the second quarter of 2012 (European Commission, 2013).

The study was informed by a literature review, key informant interviews, and a team-internal scenarios-based workshop. It also extended and tested its findings and conclusions at an open stakeholder workshop held on 30 April 2013 at the European Commission's premises in Brussels.

Results and findings

A helpful starting definition

Building on the definition given by the International Telecommunication Union (ITU), the study proposes the following definition of the IoT:

> The Internet of Things builds out from today's internet by creating a pervasive and self-organising network of connected, identifiable and addressable physical objects enabling application development in and across key vertical sectors through the use of embedded chips.[1]

The IoT presents issues across several domains

According to experts interviewed for this study, **the current development of the IoT may not be aligned with Europe's policy objectives. Part of this is due to the limited influence of European (government and industry) actors and it may not be possible to address the consequences once the IoT has matured.**

The socioeconomic impacts of the IoT are expected by many industry analysts to develop **rapidly over the next five to ten years into an important element of the European digital economy**. But it cannot be assumed that this growth will be coherent or manageable. Current trajectories suggest the emergence of multiple competing architectures and identification schemes, leading to potentially damaging **fragmentation** across and within sectors or the triumph of a **'second best'** candidate. This is **not simply a market phenomenon**; the governance of the internet involves standardisation, government policy and a measure of self-regulation, but the **institutions and decisions may lack accountability** and may not effectively balance competing interests.

In order for government, business and societal organisations to realise the potential of the IoT and meet its challenges, its application must be accepted and trusted – not universally, uncritically or unequivocally, but in a proportionate, reasoned and effective manner. This requires both accurate and comprehensible information and the operationalisation of ethical principles.

Some levels of the IoT value chain are likely to suffer classic market failure due to entry and exit barriers, natural monopolies, information asymmetries and externalities. This will not be true of all layers – the openness and interoperability on which the IoT business proposition rests should lower barriers in the device layer. But this, too, can be problematic, if effective use depends on continuing collaborative innovation by end users, application providers and other stakeholders, and if switching is easier than (investment in) adaptation.[2] The unreliability of unaided market forces can be seen, for example, in inadequate investment in security (externalities), the unreliability of consumer sovereignty (information asymmetry) and the barriers to innovation arising from inappropriate spectrum policy and fragmentary or closed standards.

State of play: the growing potential of the IoT

Section 1 examines the context in which the IoT is emerging. Despite its youth, **the IoT is seen as one of the fastest growing IT segments**. By 2020, upper estimates of its annual global economic potential[3] across all affected sectors range from $1.4 trillion to $14.4 trillion. Some of the most promising and intriguing opportunities come from the linkage of the IoT to other systems and technologies, such as clouds, smart grids, nanotechnology and robotics.

---

[1] Integrated circuits or microprocessors, commonly called 'chips'.

[2] This excess volatility (Katz and Shapiro, 1992) is characteristic of markets with network externalities and has been noted as well in the 'app economy' (Cave et al., 2012).

[3] Taking into account machine-to-machine (M2M) and Metropolitan Mesh Machine Network (M3N) applications.

Key issues: wide-ranging effects on competition and competitiveness

The potential economic implications of a rapidly developing IoT reflect the changing pattern of **horizontal and vertical** relations among the businesses that supply, use and serve the IoT. Of particular interest is the **competitive tension** between large market players from these other sectors, and the potential for a more open environment for small and medium-sized enterprises (SMEs) and innovative entrants within and beyond the IoT. In particular, because the 'things' of the IoT act autonomously and as part of a densely linked ecosystem, sole control of the IoT cannot be assumed to lie with the owners of devices or with providers of essential infrastructure services.

As in other emerging technology domains, European competitiveness can be enhanced by exploiting **the strength of its research capabilities**, reinforced by **antitrust**, **public procurement and international trade initiatives**. More specifically, businesses and other IoT users can benefit from the embedding of existing European **standards of consumer and data protection**, which may become a unique source of competitive advantage in marketing European IoT technologies and services worldwide.

But this depends on the availability and structure of **investment**. China has already earmarked €625m for IoT investment. Public and private sector investors will have the possibility to provide infrastructure and application funding for the IoT including private financing, public investment, public–private partnerships, and social (eg crowd-funded) finance.

Building an ethical IoT

The commercial and technical development and broader socioeconomic impacts of any information and communications technology (ICT) derive from the way it deals with the ethical tensions arising from the way it connects people and organisations with different objectives. The IoT creates new forms of contact that make it hard for those currently charged with responsibilities to know, understand and control these connections; the classical protections of negotiation, markets and contracts may not work as well for human-to-machine, let alone M2M contacts. Having investigated these ethical issues, especially in relation to **privacy**, **autonomy**, **trust**, **identity and social inclusion**, we note that without greater attention to improving individual understanding and awareness, solutions, even if implemented, might not survive.

Architecture, security and identification

The challenges of the IoT architecture, identification and security are examined in more depth in Section 4. Architecture, in particular, must provide a set of common rules to keep systems close enough to allow interoperability and thus facilitate efficient emergence of better systems, while allowing enough flexibility to encourage innovation.

Current development is producing substantial heterogeneity of applications, environments and systems but not (seamless) interoperability. The resulting technical and cost issues across sectors make it likely that a range of specialist **architectures** will emerge that can lock in this weakness.

The same fragmentation risk affects naming and addressing norms; differences across geographical areas and industries can limit interoperability and competition.

Much of this fragmentation can be overcome by suitable open standards. Many of the applicable standards are inherited from other areas (eg radio communication, general ICT); there is thus an ongoing

debate over the necessity for IoT-specific standards and the role of specific standards bodies. Several specific initiatives have been created to incorporate and adapt existing standards and to complete the IoT portfolio with additional standards. However, at this early stage of development, it is not clear how uniformly standards are applied or enforced, nor have any preferable approaches been identified for application and enforcement.

The ubiquity of sensor (and eventually actuator) networks poses some unique and interesting questions with respect to security as a public good and whether **cyber security** is subject to market failure as well as adding novel aspects to pre-existent privacy and security risks. The IoT could also result in cyber-attacks targeting new endpoints, such as smart homes, therefore requiring strategies that can be efficient across multiple domains and competing priorities.

Strategic objectives of European IoT governance

The study considered the case for action **at Community level and found arguments for its necessity and European added value**. Section 6 identifies the general objectives of such action. These include **accountability, safety and interoperability of an inclusive, ethical and open IoT**, characterised by **effective and efficient competition and competitiveness**.

Potential gaps in the existing legal framework

As an extension to the internet, the IoT is affected by internet governance structures. But the internet itself does not 'fit' neatly within all the relevant governance frameworks (telecom, competition, privacy, consumer protection and so on), Its problems are not always effectively addressed by extensions of these frameworks. And that extension may in turn weaken the effectiveness of existing competition and other rules. The IoT poses its own unique challenges and also involves additional reverence governance domains (eg safety, transportation) more centrally than the internet does. Section 7 examines relevant areas of EU law and identifies gaps that could hamper the realisation of the strategic objectives of IoT policymaking.

In particular, the frameworks for **competition** (in particular market definitions and the role of competition authorities), **privacy and data protection** (in particular regarding liability and responsibility), **universal service** and **cyber security** are likely to require adjustment or compensating 'soft law' measures.

Policy options

The formulation of concrete and specific policy options is possibly premature and went beyond the scope of the present study. In Section 8 we analyse three options for a broad policy approach and some tools for their operationalisation, which are summarised in Table 0.1.

Table 0.1 Summary of broad policy options

Option	EC activity	Efficiency	Efficacy
No action	Current trajectories continue	No guarantee for development in accordance with EU objectives	Market players retain complete freedom
Soft law	Using monitoring, innovation policy, industrial policy	If sufficient incentives for adoption and uptake exist, high effectiveness is possible, while incentivising coherence with EU policy objectives	Market players retain some freedom in deciding the most effective manner of complying with requirements
Hard law	Harmonisation and enforcement in IoT-related areas (e-commerce, data protection etc)	Depending on enforcement, mandatory compliance can be highly efficient	Negative externalities are hard to foresee given the early stage of technology development, therefore are difficult to avoid in legislation

Policy recommendations

Comparison of the effectiveness, efficiency and coherence of these high-level policy stances supports the soft law option at least in the near term as the best way to **create space** for IoT development, **accelerate or improve the development of the IoT market** and make progress in meeting the challenges. The details are developed as a set of recommendations in Section 9.

Our recommendations include a central role for the European Commission in **coordinating policy dialogue** to ensure common understanding and coherent effective action across sectors, regions and policy areas; support for **meaningful digital literacy programmes** and **awareness-raising** to empower self-regulation and improve individual interaction with the IoT; and support and promotion of **knowledge sharing**, **research and validation projects** with funding, **continuous debate and policy articulation** especially on identification, privacy and ethics in IoT environments. Although an **ethical charter** may be a useful component of self-regulation, support for the general approach is patchy. As an interim measure, **creating a European 'Ethical Tech' brand** could encourage innovators and providers to develop ethical technology in line with market and user needs.

Monitoring and implementation

The information necessary to track the development of the IoT is fragmented and difficult to use. This problem of too much, too little *and* the wrong kind of information may account for slow progress to date. Rapid changes – and the exaflood of data – are expected to continue. In order to develop and implement appropriate flexible and future-proof policy this problem must be overcome. In this regard, it is fortunate

that the various governance domains that affect and are affected by the IoT each collect and analyse information. This creates the basis for a coordinated policy approach allied to an articulated information structure organised around the IoT. This **IoT observatory** could follow the impact of challenges in areas that cannot be directly measured, such as ethics, privacy and security, and should lead to more joined-up policy and deeper and more balanced understanding; the sharing of information and co-creation of data resources for monitoring and evaluation will also create shared understanding and help to break down organisational stovepipes. This is not limited to past and present information: **the information should be used to create a rich set of shared scenarios for joint explorations of the emerging IoT**. As always, **it is important to establish measure-specific indicators that underpin a monitoring strategy** (in conjunction with DG CONNECT's 'Metrics' initiative).

Acknowledgements

The authors would like to acknowledge the support and critical contributions from the experts who participated in our interviews and/or workshops:

Benoit Abeloos (European Commission); Kristina Aleksandrova (ANEC); Eric Barbry (Alan Bensoussan Avocates); Alessandro Bassi (Bassi Consulting); Souheil Ben Yacoub (Verisign); Rudolf van den Berg (OECD); Aileen Byrne (Transatlantic Council); Dan Caprio (McKenna Long & Aldridge LLP); Prof. Brian Collins (UCL Centre of Engineering policy); Marc de Colvenaer (Flemish Living Lab Platform); Alain Dechamps (Comité Européen de Normalisation; CEN); Ralph Droms (IETF); Rodolphe Frugès (Sigfox); Kathleen Gabriels (Vrije Universiteit Brussel); Eric Gaudillat (European Commission); Patrick Guillemin (ETSI); Mark Harrison (University of Cambridge); Ayesha Hassan (International Chamber of Commerce); Prof. Mireille Hildebrandt (University of Nijmegen); Prof. Jeroen van den Hoven (TU Delft); Prof. Sotiris Ioannidis (Foundation for Research and Technology); Dr Stig Johnsen (SINTEF); Olaf Kolkman (NL net labs); Tobias Kowatsch (Institute of Technology Management, St Gallen); Rob van Kranenburg (Waag Fellow); Christopher Kuner (Hunton and Williams); Philippe Lefebvre (European Commission); Christoph Luykx (Intel); Massimiliano Minisci (GS1); Ludovic le Moan (Sigfox); Gerrit Muller (Embedded Systems Institute); Finn Myrstad (BEUC); Stephen Pattison (ARM Holdings); Isabelle Roccia (US Mission to EU); Kostas Rossoglou (BEUC); George Roussos (Birkbeck, University of London); Rogelio Segovia (European Commission); Marc Sel (PriceWaterhouseCoopers); Prof. Berndt Carsten Stahl (De Montfort University); Mark Townsley (IETF); Prof. Guido van Steendam (KU Leuven); Peter Walters (UK Department for Business, Innovation and Skills); Dr Rolf Weber (University of Zurich); Petra Wilson (CISCO); Tijman Wisman (University of Amsterdam).

We would like to thank Giuseppe Abbamonte, Head of Unit 'Trust and Security' at the European Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT); Olivier Bringer, lead project officer and his colleagues Florent Frederix (former Head of RFID Sector); and Peter Friess for their mentorship, constructive approach and useful feedback.

Finally, we would also like to thank staff at the Danish Technology Institute (DTI) and Jeremy Millard for their administrative support, feedback and guidance.

Introduction

The Internet of Things (IoT) is developing rapidly and may challenge conventional business, market, policy and societal models. In particular, the economic, socio-political, legal and technological governance of the internet is based on assumptions about rational choice, market forces and effective self-organisation that are most appropriate to human-controlled systems. The interacting autonomous systems of the IoT are already departing from this paradigm. This raises two complementary policy challenges: whether these departures raise any unique IoT-specific policy concerns, let alone specific problems in need of legal intervention or policy support; and whether the development of the IoT affects the rationale, impacts and/or available instruments for existing interventions ranging from regulation to development and deployment support.[4]

Objectives and research questions

This report commissioned by the European Commission aims to inform the development of a consistent European policy stance capable of fostering a dynamic and trustworthy IoT that helps meet key European challenges. The study addresses the following research question:

What can usefully be done to stimulate the development of the Internet of Things in a way that best supports Europe's policy objectives (societal impact and jobs through innovation), while respecting European values and regulations (with particular reference to ethics and data protection)?

This question can be broken down into five sub-questions, which the report will aim to address in the following chapters:

1. *How can the IoT usefully be defined in order to understand its impacts and the potential of policy to improve them?*
2. *What are the significant (current and uncertain future) technological developments affecting the evolution of the IoT?*

[4] For example research and innovation policies and funding mechanisms such as Europe's Competitiveness and Innovation Programme and Future Internet Public Private Partnerships.

3. *How is the development of the IoT affecting societal outcomes, and what are the key uncertainties associated with this impact?*
4. *How will the development of the IoT (as a sector) be affected by market forces, and how will use of its services affect the economy more broadly?*
5. *How does the emergence of the IoT affect overarching European policy initiatives and the governance of the Internet?*

The study builds on European Commission work[5] initiated in 2005, including policy discussions and recommendations including those of the European Commission's IoT Expert Group (2010–2012) in particular, the six challenges (identification, privacy and data protection and security, architectures, ethics, standards and governance) identified by that group. We also build on the results of the 2012 public consultation on the IoT conducted in the second quarter of 2012 (European Commission, 2013).

While its relevance is very wide, we recognise that some of the issues are – at the moment at least – of specialised appeal. For this reason, we have attempted to draw out the broader and deeper implications of the IoT in a way that will allow experts in other domains to further develop and apply the analysis. This applies in particular to the question of policy.

Approach

We aimed to address the research questions by applying a mix of methodologies, including literature review, key informant interviews, and a team-internal scenarios-based workshop. It also extended and tested its findings and conclusions at an open stakeholder workshop[6] held on 30 April 2013 at the European Commission's premises in Brussels. The methodologies are explained in more detail in Annex.

Structure of the report

While the research questions contain many elements of a standard impact assessment, we fully recognise that this would be premature. In particular, it is not yet established that action is required and concrete objectives and policy options have yet to be developed. Nonetheless, in order to support such a discourse and eventual policy development (should it be warranted), we have structured the report along the general steps of an impact

[5] A more comprehensive overview of EU involvement and resulting policies can he found at http://ec.europa.eu/information_society/policy/rfid/eu_approach/index_en.htm.

[6] The workshop attracted European innovators and entrepreneurs and brought together a diverse set of stakeholders involved in the policy formation of the IoT: civil society and consumer representatives; industry stakeholders who provide, support and/or use IoT devices, applications and services; and academics. The workshop served as a means to validate and refine research findings, to explore their implications and policy options with the audience, and to obtain suggestions as to the road ahead for the European Commission and other interested stakeholders. Participants are listed in the acknowledgements, and the workshop methodology is described in Annex A.

assessment: state of play (Part I), description of policy issues (Part II), problem definition (Part III), policy objectives, policy options and their assessment (Part IV), proposal for action (Part V), and refer as much as possible to concrete issues pertaining to IoT developments and to concrete examples of IoT developments, current and planned. Annexes provide more technical background and offer further analysis and insights.

Part I – State of play – provides an assessment of the current situation. It proposes a working definition and provides the context, highlighting relevant technological, societal, economic and political developments.

Part II – Description of policy issues– introduces key issues[7] to inform the policy debate, namely market forces (Section 2), education and values (Section 3), architecture, identification, security and standards (Section 4).

Part III – Problem definition – derives a problem statement and clarifies needs from a key stakeholder perspective.

Part IV – Policy objectives, policy options and their assessment – presents the case for action and examines to what extent the current framework appears capable of addressing likely IoT challenges. It clarifies competences and policy objectives (Section 6), defines the normative framework and analyses gaps (Section 7), which then feed into a consideration of policy options presented in Section 8.

We will consider the differential impacts of the policy options as compared to the base case (Do Nothing) option whose impacts are analysed above. This assessment is essentially qualitative, for three reasons. First, the specific provisions and interventions likely to develop under either option will depend on political, market and technological developments that cannot be predicted. Second, the economic context – as regards the 'IoT sector', the sectors that use IoT-enabled services and the (European and global) macroeconomy remains deeply uncertain – the available data on IoT-related business prospects and their impacts reflect concepts of the IoT that have yet to solidify, which makes the commercial prospects (and the availability of capital) hard to forecast accurately. Finally, the policy actions that could arise under either option cover such a wide spectrum that any quantitative assessment would need to consider a confusing wealth of specific actions, deriving from an equally rich set of technical , economic and societal uncertainties. In consequence, the uncertainty attached to such assessments would likely overwhelm the ranking of options along any single criterion. Moreover, the high level policy objectives for the IoT in Europe as described in this report so far have not been defined in quantitative terms.

---

[7] *Key issues* reflect the policy needs of the client. *Key issues* have been have been identified and refined on the basis of a literature review and studied in close collaboration with experts (key informant interviews, internal (scenario) and external workshops).

Part V – Proposal for action – presents the proposal for action. It provides policy recommendations (Section 9) and defines an implementation and monitoring strategy (Section 10).

PART I State of play

1. Definition: IoT in context

The evolution towards the IoT holds the promise of making significant progress in addressing global and societal challenges, helping Europe to become a smart, sustainable and inclusive economy and thereby helping to 'reboot the EU economy and enable Europe's citizens and businesses to get the most out of digital technologies' (EUR-Lex, 2010).

However, IoT-driven 'smart' meters, grids, homes, cities and transportation systems also raise some important issues that will need to be considered and addressed. In this section, we will propose a working definition and present technological, societal, economic and political developments, defining the state-of-play.

1.1. A helpful starting definition

At the outset, it is important to acknowledge that there is no globally agreed definition of the IoT.

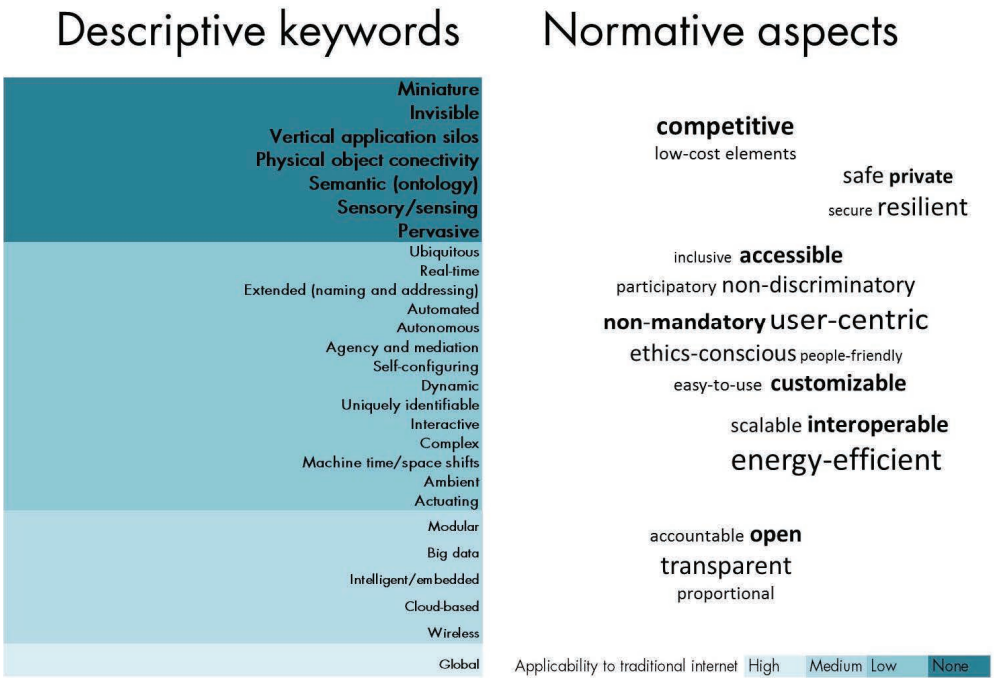
The ITU (2005) definition is widely accepted, yet very general:

> The Internet of Things is a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

This statement would remain accurate without the qualifier 'of Things'. Essentially, the IoT can be defined as a network of objects capable of detecting and communicating information between each other; but it also differs from the internet in several other aspects. To contribute to a working understanding of specificities of the IoT, Figure 1.1 presents a list of keywords clarifying the distinction between *descriptive* and *normative* aspects of the IoT and the fundamental elements that distinguish it from the internet.[8]

[8] The list of keywords shown in Figure 1.1 is the result of an internal scenarios-based workshop and has been further refined and validated by stakeholders at the final workshop held in Brussels on 30 April 2013. The list of descriptive keywords does not aim to be comprehensive but has been instrumental in the elaboration of the proposed definition of IoT and helps differentiate IoT from traditional internet. Normative aspects presented in the right hand column highlight policy terms and policy objectives, characterising what 'we' want the IoT to be; policy objectives are further detailed in Section 6.2.

Figure 1.1 Descriptive and normative aspects of the IoT



Building on the results of an expert workshop discussion of this list we propose the following definition of IoT:

> The Internet of Things builds out from today's internet by creating a pervasive and self-organising network of connected, identifiable and addressable physical objects enabling application development in and across key vertical sectors through the use of embedded chips,[9] sensors, actuators and low-cost miniaturisation.

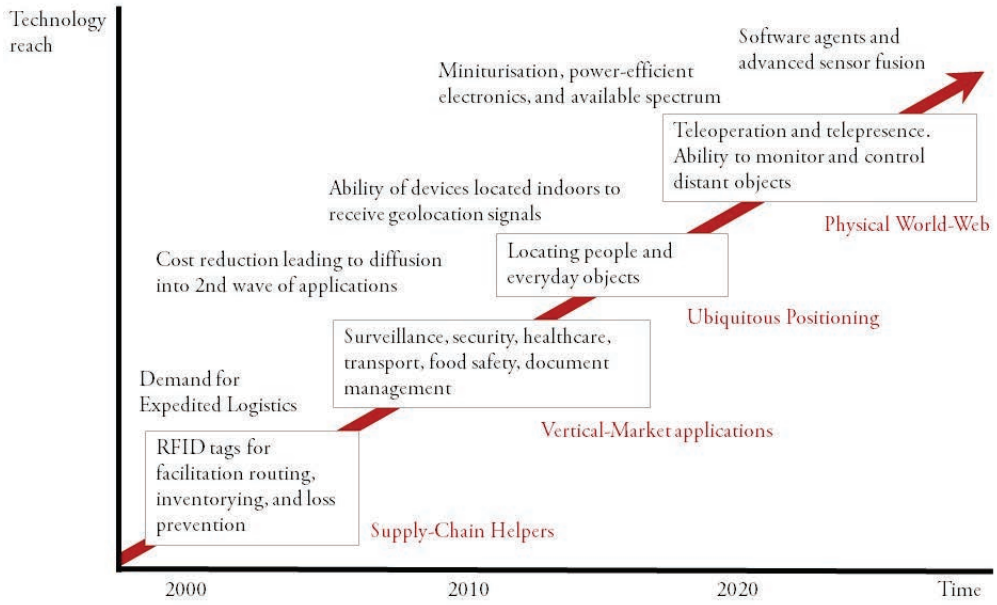
1.2. Technological developments

Increasing functionality of IoT technologies within and across sectors

The IoT is developing over time by way of coevolution, with technology, applications and stakeholders' understanding of the implications driving each other. Figure 1.2 illustrates how these dynamics have built on each other in the past and are projected to coevolve in the next decade.

[9] Integrated circuits or microprocessors, commonly called 'chips'.

Figure 1.2 A technology roadmap for the IoT



Source: adapted from SRI Business Consulting (2008)

By interconnecting and enhancing functionalities of physical objects, the IoT has the potential to affect every operational and product delivery process across the full range of economic activity. IoT sensors can collect data for storage, processing and analysis by companies, regulators and citizens using internal or external networks. This development is linked across the layers that the IoT shares with other 'internets' – technologies, networks, services and applications. Areas of application we see today include but are not limited to:

- industrial applications: intelligent manufacturing and supply enabled by machine-to-machine (M2M) applications in IoT and 'industrial internet'
- retail, logistics and product management, eg Radio Frequency Identification (RFID) tagging of goods, monitoring for conservation of perishables, sensors and actuators to track and control the use of products
- surveillance for safety and security, eg cameras and biometric readers
- smart cities, smart building and smart homes, eg illumination control, EV charging, emergency services, joining up 'intelligent buildings', home automation and ambient assisted living (AAL)[10]

[10] Gersch, Lindert and Hewing (2010) define AAL as assistant systems for the constitution of 'intelligent environments' with the aim to compensate predominantly age-related functional

- smart transportation, eg unmanned and self-driving vehicles
- smart health and public sector services, eg telemedicine
- smart grid infrastructure: energy saving, electricity and water management, network management and metering, renewable energies load balancing for the network environmental monitoring, eg monitoring of air quality.

Opportunities from linkages between IoT and wider systems: the Cloud, smart grids, nanotechnology and robotics

The most substantial benefits can be expected through three potential forms of linkage between the IoT and broader systems:

- the decentralisation and/or delegation of specific functions and decisions to IoT entities (things and subsystems of things)
- the collection, analysis and sharing of information by those entities
- the self-organisation of IoT devices into new configurations that can share the functions of deciding, acting and sensing in new ways as circumstances change.

These opportunities are well illustrated by the interaction of the IoT with developments such as cloud computing, smart grids, nanotechnology and robotics.

These are some of the connections between the cloud and the IoT:

- IoT sensors will produce unprecedented amounts of data, the collection, storage, combined processing and ubiquitous availability of which will become increasingly important. Cloud computing facilities are ideally suited to provide this, and thus to ensure that the benefits of the IoT are spread as widely as possible. The consequence is that new business and service models and new applications can be attained at lower cost.
- Cloud facilities can coordinate the collection of specific data appropriate to eg event monitoring and the detection of emerging problems by designing and implementing sensing strategies in a variety of IoT entities at various locations.
- Likewise, cloud-based computations can be used to instruct IoT devices to take actions in a coordinated and distributed manner.

---

limitations of different target groups through technological information and communication support in everyday life. At the same time they take charge of control and supervision services for an independent course of life.

- Cloud-based applications can be created and deployed to make use of sensor inputs (such apps have already been deployedeg, for example in health-related services and advice).
- Sharing of hardware resources (such as sensors) through the cloud however may raise policy concerns related in particular to privacy and continuity of service).

Similarly, the development of 'smart grid'[11] and smart meters will likely lead to a further expansion of the IoT (a network of sensors and actuators to make the smart grid work). Other mobile devices such as TomTom road navigation devices collect information on speed and location, and already provide this for traffic information applications. Likewise, nanotechnology and nano-electronics provide one of the key enabling technologies for highly innovative IoT applications such as 'smart dust', developed mainly for military use, 'ubiquitous miniature sensors' for detecting communication information with other machines and micro- or nano-scale RFID or other tags (connected through ZigBee, Bluetooth or wi-fi for instance), which could be integrated in products or even implanted within the human body.

Other technological developments potentially enabled by the IoT include robotics and unmanned or self-drive vehicles that benefit from the presence of networks of sensors in and around the object itself in enhancing their awareness (Kalra, Anderson and Wachs, 2009). More generally, these prospects include the potential for new systems and new forms of interactions within and among them.

1.3. Societal developments

As described above, IoT applications are likely to span across socioeconomic segments. At present, these applications have particular relevance in certain social developments posing challenges to European policymakers, such as that of an ageing society, persisting inequalities and changing attitudes to surveillance.

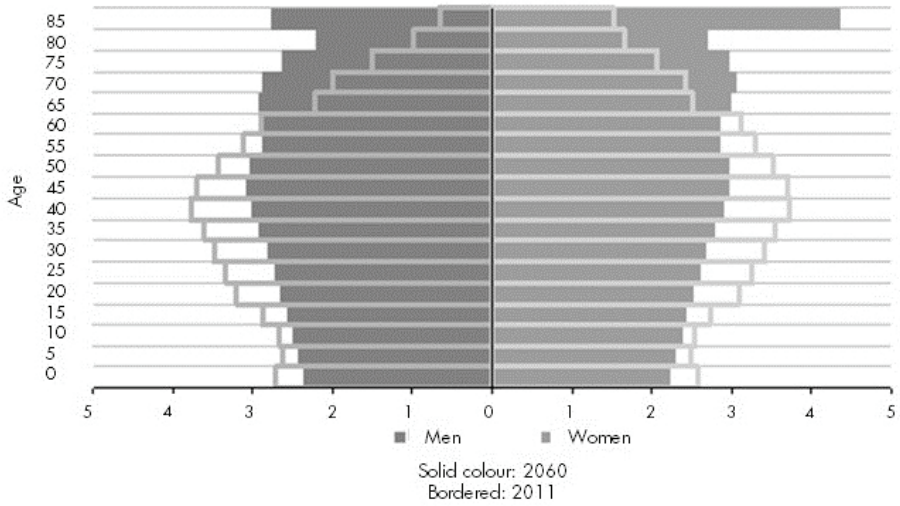
IoT for an ageing society

The challenges associated with an ageing population are particularly acute in Europe. The IoT is expected to offer solutions and services enabling us to increase the healthy life

[11] A smart grid is an electrical grid that uses information and communications technology to gather and act on information, such as about the behaviour of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics,and sustainability of the production and distribution of electricity. When this report was written (in early 2013) a public consultation was under way to inform a communication on energy technologies and innovation in Europe. A European Technology Platform SmartGrids was set up in 2005 to create a joint vision for the European networks of 2020 and beyond. Smart grids are also central to the societal goals addressed by the Digital Agenda for Europe Flagship Programme.

years and live more independent lives, even in the context of an economic downturn limiting public spending and a rapidly increasing old-age dependency ratio (illustrated by the age distribution within European society; see Figure 1.3). For instance, sustainable new care environments would require a greater proportion of care at home, made effective and affordable by IoT applications such as telemedicine and AAL.[12]

Figure 1.3 Age pyramid EU 25, 2011–2060



Source: Eurostat population data[13]

At the same time, IoT-enabled applications may increase the age range of economically productive life, both as suppliers of labour and as active consumers of goods and services. But at the moment, these have not been widely deployed or taken up; the result has been a series of further changes designed to cope with ageing as a collective problem (and a new business sector).

IoT for an inclusive society

Despite austerity, domotics (or home automation) are becoming rapidly taken up by markets, even if applications that allow people to adjust the heat at home remotely, or even to monitor rooms in their home via their smart phone, seem to grow faster than the famous 'self-ordering fridge', which people have been talking about for decades. Thus IoT development can be expected to contribute to improved lifestyles, provide solutions that can cater to the needs of a modern and connected society, and bring comfort,

[12] Within the European Union such issues are explicitly addressed by AAL activities fostered by the DG Connect Focus of AAL: delivering cost-effective health and social care in the future, and growth opportunity for European Business. See http://www.all-europe.eu.

[13] Data for 2011 are provisional. Data for 2060 are based on the EUROPOP2010 scenario; see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/en/proj_10c_esms.htm.

environmentally sound and cost-effective consumption within the reach of larger sections of society. However, in a context of growing inequalities within countries and the persistence of digital divides and social exclusion, it remains to be seen whether the development of an IoT will contribute to diminish or exacerbate these inequalities. In order to diminish inequalities, emphasis in development will need to be on low-cost, easy-to-use inclusive solutions that can communicate across low bandwidth facilities.

IoT, safety and the 'surveillance society'

The IoT enables several applications aimed at monitoring systems continuously in real time in order to anticipate and address potential problems or incidents. This development can apply to several levels of safety, from environmental monitoring and building management to national security and crime prevention, and can contribute to a safer society.

At the same time, as a combined result of enhanced concerns for security and new ways to exploit data concerning individual behaviour, many expert content that monitoring has become far more extensive and crowded out trust, while awareness, consent and control by those monitored have not kept pace.[14] The technological possibilities of the IoT are likely to further this trend. Beyond the security-related monitoring of individuals, a similar erosion of privacy boundaries can be seen in relation to other forms of behaviour linked to business offers, such as purchases, transportation and healthcare-related behaviours. The degree to which such trends are self-limiting (by provoking public resistance) or self-catalysing (by creating increased awareness of the danger posed by 'others' and progressive loss of trust) is, at present, uncertain.

1.4. Economic developments

The IoT is still in its early stages of development. It is seen as one of the fastest growing technology segments of the information technology sector in the next five to ten years, but projections on the future potential of the sector differ regarding their specific focus and the order of magnitude of the projections. In 2011, the M2M market was estimated to be worth $44 billion (about €34.3 billion) worldwide and (conservatively) projected to have a compound annual growth rate of 30 percent, growing to $290 billion (about €226.2 billion) by 2017 (Markets and Markets, 2012). An industry report expects benefits of industrial internet diffusion to have the potential of adding $10–15 trillion (about €7.8–11.7 trillion) to the world economy over the next 15 years (Evans and Annunziata, 2012).

[14] Further explored in Section 3 and Section 4.3 of this report, looking at ethics, privacy and security.

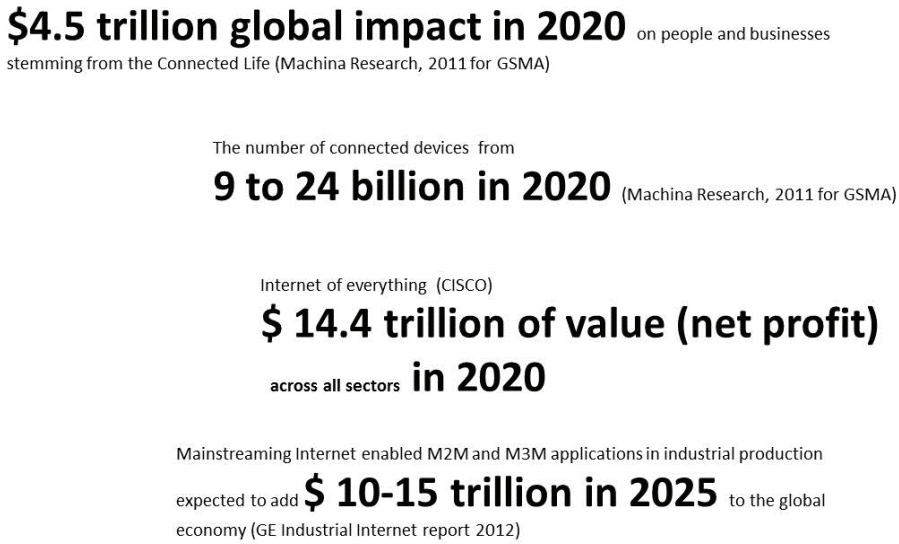
By 2020, upper estimates of the economic potential of IoT with M2M and Metropolitan Mesh Machine Network (M3N) applications predict the generation of benefits to range from $1.4 trillion per year (about €1.09 trillion) (Thanki, 2012) to $14.4 trillion (about €11.2 trillion) across all sectors globally (Bradley, Barbier and Handler, 2013). Revenues from the sale of connected devices and services, and from related services, such as pay-as-you-drive car insurance, have been estimated to be worth US$2.5 trillion in 2020 (Machina Research, 2012).

Besides, the connection of 100 billion devices globally indicates accumulated investments to 2025 of at least €2 trillion at present prices.[15] For example, China has already earmarked €625m ($775m) for IoT investment. In China, the IoT infrastructure investment costs cut across both public and private sectors. In 2012, China's Ministry of Information and Technology set up a fund of $775m to support IoT build over the next five years, with investments for ten IoT industrial parks and in more than 100 core enterprises across the country by 2015. The Ministry estimates that China's IoT market will grow from $31 billion in 2010 to $116 billion by 2015 (Xinhua News Agency and Booth, 2012).

Figure 1.4 illustrates some forecasts and estimates for the IoT.

[15] SCF Associates Ltd's estimate for smart grid analysis in a submission to Ofcom Consultation on 870–876MHz and 915–921MHz bands, March 2013, worldwide (no future discount). For Europe, it translates to over €400 billion of investment to 2025.

Figure 1.4 Forecasts and estimates for the IoT



The macroeconomic picture and a range of sector-specific developments shape the opportunities and challenges that will define European contributions to and use of IoT, the extent and distribution of its emerging economic impacts, and (especially at sectoral level) governance mechanisms and associated challenges.

From an industrial perspective, Europe is well placed to benefit from IoT developments because it has strong industrial capabilities in the supply side (eg telecoms, smart cards industry) and the demand or user side (energy companies, car makers, construction, agriculture and so on). The emergence of an IoT sector has significant potential benefits for the core economic fabric of the EU by enabling employment and growth in European SMEs and larger companies

Taking into account the development of markets around the world, and the fact that the IoT may well benefit from being part of a truly global internet, it seems clear that **developers of technologies** and services need to consider a global perspective.

Europe is an important market and offers rich opportunities for adopting new technologies and services as a solution for societal challenges. Beyond this, the challenges Europe currently faces – and which will shape the form, functionality and business architecture of the kinds of IoT-enhanced services and devices that Europe will demand – merely show in sharper form the challenges that users in other markets face or will face, and therefore allow Europe to take a leading role (and hence justify innovation and investment). This can enhance European IoT players' competitiveness in the early phases of the global IoT market's development.

1.5. Political developments

For many governments economic growth, employment, keeping up the banking system and controlling national debt has become a dominant concern, next to issues like security and sustainability. Within Europe, discussions about the new common budget for the next seven years took a lot of time and effort, as many national governments, even more than in the past, are placing their own domestic political and economic agendas ahead of collective European policies.

With regards to **internet governance** (those platforms and institutions that bring stakeholders around the world together to decide jointly on aspects of the 'global' internet), we note that there is a difference in approach between countries that look primarily at multi-stakeholder organisations to take care of important aspects of the internet, like the Internet Corporation for Assigned Names and Numbers (ICANN), the Domain Name System (DNS), the Internet Assigned Numbers Authority (IANA) and the Internet Engineering Task Force (IETF) (development of standards), and others that place their trust in more government-driven institutions like the ITU. The difference in view came out strongly at the end of the World Conference on International Communications in Dubai in December 2012, when 55 of the 144 states present decided not to sign the new international telecommunication regulations (ITRs) that had been developed, as an update to the ITRs dating from 1988.[16] One reason given was that many of those 55 states did not think ITRs were the best place to take care of things related to internet governance, such as spam, and subjects like cyber security.

A further policy-related development with a political aspect concerns the proliferation of (partial and competing) standards relating to the IoT or affecting its function. As will become clear below, standards affect the workings of markets and the levels and availability of performance, and thus the realisation and direction of IoT development. Similarly, regulatory initiatives will likely have a significant impact on how the IoT develops, and can help to ensure that EU social, political and economic values and principles remain adequately protected. Current European data protection reform (notably the proposed General Data Protection Regulation) can help ensure that personal data in the IoT is protected equally across all Member States, and that citizens receive better recourse mechanisms than under current rules. Similarly, the recently proposed Internet Security Directive aims to raise the level of protection of key online infrastructure and services, and may become applicable to IoT networks as well.

[16] 'By creating a new cold war, we are making everyone a loser, it is a no-win situation. The best way to win a war is to avoid it in the first place,' said Hamadoun Touré, secretary-general of the International Telecommunication Union (ITU), at the GSMA conference in Barcelona 28 Feb 2013.

Spectrum allocation and licensing conditions (see Box 2.1) will affect the availability of spectrum for IoT and the extent to which such products and services can compete on a pan-European or global stage. In short, the fundamental legislation is already in place, and is being continuously streamlined to address new challenges.

PART II Key issues

2. Market forces

According to experts interviewed for this study, the IoT combined with big data analytics is expected to enable the distillation of meaningful information (eg on consumers and processes) from the large amounts of data collected by sensors and other devices and means. These can significantly impact on the cost structure of an enterprise as well as its ability to set prices. Dynamic effects of the IoT on competition among businesses will depend on several factors, such as the size and nature of the other players in the market, the nature of demand and the regulatory context. At the same time, large market players can raise significant barriers to market entry for new entrants, while certain characteristics of the technology create incentives for vertical integration. All these developments emphasise the need for the definition of an adequate and empirically driven approach to competition regulation and enforcement.

This section explores the potential impacts of the IoT on the market environment in which businesses producing or using IoT technology will compete. Impacts on competition will be examined from the perspective of businesses using the IoT, vertical sectors driving innovation and take-up of the technology, and the way these developments interact with competitiveness at the international scale.

2.1. Competition among businesses that will use the IoT

We first consider the **static (single time period) effect** of IoT technology in a single horizontal market involving firms producing alternative or substitute products (goods or services). Production costs may be affected in several ways by data collection and analysis enabled by the IoT. Use of the IoT to optimise business processes can potentially lower operating expenses[17] (OPEX) in several ways. Holding business processes constant, IoT monitoring of the location and physical status of inputs, partially completed stocks and finished inventory provides more complete, usable, accurate and timely information than human-mediated data collection. The resulting reduction in data collection, processing, analysis and curation costs allows firms to shift labour to more productive tasks (egfor

[17] Operating expenses are associated with the day to day running of a business, including administrative and managerial costs.

example data interpretation). More accurate and better synchronised data flows also improve the speed and quality of reporting and decisionmaking. Further, sensors attached to machinery and/or employee badges may be used to improve workflow and reduce costs associated with shirking. Furthermore, by facilitating precise handling and positioning of product components in mechanised assembly lines, the IoT can minimise blockages and improve speed and flexibility in response to supply, processing and demand shocks. For example, information about the temperature and age of perishable items may be used to fine tune delivery strategies. The IoT may also affect capital expenditures[18] (CAPEX), replacing monitoring and surveillance systems with constant feedback from sensors and identifiers attached to inputs, staff and machinery to offer highly detailed, real-time information on business processes.

However the net OPEX and CAPEX effects reflect the way firms gain access to the IoT. Those who invest in their own IoT infrastructure are likely to see a net shift from OPEX to CAPEX. All else equal, this would enhance an adopter's competitive position relative to non-IoT adopting rivals, allowing it to price more aggressively and capture a greater market share. Firms with less access to capital and those unable to sustain sufficient market volumes may be forced out of production. Firms that choose to subscribe to a third-party IoT service will see a shift from CAPEX to OPEX, which may give them higher OPEX than non-adopting rivals. Such firms will only adopt if they are able to leverage strengths on the non-price front, using its branding power or customer loyalty in order to ensure that they can generate the increased sales volume required to moderate the effects of higher OPEX.

On the **revenue side**, the IoT can enhance firms' ability to **monitor buying patterns**. Real-time tracking and modelling of such patterns – in suitably anonymised form – can help firms to adjust prices to shifts in demand over time and across locations. This kind of dynamic and adaptive pricing can generate higher profits than uniform prices or less granular forms of dynamic pricing. Such variations can benefit firms and their customers alike. Within the limits imposed by consumer awareness and preference and data protection regulations, firms can also use such data to create bespoke offers for individual consumers. For better or worse, this approaches first-degree **price discrimination** – personalised prices based on past purchases and closeness to (revealed) preferred product characteristics. Firms could also enhance loyalty and the (individual and collective) value of purchases by selectively sharing (via smart labelling) information about the number and type of consumers buying the good (using status or behavioural biases to increase likelihood of purchase), or providing detailed information on hedonic characteristics such

[18] Capital expenditures are expenditures on acquiring and/or increasing the productive capacity of a firm's assets.

as compatibility with prior purchases, energy use, nutritional characteristics and provenance. Despite the potential to improve profitability, the welfare effects of such strategies are by no means certain to be negative. More effective price discrimination will raise prices for some consumers and lower them for others, and will almost certainly make products available to a larger and more diverse set of consumers. Also, the provision of ancillary information may improve the societal return to consumption and facilitate market incentives to design and sell better products. Other situations may prove more concerning: specifically, in the presence of network effects,[19] increased market share resulting from IoT deployment may allow firms to lock in and exploit existing consumers. This is magnified in two-sided markets, where the adopter firm(s) may use its increased customer base to lock in suppliers. This may weaken competition or make it less efficient.

Over time, the effect of the IoT on competition is markedly less predictable, depending on the speed and pattern of adoption across firms. If the technology is deployed in ways that raise CAPEX, increase pricing power and/or enhance network effects, adopter(s) can drive out other competitors. If large companies invest in their own IoT networks while SMEs need to subscribe via an IoT provider or to interconnect with networks of larger firms, the technology will also affect subsequent firm development and market structure. This issue area is well exemplified by the case of licensed and unlicensed spectrum policies, which is examined in Box 2.1.

Box 2.1 Smart spectrum policy is of key importance for competition

Future allocation of radio spectrum is a crucial issue for the IoT's basic infrastructure, innovation capability and development paths. Various novel forms of radio networks are emerging for the IoT. These range from slow frequency hopping spread spectrum for energy smart grids, deployed in the US and the EU, or command-response networks for reading RFID tags based on the ISO/IEC 18000-7 norm (known in the industry as DASH7) at 433MHz, an initiative originally from the US Department of Defence, which has generated a major ecosystem, especially in the defence industry.

A 2012 study found that the net economic value of spectrum use in general has increased by 25 percent in real terms since 2006 to €63 billion (£52 billion) in 2011 (Kende et al., 2012). The extent to which societal benefit can be realised through these applications depends on the configuration of shared spectrum access rights. This can be achieved in two ways: either based on the Collective Use of Spectrum Model, which allows spectrum to be

[19] Network effects arise where consumption of a good by one consumer increases the utility derived by other consumers of the same good. Examples are software (use by others increases the potential audience with which an individual can share output from the program, increasing the benefit to an individual's use of the program).

used by more than one user simultaneously without requiring a licence (licence exempt), or on the basis of a Licensed Shared Access Model, in which users have individual rights to access a shared spectrum band. The former, licence exempt, approach for collective use is far more attractive for the IoT applications because no contractual negotiations are required – just 'manufacture and use'. Availability of unlicensed spectrum can enable production of large numbers of devices at low cost, leveraging economies of scale, and making communications technology affordable.

The spectrum bands that need to be considered for the IoT have highly varying properties and utility as far as the various different IoT applications go. While broadcast and mobile fight over the prime spectrum area (UHF, 300MHz to 3GHz) which gives the best long range propagation, it will also be needed for IoT devices that must transmit over kilometres. Other applications, such as near field communications (NFC) at 13 MHz, may also use EHF bands as they need to transmit over centimetres or millimetres for non-contact transactions. The traditional AM/FM bands in the VHF range may also be useful for some IoT applications.

The political dimension of spectrum access in becoming increasingly present in debates surrounding the IoT. At the World Radio Communication Conference in 2012, certain countries requested release of the 700 MHz band from broadcast services for use instead by mobile and other purposes, resulting in a political upheaval between supporters and opposition of the licence exempt approach. If granted, the IoT could gain the prime range spectrum it needs for large metropolitan area mesh machine networks and other applications that require ranges of over 30 metres. The European Commission has a key role in ensuring that rights to spectrum access are configured in a way that does not end up hampering the growth of innovation and development of IoT applications, including the harmonisation of conditions across the EU. Studies analysing the potential release, and which have already been presented to the European Commission, propose that one sub-band of the potential 100 MHz spectrum release should be reserved for licence exempt devices and that whole band should not just be reserved for licensed mobile use for long-term evolution (LTE) roll-out (SCF Associates Ltd, 2012). Naturally this might be progressive with a first reservation expanding as more applications using licence exempt come into play over the next two decades. The bandwidth of the licence exempt section may expand from a first range of perhaps 20 MHz for IoT type applications and 10 MHz for emergency services in a new generation of Terrestrial Trunked Radio (TETRA)-like emergency services in 2016 to perhaps 50MHz for licence exempt services after 2030.

Further, the use of compatible and interoperating IoT systems may also reduce extensive competition, while facilitating intensive collusion via information exchange among firms.

This potential adverse effect might require enhanced **antitrust scrutiny or enforcement**. Conversely, the simultaneous adoption of IoT by a 'core' of large businesses could increase competition among them even if competition between the core and smaller peripheral firms is reduced. This may transform quality-based competition into price competition and squeeze margins, benefitting consumers.

However, there may be a prisoners' dilemma effect: firms may adopt IoT because their rivals have, whether or not it raises industry profit or societal welfare. The result is over-adoption and overinvestment by incumbents and insufficient entry by firms unable or unwilling to make this investment.

The IoT may have other important **dynamic effects**, in that by increasing mechanisation, firms may counterintuitively become less responsive and flexible. While in the static case production costs may be lowered and managerial decisions easier to implement (people are harder to hire and fire, and machines can be turned off and back on again as market conditions require), such reliance on data and monitoring rather than human interaction may slow the firm's ability to recognise structural or qualitative changes, resulting in reduced worker loyalty and motivation (therefore higher turnover), and lead to weaker incentives to form and exchange human capital. This may be a problem particularly in times of severe market shocks, when staff can use their experience and knowledge of past market shocks to craft responses to current issues. The result may be deterioration in the balance and level of product, process and effort innovations, diminished firm resilience, deadweight loss and/or slower innovation post crisis.

We next consider implications for **vertical markets**. Differential IoT adoption across stages of production could shift the balance of power between upstream and downstream firms. Consider the case where the technology improves the position of a downstream firm relative to upstream firms (eg if a major retailer, adopted the technology while its myriad suppliers did not, or did so less successfully): increased market share would raise the bargaining power of the retailer in supply negotiations and allow it to extract a larger amount of any surplus enjoyed by suppliers (eg via increased discounts). However, the effect on consumers is ambiguous. On one hand, if downstream competition is sufficiently strong, the retailer would pass these savings to consumers by pricing even more aggressively, or could maintain its low prices and use the additional surplus to improve products. On the other hand, if it faces little competitive pressure, the retailer could use its increased power to raise prices. In either event, the effect of the increased bargaining power relative to suppliers is to magnify the effects of IoT adoption in the downstream market. (Analogous reasoning holds where IoT technology improves the bargaining position of upstream firms relative to downstream players.)

In the dynamic case, there are two interesting questions. One is what effect such a shift in the balance of power will have on the likelihood of vertical integration. **Vertical integration** is most often pursued so that a firm can control the full supply chain and, by suppressing multiple mark-ups, offer a more competitive downstream price. Integration by the IoT adopter would allow the firm to deploy the technology over the whole value chain and offer lower prices; but, conversely, the IoT adopting firm gains greater ability to extract surplus even without such a merger, so the predictions are unclear. Even in cases when the technology is linked to price decreases in the downstream market, antitrust authorities may also be concerned about possible supplier 'lock-in' and the increased power enjoyed by the adopter-firms in vertical contracting. The question becomes even more complex when user firms access IoT technology via subscriptions, as it may be that the 'pure IoT' service providers could come to control retail markets in which they have no direct stake. Since such players are likely to be few in number, large in size and may be non-European, there may be a significant risk of **market foreclosure**.

The second question focuses on whether the adopter firm would ever choose to **license or otherwise share data collected via that technology with others**. The standard answer should be no, but this reasoning may not hold where the firm faces a powerful countervailing party (egfor example a large manufacturer retailing through a large distributor). In that case, the firm may be interested in helping the cost and/or flexibility of rivals of the countervailing party to 'catch up' so as to use them as alternate channels, blunting the market position of the countervailing firm and recouping some of the lost surplus. Then the firm might consider licensing its (access to) sensor technology. Further, as alluded to earlier, firms may be able to use interoperable IoT systems as a means for collusion.

As a result, likely dynamic effects of the IoT on competition depend critically on the size and nature of the other players in the market, the nature of demand and the regulatory context. Greater focus on these, **using empirically generated parameters and/or case studies, may be useful to generate a better understanding of when the technology may lead to negative effects on competition**. The overall message is that antitrust regulators will need to carefully monitor major markets affected by the IoT. Given that the effects are likely to differ significantly across industries, the IoT may therefore strengthen the case for an antitrust policy interpreting principles within changing contexts rather than one operating on the basis of rigorously pre-defined rules.

Note that in the above, we have assumed that consumer demand is not affected by the introduction of this new type of technology. **If consumers are attracted by the increased personalisation made possible by IoT technology then, all else equal, these sectors will enjoy increased demand. However, if consumers are put off by concerns about privacy, psychological manipulation or lack of clarity on legal implications of IoT –**

or by the very shift of power from buyers to IoT-enhanced sellers implied by the above analysis – **their demand may shift away** towards firms using the standard production, distribution, marketing and transactions processes, so IoT investments will not be recouped or that the nature of IoT innovation will be distorted. Indeed, privacy-related issues may even generate legal cost and potential loss of further customers, which may outweigh the benefits of adoption.

2.2. Competitiveness (among countries) hangs on productivity

The effect of IoT development on EU competitiveness requires different elements to be taken into consideration regarding firms operating on the demand and supply side. On the supply side European competitiveness can **tap into the potential of European science and technology research capabilities**, and be **promoted through antitrust, public procurement and international trade initiatives**. At the same time, businesses operating on the demand-side can **potentially leverage high standards of consumer and data protection built into European technologies**.

The growth potential of IoT producing (supply-side) firms in global markets differs across countries and industries, and across key market players within each industry. It depends on the value chain 'location' of those firms in key sectors (what aspect of the IoT architecture the firms of a particular country supply – hardware, software, protocols, standards), the portion of value created in the particular aspects of the chain, and the extent to which technologies are protected. If the increased demand for such technologies allows EU firms to make better use of the EU's world-class **science and technology** research and training, EU firms will have a competitive edge on global markets. Further, if development of IoT systems proceeds along **open access** lines, EU firms will not be impeded by vertical foreclosure on the part of extra-EU producers. As seen above, the role of **competition policy** is central in defining conditions of access to markets. As regards domestic markets, **public procurement** may be a valuable mechanism to build sustainable demand for these technologies. To the extent that EU supply-side firms, by dint of better local knowledge, can provide services that are aligned to the requirements of EU public procurement, these contracts can provide firms with adequate demand to allow them to become globally competitive. In this way, EU governments can support development of EU firms in a way that does not exclude foreign firms, and increases effective competition in these areas.

EU firms may also find themselves well placed to support IoT investments in other jurisdictions, particularly China, which has been investing heavily in this technology (there is more detail in Section 1.4) and there is scope for EU supply-side firms to grow their businesses by connecting with Chinese firms to provide enhanced tracking of movement of goods through the Single Market and helping those firms learn about the adoption and use of Chinese goods, services and technologies in the EU.

We turn now to competitiveness of EU IoT-using **(demand-side) firms**. As a starting point, we note that EU firms operate in an environment where legal requirements surrounding privacy and consumer protection are elevated relative to other major extra-EU jurisdictions. As a result, EU firms generally face a cost disadvantage in global markets. However, the competitiveness of EU firms may be improved substantially depending on the evolution of the attitudes of extra-EU consumers about the treatment of the increasingly personalised data that might be generated by the IoT. In mature markets, businesses need innovative delivery models and unique value propositions to attract and retain customers.[20] One component of such a business proposition that could align competitive forces with the ethical issues, might be a form of marketing based on '**ethical IoT technology**' to enhance branding and increase customer bases, much like the 'green tech' revolution of the last decade.[21] In this context, an understanding by businesses of user apprehension and related needs will foster better brand and service positioning within the full IoT human interface environment. This in turn may have positive effects on the ethical content of market innovation and business profits. Indeed, to the extent that **consumers call for increased protection from all firms and for privacy, security and other ethical concerns in design**, EU firms, already well versed in providing higher levels of protection for consumer data, may find themselves well placed for competition in global markets. In this way, by leading the trends for global demand, EU IoT demand-side firms can also improve the business prospects for EU IoT supply-side firms.

Differential adoption rates and **differential national absorptive capacities**, linked – *inter alia* – to differences in the ratio of large corporations to SMEs, may therefore **produce divergence within the EU**, though the extent to which the divergence reflects the true differences in comparative advantage between countries will need to be carefully monitored. The potential for divergence also highlights the importance of policy coordination actions across the EU, to minimise the possibility that national policies counteract each other or otherwise have unintended consequences at the level of the Single Market.

---

[20] This could lead to improved results. However, one argument against easy consumer mobility, which has also been made in relation to the app ecosystem, is that a wide range of choice and low switching costs leads to 'competition by features' rather than competition by functions; consumer churn is very high and firms cannot retain customers long enough to develop loyalty or come to a user-led understanding of the virtues of their offerings (and thus the best direction for further refinement or innovation).

[21] However, the analogy with the green revolution also sounds a note of caution; there is ample evidence that people pay more for 'virtue goods' than the benefits warrant and that the linkage between price margins and 'ethical demand' and delivery of concrete advances in 'warm glow' attributes may be weak, unreliable, difficult to audit or even perverse

2.3. Vertical sectors (eg driving sectors, health, energy)

IoT development will likely follow the needs of the main sectors in which it is applied, potentially leading to the coexistence of multiple systems and raising questions related to the interoperability of these applications and the development of shared platforms.

Fundamentally, IoT technology must help firms to meet the needs of end users in the relevant sectors. Thus, the evolution of the use of such technologies in each sector will be demand driven, though it does not necessarily follow that development of the constituent parts of the IoT infrastructure will be demand driven. **Each use case will have specific needs, as different sectors will generate different sets of requirement for things like privacy and auditability.** For example, health uses (such as organ monitoring) may place more emphasis on the need for constant contact with remote networks, requiring complex interconnectivity in devices, while energy uses may be more concerned with constant monitoring and periodic information transmission to remote networks, requiring data storage and larger file transmission across networks. The IoT will therefore contribute to rich ecosystems, which are very different from sector to sector (eg linking surgeries, doctors and patients in health care, versus linking residential and commercial users to suppliers in energy, versus linking within residential and commercial networks in transport), each of which will interact with and influence the technologies in different ways. This may lead to a focus on the **coexistence of different systems and on interoperability across these systems**, which contradicts the classical concept of economic efficiency, which would suggest that economies of scale may be enjoyed with less variety in systems.

Further, different use cases may also need to **function via a single platform device** such as a mobile phone, which might serve both health and energy consumption monitoring uses. As a result, the mix of end uses will instantiate areas of specialisation, though the need to serve a range of different functions will require a good balance of generic enablement across devices. Thus, the architecture of existing industries will change if its outputs can be used as the basis of an IoT for other things: returning to our example of the mobile phones above, this might require that smartphones have NFC functionality alongside its networking functionalities (so that health information can be communicated by other means when the device is out of network coverage areas). One particular issue within the mobile market is the control exercised by mobile network operators (MNOs), which have significant incentives to restrict network access through spectrum ownership structures, control over mobile numbers and the use of SIM cards, for instance by proposing to use existing mobile cellular numbering for identification and addressing of M2M communications, with identification based on the SIM card International Mobile Subscriber Identity (IMSI). Although the ultimate extent of these incentives depends on the payoffs that can be derived from granting access, the network effects of these competition-limiting strategies would not only enable MNOs not only to charge higher

prices for IoT-related services, such as M2M roaming, but would also limit competition in downstream markets of M2M services (see also Section 2.4).

This raises another important policy issue. Financing for investment in these technologies makes business sense only if a minimal, basic infrastructure is in place for the use and funding of the 'things' to be operationalised and interconnected; as a result, research and development may be more likely in specific sectors. If policymakers can therefore find and **support the sectors which are likely to have the required catalytic roles**, they will be able to drive the evolution of the IoT in important areas.

Box 2.2 describes some of the opportunities and challenges for I0T and big data.

Box 2.2 IoT and big data – opportunities and challenges

IoT and big data[22] reciprocally enable each other: while sensors are able to provide the large volumes of data fundamental to closed and open loop analytics used within and outside the IoT, realising the potential of several IoT applications relies on the analysis and continuous feedback of big data streams.

Big data analytics has significant potential for enhancing the efficiency of IoT applications listed earlier in this section; for instance, through big data analytics an application monitoring pollution can scan for warning signs and critical levels of the presence of certain agents in the air or water based on past incidents. Closed-loop applications of data analytics are already used in several processes linked to industrial and product management functions. As further explained in Section 2.1, analysing sensor data can ultimately allow companies to optimise spending on capital and operational expenditure. Harnessing the possibilities for value creation created by these interlinking developments as the number of sensors increases will likely impact on markets by increasing demand for an infrastructure that can support data flows of unprecedented size and for analytical capabilities in software, hardware and human capital.

Data processing remains a two-sided market in the IoT: companies can gain insights through using the data that is already in their possession, but there is a secondary market of data collected for certain purposes that can be fed into uses different from the original aim of the collection – egfor example health sector companies can acquire data on patient behaviours through telemedicine applications, while selling data on interventions.

While the use of analytics for data originating from sensors for industrial applications and in closed-loop settings has the potential to enable the creation of efficiencies and economic

[22] Big data technologies can be defined as a 'new generation of technologies and architectures designed to extract value economically from very large volumes of a wide variety of data by enabling high-velocity capture, discovery, and/or analysis' (Vesset et al., 2012).

value, technologies that involve processing data linked to individuals or their behaviour present several challenges cutting across privacy, security and consumer protection. While these issues are similar to those encountered in other applications relying on big data analytics (eg internet-based behavioural advertising), the IoT's scale, pervasiveness and ubiquity provide new dimensions to concerns about the accountability and transparency of these methods. For instance, defining 'personal' data, ownership or an optimal level of control of the user in the context of data mashing and mining becomes increasingly difficult in applications using data from sensors. Furthermore, although anonymisation standards and best practices exist for the secure management of personal data, collating ('mashing') data from multiple anonymised or open datasets has been shown to enable the re-identification of individuals. These developments continue to raise concerns about desirable and feasible levels of anonymity in these applications, especially in sensitive fields such as healthcare.[23]

2.4. Investment (good and bad)

The development of the IoT will require investment at all levels from basic infrastructure (much of which it shares with the internet more generally) to IT-specific applications, services and devices. Some of this investment will be devoted to fixed capital creation, but investment in research and innovation (in human, social, organisational and fixed capital) is also required. The potential of the IoT is thus bound up with investment quantity, availability, cost, structure and conditions. These in turn depend on the expectations of potential investors as to the likelihood, timing and correlation of returns. Therefore, the timing of investment in different layers needs to be favourable. For instance, investment in IoT devices and service development will be stronger if the necessary infrastructure capacity is available and will be maintained.

Currently, there is much uncertainty as to where such funding will come from and how business models and contractual and market arrangements will develop to permit investors to capture appropriate returns and to encourage entrepreneurs to make best use of existing (sunk) capital. In view of the complexity of the risks, the likelihood of significant failures in specific technologies, standards and business models and the long time-scales involved (10–15 years for global roll-out and possibly longer for pay back), financial markets may not make the right amount and kind of capital available. To assess the current prospects and potential need for support, this section considers the factors affecting IoT investment.

[23] There is significant scholarly literature on the re-identification of anonymised and de-identified datasets. See eg Narayanan and Vitaly Shmatikov, 2008; Ohm, 2010; Ramachandran et al., 2012.

This is not simply a matter of providing capital; there are clear governance issues including final ownership of the infrastructure and the openness of the extended value chain; these will be influenced by and will in turn alter the levels and kinds of investment available and thus the costs and benefits of the IoT.

Box 2.3 analyses the development of the IoT in a global recession.

Box 2.3 The development of the IoT in a global recession

The persistent recession in Europe and its attendant phenomena (including the weakness of the Euro, increased demand for social benefit expenditure and downward pressures on tax revenue) create a challenging climate for the emergence of a new IoT cluster, made even more difficult by its exposure to global competition and as applicable to global markets as the IoT.

In particular, despite a somewhat brighter GDP growth and employment in individual countries (especially traditional technological leaders and some new Member States), the overall picture remains weak and the resulting divisive discussions over macroeconomic and monetary policy continue to hamper Europe's access to global capital. In addition, some of the recovery in export growth is driven by the weakness of the Euro vis-à-vis other global currencies and the resurgent demand in those countries whose recovery is proceeding more rapidly. This provides a brief window of opportunity to convert these revenues into the basis for sustainable future growth, but a depreciation-led export surge on its own cannot provide this. In addition, disagreements as to the pace and nature of austerity measures (and the proper mix and government level of recovery stimulus policies) together with serious friction over financial regulation create aggregate uncertainty, which discourages the inward flow of global capital and the reinvestment of European businesses' substantial cash balances in innovation, infrastructure renewal and other forms of productivity enhancement.

The picture is somewhat brighter at the sectoral level, at least potentially. Although European manufacturing is extremely weak across the board, there are some bright spots and some true global champions in IoT-related areaseg, for example ARM Holdings, whose business models (gazelle-like growth with minimal direct investment in costly and rapidly obsolescent large fixed capital) immunise the company against the most dangerous aspects of the recession. In addition, the **services economy**, which has enormous future potential to benefit from IoT-enhanced capabilities, is strong enough (in access to capital and in market power) to fund this technological transition.[24] The 'leverage' effect of further

[24] One critical uncertainty concerns the financial services sector. While this is not – as yet – directly dependent on the IoT, modern computerised price discovery, valuation and trading systems certainly depend on real-time access to vast volumes of data, and thus on the sensors needed to

development of the European services sector is likely to sustain a positive feedback loop, with new forms of IoT capability driving and being driven by service expansion and globalisation along lines that characterise the European market model – not only providing an IoT environment but also building services that use the data that result from this environment.

Investment at all levels is required to support optimal development of the IoT. These layers include devices, infrastructures, services and applications. An efficient IoT would 're-use common elements where possible and permitted[25] – especially as regards high fixed-cost infrastructures. This corresponds to the 'ladder of investment' approach, developed by Cave (2006), which is based on the idea that investments in shared facilities have a multiplier effect that stimulates investment and competition in layers that use these facilities. It has been used by European national regulatory authorities in utilities and telecommunications to justify measures to force incumbent operators to open even vertically integrated networks to access at multiple levels in order to let alternative operators climb up the ladder, using more of their own infrastructures and thus decreasing their reliance on the incumbent's wholesale resources. To market its own services, these rivals must complement the incumbent's wholesale resources (created under regulated conditions) with their own capital, which should (in principle, see Herrera-González, 2011) be formed under commercial conditions. Of particular interest is the possibility that this approach may stimulate production of capital that complements 'generic' communications infrastructures with specialised IoT-orientated resources.

Table 2.1 lists the investment level required for each IoT value layer.

collect them, the networks that transmit them and the data centres and server farms that store, process and make them available. The flexibility, low entry costs and self-organising scalability of the IoT point the way to a much tighter fusion in the future, providing current regulatory discussions find successful, swift and effective resolution. At the same time, the relative paucity of good productive (as opposed to speculative) investment opportunities suggests the potential availability of a reservoir of capital available to promote the development and rapid deployment on European scale and beyond of IoT technologies and services at all levels from individual devices to network architectures.

[25] SCF Associates Ltd, 2013, submission to Ofcom Consultation 870–876MHz and 915–921MHz bands.

Table 2.1 Investment level required for each IoT value layer

Value layer	Additional investment required	IoT-specificity
The application layer, which stores, processes and applies the digital signals received through networking services and adds value by supplying required services or sending instructions to actuators	Medium–high	Medium–high
The platform layer, which provides the computing infrastructures[26] on which IoT-derived data are stored and processed and over which IoT applications operate (and are delivered)	Low–medium	Low
The services layer, which governs the transmission and routing of digital signals between applications and devices	Medium	Medium–high
The network layer, which transports the digital signals between devices and application platforms	High to very high	Low
The device layer, which consists of connected sensing or perception and actuator objects, gathers and transforms information from them, or distributes and coordinates instructions to them via suitable protocols	Low–medium	High

There are **multiple (current and potential) investors planning infrastructure and application funding**. Investment in all of these layers may (now or in the future) be delivered through a variety of models, including:

- private financing
- public investment
- a mix of public and private investment
- social (eg crowd-funded) finance.

This section concentrates on the two layers combining medium to high levels of investment with a substantial degree of shared capability between the IoT and other uses: the infrastructure layer, because the creation and maintenance of suitable capacity is a necessary precondition for development in other layers; and the applications layer, because utility computing applications are required to generate added value for innovative IoT services and business models.

[26] This may be provisioned as cloud platforms; in any case, the IoT may share the platforms.

Private financing, especially at the infrastructure layer, can be obtained through investments by five main types of industrial players, sometimes with specific investment and business models. Telecommunication carriers, especially MNOs, will invest in an attempt to consolidate a market position as carriers of all radio-based information. MNOs have signalled their willingness to extend their legacy infrastructures to handle IoT traffic by proposing to use existing mobile cellular numbering for identification and addressing of M2M communications, with identification based on the SIM card IMSI. Because SIM cards for mobile connection are issued and controlled by operators, they view them as a market control mechanism to protect their infrastructure (for the IoT or otherwise) investments and their market power and profits. They are especially interested in financial transactions (Palmer, 2013, which spans mobile purchases and banking) but are also exploring new services.[27] Peripheral telecoms players are also moving into the market, from fixed line operators to new players like Arqiva in the UK, which owns sites for radio[28] transmissions and is now targeting smart energy grids with transmissions in unlicensed spectrum bands. Competition for the lucrative carriage of IoT data is already intense in this segment, and major investors are launching campaigns to exclude rivals on technical grounds.

These developments highlight an important aspect of the investment issue: commercial players will invest in ways that optimise commercial returns, and the struggle to create and protect these returns may be costly to the segment as a whole. The traditional tensions between telecommunications sector development and competitive efficiency that led to the regulatory framework for electronic communications (European Commission, 2002) and continue to affect the development of the internet (Libenau, Elaluf-Calderwood and Karrberg, 2012) may well persist into the IoT. These are some examples:

- Vertical industry players are building specific 'smart infrastructures' for their own businesses – energy, logistics, automotive, building services etc – with many additional players supplying specific equipment and services; they are often heavily involved in the IoT community (eg Schneider Electric in automation).
- Major 'electric' infrastructure providers are capable of building end to end systems at reduced additional cost using their existing infrastructures – such as GE (with its industrial internet for manufacturing and supply chains) and Hitachi (which has a portfolio of investments in leading smart energy players such as Silver Spring Networks). These players tend to

[27] For example, AT&T's alliance with Ford to locate recharging stations for electric vehicles.

[28] Mobile, WiFi, broadcast, satellite, etc.

develop the technology and sell it to telecom and vertical investor, while also using it for their own major development projects.

- Web or internet service providers are already beginning to invest in infrastructures and may extend this into IoT provisioning in order to offer multiple services that increase their media and consumer operations into the IoT. They are more likely to invest in IoT applications and open standards rather than infrastructure. For instance, large search engine or e-commerce players already aggregate consumer data for sale to interested third parties and may seek to extend this to data from the use of smart appliances.
- Other private investors may invest in all layers shown in Table 2.1 to support a range of business models, accepting varying payback periods, acceptable levels of risk and types of development. The IoT may offer long-term investment opportunities that might particularly attract very large investors under current conditions, which have led to large cash surpluses.

Public funding for an IoT is likely to come from several sources:

- *national governments and their respective industry related ministries*: for instance energy and environmental agencies investing in a national smart grid, or investments and other forms of financial stimulus undertaken in conjunction with broadband deployment programmes
- *local and regional governments*: for example as part of investments in forest fire monitoring, seismic fault activity, river levels or agricultural networks over large areas or in conjunction with local economic development initiatives
- *municipal administrations*: for instance investing in a smart city[29] or incorporating it in delivery of municipal services ranging from waste collection to social care
- *investments by state owned corporations*: for instance postal and transport services
- *EU-level funding*: including economic development, structural and cohesion funds.

[29] This is already under way in the UK as part of the TSB 'Smart City' competitive funding initiative. Glasgow's IoT infrastructure and applications formed a major part of its winning bid.

Mixed public and private financing – collective arrangements are often considered suitable for the longer-term investments and can take several contractual forms, eg for example:

- *co-financing* via public–private partnerships (PPPs) with a variety of shared investment, ownership and use arrangements, including leaseback
- *sub-leasing* in which public infrastructure is leased to private operators and/or service providers, or reverse arrangements where privately owned infrastructures are leased to public authorities (eg in a private finance initiative, for example an energy company's smart grid may be used by a local authority to gather air pollution sensing data, while the energy company uses a separate services company to operate the infrastructure it owns)
- *differentiated shared investment* in which public and private entities invest in different layers of the IoT in order to ensure efficient delivery of infrastructures, applications and services that reconcile value for money in IoT delivery of public services with competitively justifiable and efficient economic returns.

2.4.1. Governance implications – who 'owns' the IoT?

Conventional notions of ownership bundle together a range of property rights and obligations including control of use; claims to economic returns; ability to sell, transfer or destroy data; ownership claims on derivative assets (eg intellectual property); and liability for harm. Different investment vehicles result in variants of this notion of ownership – partnership provides something close to joint and several conventional ownership (as above); equity conveys a qualified voting right of ownership with limited liability; and debt provides only a legal and monetary residual claim. The differences in these claims lead to well-known governance distortions. For example, the presence of debt claims may lead management to embrace investments with negative net present value (debt overhang) or reject investments with positive net present value (asset shifting). Some of this distortion can be controlled by changes in ownership or the separation of ownership from control; for example, failing banks have been partially nationalised in many European countries to ensure continuous delivery of necessary retail banking infrastructure services, and economic regulation has long been used to ensure adequate investment in critical infrastructures, to control abuse of market power by infrastructure providers and to ensure (through universal service obligations) the necessary availability, quality and affordability of key public services delivered over such infrastructures.

There is ongoing debate about how (or whether) to extend these considerations to the internet and to other related areas (eg cloud computing). For present purposes, we note

that all these issues are connected to investment and the type of ownership to which it gives rise. To gain an appreciation of the direction of travel of these developments, we here discuss three investment scenarios[30] that carry different implications for the governance of the IoT and its impacts on European society: the free market, the mixed market and green life.

The free market'

Highly aggressive private sector players will invest heavily and claim market dominant positions in key industrial sectors using network effects and embedding standards that give them control of interoperability. Public sector investment is absent and competition rules are weakly enforced, leading to a situation akin to the web services market. The major players are the larger multinational corporations, all based outside the EU. They gained a first mover advantage through early innovation; this is preserved by network 'tipping effects', the law of increasing returns on software (which also applies to some extent in low-cost devices and sensor capillary networks), and effective control of standardisation and capture of regulatory authorities. It may result in a stable situation of sectoral monopolies, oligopolies or cartels. The global IoT sector becomes a set of markets effectively stove-piped and closed to new entrants. Public interest motives in sectors such as health, education and care of the aged and infirm tend to be neglected or operated as business with high margins. There will be relatively few social and macroeconomic benefits in the form of jobs, innovation and new industry in Europe. Moreover, ordinary citizens suffer because of the lack of effective governance in areas ranging from privacy to liability for malfunctioning of IoT networks.

The mixed market

public sector and public services invest collaboratively under this scenario. Public sector investment creates a strong infrastructure based on open standards and linking major networks for managing energy distribution, cities, transport, health and education with high levels of benefits for everyday life. This could encourage the creation of new industry and employment, and the education of a new generation of highly skilled knowledge workers, and therefore create new export markets for European expertise in IoT infrastructures, specifically the technologies, software applications and devices across the major 'soft' and 'hard' infrastructure markets. Moreover the EU's internal efficiencies drive its own renaissance in areas ranging from imports of hydrocarbon fuels to the incidence and costs of mental health treatment. Major investment programmes for start-ups with

[30] Scenarios take a hypothetical position on a prospective reality. The scenarios presented here build on work already completed for the European Commission on the Future Internet, report available on request from the Oxford Internet Institute website:
http://www.oii.ox.ac.uk/research/projects/?id=56.

venture capital and validation pilots for the interoperability of large-scale infrastructures are needed to seed this, as well as basic research, development and innovation (RDI) investments in early stage research, particularly in embedding governance for safety, security and privacy.

Green life

In this investment scenario, Europe and the rest of the world are forced to invest in a highly specific IoT. Global warming and the IoT economy become inextricably linked.[31] As environmental issues dominate with the planet's warming accelerating, in this scenario, the IoT is seen to play a crucial role in combating climate change and achieving sustainability in Europe. It provides the global network that can intercede by managing the situation, cutting energy with smart energy grids and continually monitoring the state of vital parameters. It hereby underpins new ultra green technologies that enable a low-carbon green society. This also provides a strong economic rationale for aggressive action against climate change. By creating new industry sectors, products, services and employment a green economy becomes key to EU economic recovery.

2.4.2. How the IoT might serve as an attractive new investment opportunity

If stability for investors can be combined with suitable governance, the IoT might serve as an attractive new investment opportunity and fulfil its promise to meet Europe's strategic goals. Such an opportunity would stretch across many sectors and into the everyday life of most European citizens. If realised as imagined in the mixed market and green market scenarios, investment in smart infrastructure is one of the few opportunities for high tech growth currently on the horizon that could strongly stimulate the European economy and provide a sustainable way of life. The key questions will be: who 'owns' the IoT and whose interests and capabilities will determine its evolution?

While good investment may benefit the citizen and the economy, bad investment models may threaten competition, by building monopolies with entrenched vested interests. There may then be further negative effects for the citizen: danger to life, or if safety, privacy and security is not emphasised. At this point, who 'owns' the IoT infrastructure becomes important – could it be a fragmented ownership, or like that of the mobile networks (multiple private enclaves), or instead like the internet (nobody owns it but many bodies

[31] There is now further evidence confirming that climate change is accelerating, with more global warming in the last 15 years than in the previous 15 years. A new study of ocean warming has shown that deep oceans are absorbing heat, lulling observers into a false sense of security of the overall rate at atmospheric level, which has been more moderate over the last decade but may now accelerate. See Balmaseda, Trenbert and Kallen (2013) and Wolf (2013).

collectively cooperate to perform its governance). Investments will reflect the final ownership structures and governance must assure the ultimate liabilities and benefits.

3. Education, values and social inclusion in the IoT

This section will take brief look at the most prominent ethical issues surrounding education,[32] identity, autonomy and trust in the context of the IoT, which emerged as the most important ethical concerns capturing the friction between our current value systems and the development of technologies potentially enabling other people, organisations and machines to act in dissonance with those beliefs. We will concentrate on the characteristics of the IoT that raise ethical concerns, differentiating this technical development from other networks, as summarised in Section 1, and the operational approach that policymakers can consider adapting when confronted with value-based tensions. Furthermore, our analysis will remind the reader that it is not always all of these elements that pose ethical challenges, and challenges are not always posed in the same way. For instance, the fact that objects are connected raises a different set of challenges to values from the development of smart or invisible ones.

3.1. IoT: a new dimension to pre-existing ethical tensions

Most of the ethical tensions surrounding the development of the IoT are also present in the debate about the internet and other emerging technologies. However, the specific characteristics of the IoT, such as ubiquity, smartness and connectedness, together with the progressive invisibility of the infrastructure, tend to lend particular relevance to certain questions. For instance, limits to the user's awareness of the process of interacting with the technology, as well as informed consent and autonomy of action and decisionmaking become challenged in new ways. Beyond the uncertainties surrounding the future of privacy – dealt with in Section 4.3 – autonomy, trust, identity and social inclusion are further challenged by the emergence of the IoT.

At present, the benefits of the IoT are easier to capture at the level of applications and their potential to pursue the values of an inclusive and just society rather than the solutions offered by them to ethical challenges. Therefore, the policy and design communities have to operate challenging trade-offs between straining ethical concepts and practical benefits.

[32] By education we mean user awareness and the skills to benefit from IoT, not education as a sector.

One such overarching tension is represented by the functioning of technology, intended to evolve towards ever more seamless operation, thus pre-empting or replacing user action, and that of user autonomy in internal and external self-determination and the principle of protecting a user's autonomy through guaranteeing that decisions are made based on her informed consent.

Autonomy

The IoT has the potential to empower individuals to dedicate themselves to more complex tasks by delegating lower-level ones to technology, or offer valuable tools to 'nudge' individuals towards socially more desirable behaviours. At the same time, profiling algorithms and self-learning autonomous systems may also reduce the external autonomy of users through restricting the range of options available to them.[33] They might also reduce individuals' internal autonomy (the freedom to make up their own minds) by redefining their identity to conform to the capabilities of the technology to process and interpret data.[34] This risk also appears to be felt by the respondents to the public consultation, 65 percent of whom felt that IoT could interfere with user autonomy. The use of IoT and big data analytics by different actors can result in a skewed balance of power between individuals and states or companies.[35] Furthermore, changes to the degree of autonomy exercised by technology will likely necessitate a revision of the legal architecture defining the distribution of **responsibility and liability in the IoT**.

Identity

The smartness and ubiquity of IoT systems question the concept of a person's right to maintain **multiple identities** (and feasibility of doing so) in the offline and digital world or creating digital identities that do not entirely fuse or overlap with the real life ones (seeeg for example, de Hert, 2008a, 2008b; Hildebrandt, 2009; Prins, 2009). For instance, a person whose patient profile has been constructed through e-health applications might want this profile to be separate from a consumer profile based on her financial habits, and egnot be judged or profiled on a past health status (eg a cancer patient in a job interview occurring after the completion of cures). However, insurance companies and potential employers would have an incentive to mash these different data sources together (eg Halperin and Backhouse, 2008; Hildebrandt, 2009, 2012; Pagallo, 2012).

While storing information can potentially serve the need to preserve social memory, it can at the same time limit a person's right to self-expression and self-determination by anchoring ('freezing') an identity to specific moments in time. Literature (de Hert, 2008b;

---

[33] Response to the public consultation by a telecommunications company.

[34] See, for instance, van Dijk (2010).

[35] See, for instance, Hildebrandt (2009, 2012), Tene and Polonetsky (2012), Daskala (2010), van Dijk (2010) and Prins (2009). This was also underlined in our interviews with academics.

Andrade, 2012; EGE, 2012) and one of the ethicists interviewed for this study highlighted that the extent to which the reinvention of identity is considered desirable requires deeper reflection in particular about the scope and quality of the so-called 'right to be forgotten' or 'right to be erased' (we can think about how health data, criminal records or location information may give rise to different question). The 'right to be forgotten' or 'right to be erased', often cited in relation to the right to privacy, therefore present a particular dimension in the IoT and has to be re-thought to reflect the relative importance of these factors for personal identity to evolve in a smart context over time (eg De Hert, 2008a, 2008b; EGE, 2012).

Trust

Trust is particularly relevant in the relationships between all stakeholders (business, governments and users), as perceived abuse could lead to a societal rejection of new technological developments.

A decrease in the relevance and reliability of the concept of **informed consent** would also result in an increased need for something that can replace it as guarantee for users while respecting the requirements of independent decisionmaking (see for example Prins, 2009).[36] Ultimately, the purpose of ethical tools, such as informed consent, is to ensure trust in the systems and thus social acceptance of the technology. Trust is a vast topic that incorporates trust establishment, trust management and security concerns. Although trust can be broken down into several specific concerns (eg a vicious circle of replacing broader trust with greater reliance on control, surveillance and regulation (Bohn et al., 2005; Ess, 2010) the feature differentiating the IoT from other infrastructures and technologies is that with the transparency or invisibility of the technology and the lack of interfaces, trust – similarly to consent – is being assumed and designed into the system. **An emphasis in governance on control and surveillance has the potential to decrease trust in the systems, especially as increasing mediation by the system (actuation without human intervention) increases the potential for deception through technology** (Grandison and Sloman, 2000; Ess, 2010).

The characteristics of the IoT therefore necessitate the creation of a **systemic trust**, which does not need to be negotiated application by application. Trust therefore would **have to be defined at the architecture and governance** levels of the system and rest on higher-level guarantees. As emphasised by one of the ethicists interviewed for the study, real trust would embody several elements (eg a reliance on the steady provision of services, conformity to legal and contractual obligations, such as purpose specification, and so on) but ultimately could be distilled into reliance on the beneficence of systems: that the user

[36] See for example Prins (2009).

could trust that the systems, however complex and difficult to understand, would act in the best interest of the user. IoT components are currently not perceived to be fully trustworthy, because humans do not have the possibility to check the true intent of the device. Such **lack of control** often leads to a higher perception of risk connected to the technology. At the same time, a fundamental assumption behind the development of ambient intelligence systems is that progress towards more anticipation and pre-emption of the user's reaction is desirable. However, research has shown that such behaviour is not necessarily in line with the preferences of the users themselves, who often prefer to maintain a degree of control over their interactions with technology (Emiliani and Stephanidis, 2005; Aarts and Grotenhuis, 2009) .These limitations could be potentially overcome by usable and understandable design of the interface in contexts where it is applicable (Køien, 2011; Hochleitner et al., 2012). However, the ubiquity and miniaturisation of the IoT may signify that in most cases this is not a viable approach and further solutions need to be sought, keeping present the necessity to balance elements of human and machine control.

3.2. An ethical and inclusive IoT

In accordance with the principles of the treaties,[37] the Commission aims to make sure that the development of the IoT does not compromise the fundamental values on which European society is based. Furthermore, potential challenges surrounding the social impacts (including impacts on inequalities, social exclusion and the labour market) and the social acceptance of the IoT pose challenges to be addressed through **horizontal initiatives** (Rogers, 2003; Bohn et al., 2005; Gheorghiou and Unguru, 2009; Daskala, 2010). Ultimately, **the business case for an ethical development** of the IoT could be further examined and developed. As mentioned in Section 2, higher standards regarding values (similarly to those relative to data and consumer protection) incorporated in European technologies could potentially give EU firms a competitive advantage in international markets. There is also a deeper advantage – the inclusion of *specific* and *verifiable* 'ethical' attributes in IoT devices and services (eg offering suitable control mechanisms and interfaces that enable consumers to control and modify data that are being collected about them, clarify why and how data are being collected, stored and used) can also raise the awareness of consumers about these issues. For instance, the right kind of marketing of privacy-friendly capabilities can lead consumers to pay more attention to privacy and behave in more consistent ways; the wrong kind of marketing can displace sensible precautions.

[37] Consolidated Version of the Treaty on European Union, 2010 OJC 83/01, (hereinafter TEU).

As mentioned in Section 1, the IoT has the potential to help Europe develop solutions for several challenges faced by society, including ageing and social inclusion, but social acceptance of the technology is a necessary precondition to deploying these solutions. Social acceptance of technology ultimately hinges on the extent to which citizens can understand the technology and perceive it as suited to the expression of their values and priorities. As its characteristics and uses challenge existing ethical concepts and tools (as illustrated by the cases of privacy and informed consent), in the absence of an ongoing societal dialogue about these values and policy that aims to incorporate them into the design of applications, the ethical categories themselves may hollow out, ultimately leading to social tensions.

Another risk is related to the societal effects of the development of the IoT. If principles such as **accessibility and inclusiveness** are not retained in the formulation of policies, technology could exacerbate rather than improve social and digital divides between European citizens of different socioeconomic status.

Avoiding a negative impact of the IoT on **social justice and inclusion** is also a concern felt by the majority of respondents to the public consultation of the Commission: more than 80 percent of them considered this an important issue. At the same time it has been recognised that ensuring universal access to IoT applications, for instance to ambient intelligence, has a vast potential for contributing to a better quality of life of users through stimulating participation in public life and policy; stimulating long-life learning; and minimising the effects of ageing, illness and handicap.

While **digital divides** are already visible in internet use, they are likely to be reproduced and possibly exacerbated with the emergence of the IoT. The **skills** demanded by the IoT are different from those required to use other technologies successfully, as in this case success is not determined by the ability of an individual to operate technology for a specific purpose, but rather her capacity to understand and exploit the potential of the IoT. Therefore, the education of users and the design of interfaces are fundamental to ensuring social acceptance and equal distribution of positive outcomes of technology development.[38] The necessary corollary to education and awareness-raising is the education of people who are active at the back end of the technology; however, engineering communities often do not perceived this.[39]

IoT, risks and the surveillance society

[38] Tapscott (2008) and several of our interviewees from academia emphasised the need to educate children and users to interact with IoT environments.

[39] See Connolly (2011) and Spiekermann (2011); this view has been corroborated by our interview with practitioners and academics.

While the IoT has widely recognised potential to enhance the safety of citizens through applications, for example, in environmental monitoring, national security and crime prevention, it also introduces concerns about discrimination, trust and inequality. The emergence of a society characterised by the possibility of permanent recording of data goes hand in hand with the increasing threat of control – legal and illegal forms of social sorting and **discrimination, surveillance and sous-veillance**.[40] These mechanisms are progressively replacing systemic trust and bear an impact on the distribution of power between individuals and their governments. The fact that IoT-based analytics are predominantly available to governments and companies, but not to their consumers and citizens whose data they manipulate, is at the base of this **inequality**. Furthermore, limits to the awareness and understanding of IoT system by individuals, and the possibility of a function creep between technologies used for a variety of purposes and their possible utilisation for limiting citizen's autonomy, may further increase this difference in the relative power of individuals on the one hand and governments and companies on the other.

[40] 'Sous-veillance' is the use of inferred data for diffuse supervision purposes. It underlines the necessity for a reflection of societal values around the acceptable deployment of technology and data, also beyond concerns about privacy (see for example Callaghan, Clarke and Chin, 2009; Dodge and Kitchin, 2007, Ess, 2010; Spiekermann, 2011).

4. Architecture, identification, security and standards

The emergence of the IoT has posed fundamental questions to the pre-existent systems for architecture, identification and standards and will likely add new dimensions to security challenges at a new scale. In this section we will explore these four technical areas, provide a summary of today's state of play and clarify the relevance and implications for the government of a future IoT.

Several of the challenges faced by networked system architecture of the IoT stem from the characteristics of the 'things' and sensors in the IoT resulting in a more complex set of requirements than the internet. The heterogeneity of applications, environments and systems involved in these developments and a lack of (seamless) interoperability are likely to result in diverse technical and cost issues across sectors; therefore a range of specialist architectures are likely to emerge. Similarly, identification schemes are challenged by the increasing spread of electronic and optical machine-readable tags (RFIDs) and the existence of diverse naming and addressing norms between geographical areas and industries, characterised by limited interoperability as the internet identification system is unlikely to be a vertical sector choice within all industries. These trends, along with the persistence of proprietary identification norms, may lead to a fragmented landscape in identification, while the absence of open platforms may lead to concentrations of power. At the same time, the characteristics of the IoT, the persistence of disparate and divergent security models, paired with an often lacking technical capacity, add novel aspects to pre-existent privacy and security risks while involving a higher than ever number of stakeholders.

4.1. Architecture

The IoT and its architecture have grown up over the last ten years from a set of commercial initiatives, from a variety of industrial stakeholders, as well as a significant publicly funded research agenda, most of which in the EU has been at EC Framework Programme level.

Some of the architectural design has developed out of the internet, but much of the IoT's **architecture is still evolving** either from existing industrial networks, especially existing

identification schemes such as the electronic product codes (EPCs) from identification issuers, or from novel and innovative RDI.

In consequence, the European Commission views the IoT as a pillar of the Digital Agenda for Europe and the 2020 targets. These efforts have produced **a range of architectural research findings and models**, notably the IoT-Architecture project (IoT-A), the CASAGRAS 1 and 2 projects, and others. Importantly, there is currently no single architecture emerging. Note that an IoT architecture can be considered to consist of several supporting pillars, each of which we cover here:

- an architectural model, with its conceptual principles for distributed processing, communications and storage, with its interactions often running across radio links, which require appropriate spectrum (either licensed or licence exempt)
- identification schemes, with naming and addressing systems, to label and find the things (or objects), schemes which are flexible and interoperable for working across multiple namespaces perhaps requiring (network) address translators or naming directories
- safety, security and privacy, which need to be built into the architectural design from day one – and not added afterwards, as the internet has experienced
- standards that underpin the IoT and form the basis for its technical architecture.

In consequence, the IoT architecture is appearing in an evolutionary way, from a variety of disconnected contributions, as they come from multiple stakeholders with different backgrounds and aims.

Multiple current efforts for architectural models are under development, and principal efforts include the Architectural Reference Model from the EU IoT-A project, the EU project's CASAGRAS design, which is more RFID oriented, the ITU-T model, and the Sensei M2M model from the European Telecommunications Standards Institute (ETSI). There is also related architectural design in other international fora – the IETF, W3C and so on – which may also contribute to its design. Moreover, such models have been put forward in the US with the model for a smart grid of the National Institute of Standards and Technology (NIST), and now China is interested in such architectures. All may potentially have a future place.

These sources also include those from the private sector, especially large industrial and ICT players such as GE, Google, Intel, CISCO, IBM; European firms such as ARM Holdings and corporate social responsibility, with components as well as the MNOs; and SMEs such as Neul, standards organisations, academic research and industrial collaborative projects.

Architectural design development is also being shaped by whole industries, through their representative organisations and consortia. The electrical supply industry is especially active with the smart metering initiatives expanding towards smart grids which can support multiple functions from the requirements of smart cities (eg for electric vehicle charging, traffic monitoring, integration of multiple renewable energy sources, or street lighting control) to monitoring networks for river levels and rainfall or energy pipeline controls. For instance, in the US this initiative is being led by the Electric Power Research Institute (EPRI) with its smart grid research and design.

In conclusion, the state of play in IoT architecture is that no common architectural approach has been agreed, such as that which exists for the internet, for instance. No common reference model even is likely to emerge. The best one can hope for is that the various vertical industry implementations will be interoperable to a useful extent.

Table F.1 in Annex F lists the main players in the area, summarising their role, IoT focus and relationships with other bodies.

4.2. Identification

The second technical challenge is to identify the objects connected into the IoT's multiple networks. Identification requires schemes of naming to identify the objects and addressing to locate them, with discovery mechanisms to find new and existing objects. This has governance implications for setting up and managing common systems across industries, technologies and geographies.

4.2.1. The objectives of identification in the IoT

With billions of objects ('things') linked to many different local, regional or global networks, and a lot of them being nomadic or mobile objects, finding the location of and verifying the correct identity of a specific item will be a major problem for the IoT infrastructure. Such identification and authentication will need to satisfy the core requirements of object identification, which involves object resolution, with some form of network addressing in a global context. Identification technologies will form the foundation of the IoT architecture because the essential IoT concept envisions a situation where everything (person or machine) communicates with everything attached. That requires machine-readable identification, so that any object may have an exclusive way of identifying itself to other machines, for 50–100 billion objects.

This needs some scheme of unique addressing, comparable to the internet's URI[41] or equivalent, across networks, functional domains and geographies. If successful, the

[41] The internet uses a hierarchical naming scheme in URLs. Being network location dependent, URLs use and indicate information on where an object is located, associated with a name. This may

identification scheme would create a continuum of sensors, actuators, mobile phones, computers and any object with embedded intelligence. Discovery services would provide sources of information for a particular object to authenticated and authorised users.

Note that such an identification scheme, entailing a vast number of unique identifiers, would require trade-offs between operational objectives of high performance and robustness as well as scalability, interoperability, transparency or network independence, efficiency for very simple devices, preservation of privacy, flexible authentication, reliability, flexibility and extensibility, and support for mobility.

In addition, such a scheme, like the internet or telephone network, should be open to all organisations and enterprises – existing and entering the market – without favour.

4.2.2. Today we have a state of play in identification that is still emerging

To some extent, this state of universal identification is already emerging, but it may not be based solely on one standard identification scheme in the whole IoT. For the internet, a single numbering scheme, IPv6, could make every object identifiable and addressable in the near future, with the spanning capability to contain all the IoT's objects, even if that reached over 100 billion items.

For the IoT, today, a variety of identification standards organisations (and issuing agencies, in particular the International Organization for Standardization (ISO) and Global Standards One (GS1), are at work on schemes in parallel – see Table F.1 in annex F, which lists the main players, their inter-relationships and focus.

One of the most important contenders is the EPC aimed originally at RFID tags, from the GS1 organisation[42] and supported by Auto-ID Labs worldwide, which have researched the field since 1999. It features:

- EPC identifiers, divided into groups, or namespaces, each of which corresponds to a particular subset of items; an identification namespace is further subdivided into sub-namespaces corresponding to different naming schemes for physical objects
- structures to name and locate objects with EPCs, which may be referenced in the Object Name Service (ONS) and Object Directory Service, which are overlay resolution mechanisms that leverage the internet's[43] DNS to

---

make them less compatible with the IoT's mobile environment if there is an overhead of moving between networks and the object name has to change to move from one network to another.

[42] GS1 acts as both an issuing agency and a standards development organisation facilitating the development of open standards of direct relevance to IoT policy.

[43] The Domain Name System (DNS) is the internet name resolution service, designed to translate human comprehensible computer names on a TCP/IP network into their corresponding machine-

carry out naming services and discover information about a product and related services; the identification namespace is generally reserved for EPCs that can be encoded onto RFID tags and for which services may be searched using the ONS; there are questions over the globality of the ONS structure, if national domains could be government controlled, possibly leaving the choice of participants to national interests

- EPC information and discovery services,[44] which complement the above functions.

Note that several EPC schemes are currently defined, most of which support encoding of existing GS1 identifiers, although some EPC schemes are not aligned with these. As new industry sectors consider adoption of low-cost RFID, they must consider whether they can reasonably use one of the existing EPC schemes or ISO application family identifiers.

A further identification proposal, linked to the hopes of the mobile industry, is the use of the existing cellular mobile numbering scheme, the IMSI (COMREG, 2013),[45] a 15-digit decimal string. Every SIM card in every mobile device in the world has a unique IMSI number, which identifies the home country, the home network and the subscriber. Some sources, such as the MNO's industry organisation the Groupe Speciale Mobile Association (GSMA), predict that in the medium or long term, a proportion of IoT machine-to-machine (M2M) applications would run on mobile networks. This rests on the use of ITU recommendation E.212 (ITU, 2008) for IMSI. The identification plan E.212 was originally developed for use in cellular mobile networks (public land mobile networks) to identify geographical areas, networks and subscriptions, and to be used by MNOs only. It may be illegal for other organisations to be issued with IMSI numbers in many countries at this time. The IMSI consists of three fields and defines a unique international identification plan for public fixed and mobile networks providing users with access to public telecommunication services. Thus blocks of numbers may be released by certain regulators for use by other large M2M user organisations, a proposal at this time (COMREG, 2013).

In a nutshell, IoT identification schemes are still work-in-progress. Major developments are expected to progress towards identifiers that are unique in their own spaces and will

---

readable IP addresses. It is also used for email by mail transfer agents and as a general mechanism for locating services in a domain as well as resolving non-standard identifiers (RFC1034).

[44] EPC Information Services, EPCIS and EPCIS Discovery Service for distributed sharing and discovery of notification events between associated partners within a supply chain, an application layer protocol – Extensible Supply Chain Discovery Service.

[45] This document gives figures of a third of M2M communications over cellular mobile connections up to 2020.

also enjoy greater interworking. Some of these may perhaps be based on MNO SIM card IMSI systems assuming that competition issues can be resolved. Greater convergence between existing IoT schemes with internet schemes is also likely (see Appendix C for an example of the encoding of an internet Uniform Resource Identifier in RFID tags – an identification solution for RFID between EPC and URI).

4.3. Security and privacy of the IoT

4.3.1. Security as a public good in the IoT

In this section, we will focus attention and discuss some of the issues pertaining not to security of the IoT infrastructure viewed through the lens as a critical information infrastructure (CII), but rather as a place, or domain, where considerable value is created, exercised and exchanged. This value will be held and exercised through personal data (a more pressing understanding of personal data as the lifeblood of the internet economy) and economic potential made possible by the possibilities for mass fraud of home smart utility networks, mobile e-cash alternatives and so on.

Next, we briefly outline existing governance approaches concerning cyber-security and infrastructure protection as the three main contributing domains to an IoT world, highlighting some of their key characteristics and outlining how these governance mechanisms will need to evolve to take account of the new dimensions of the IoT.

As a starting point, the governance of cyber security at European level is currently managed in a rather diverse way. Complexities of understanding of the meaning of terms remain at the European level (between CII initiatives, cyber crime and defence and national security), and efforts to engage the private sector such as through information exchanges or public–private partnerships (PPPs) meet with mixed results. The network of national governmental computer emergency response teams that has been proposed a number of times since the publication of the Digital Agenda and the Communication on Critical Information Infrastructure Protection (CIIP) constitutes a diverse set of organisations with varying degrees of mandate. Efforts articulated in the 2013 European Cyber Security Strategy to create a network of competent authorities with responsibility for cyber security in the respective Member States constitute a rather ambitious goal because of the diversity in the ways that cyber security is tackled and policy remits across the Member States. There is a mix of regulatory and self-regulatory approaches to setting policy for the governance of security in the private sector. Security is still often seen as a technical issue and there remain challenges in getting companies to adhere to standards (eg the suite of ISO 2700x Information Security Management Standards), to improve the quality of software code and to implement better security (eg many exploits recorded by Microsoft's

Malicious Software Removal Tool have had patches around for one to two years).[46] Recent data from the UK suggest that information security is still challenging (BIS, 2013). There are a variety of formal (eg CEN in Europe) and de facto standards in operation covering security including the ISO 2700x suite of Information Security Management System standards, Organization for the Advancement of Structured Information Standards (OASIS), different cryptographic standards and those for smart cards. The security market is dominated by large US headquartered firms – either those providing a range of security products (Symantec) or those where security is a key element in their products and services (Microsoft; CISCO Systems).

Conversely, the world of infrastructure security is characterised by a different approach that is beset by the security as obscurity paradigm. Technical standards for availability dominate and many sectors (eg energy, transport) are heavily regulated by sector-specific regulations. Organisations such as the US National Reliability Interoperability Council have been instrumental in providing guidance on infrastructure security; the European Supervisory Control Security Information Exchange is another example of an initiative at the European level aimed at improving infrastructure security.[47]

Finally, it is worth mentioning the governance of security and privacy with regard to data protection. Here, the approach may be viewed as primarily through legal compliance, although technology plays a part, for example, in meeting the obligations of data security and user involvement (eg through Do Not Track). Compliance in this domain would seem to be viewed through procedural means in data controllers and data processors leveraging and using personal data: technological *per se* to govern the right to the protection of personal data are limited; the domain is characterised by relatively low levels of automation.[48] Indeed, the regulatory interpretation of privacy by design as a compliance principle rather than a technical route to providing for privacy is somewhat indicative of this worldview.

Given the complexities of security and privacy in the IoT, the role of technical measures to help afford either security or privacy is important (eg Schneier, 2013). By way of exemplar, one key consideration is how privacy enhancing technologies (PETs)[49] might be implemented in the IoT. There is something of a tension between technical measures that

---

[46] Microsoft SIR 2013.

[47] See http://www.cpni.nl/informatieknooppunt/internationaal/eurosCSIE/ (accessed 23 May 2013).

[48] EgFor example, the German government requested that Google offer a paper based letter opt out for Google Streetview when it was rolled out in 2009.

[49] Van Blarkom, Borking and Olk (2003) define privacy-enhancing technologies as a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.

may afford or enhance privacy for individuals and the drive for innovation. The IoT is expected to facilitate innovation through a seemingly endless set of possibilities to explore correlations between different sets of data and then explore ways to monetise this. Exploring if and how a market for PETs might evolve in an IoT world represents a microcosm of the potential for how other competing considerations might be dealt with. Nonetheless, the market for PETs remains moribund because of the simple lack of demand and secondary role privacy plays as a determining factor in consumer-to-business transactions (Cave et al., 2011).

Having briefly summarised the existing state of governance of security across the three main contributing domains in the IoT, we now turn to consider challenges to these approaches posed by the IoT.

4.3.2. Challenges for the future

According to results from consultations, previous research, for example by NIST and the European Network and Information Security Agency (ENISA), the IoT is dominated by a plethora of technical and operational security challenges, not least around the availability and integrity of data generated in an information rich world, the ability of parts of the infrastructure (smart cards and RFID) to meet security objectives and also concerns stemming from the increased quantity of personal data in this domain used as the mains means to extract value. Viewed through the prism of risk, an IoT-centric world has the potential to offer an expanded and diverse range of issues to deal with. In this section, we will outline some of these pertinent issues.

The ubiquity of sensor networks, connected seamlessly to an internetworked infrastructure model, poses some unique and interesting questions about security as a public good.

Perhaps first and foremost is the explosion in the number of entities (companies and authorities) that will each play a role in helping to meet security objectives. As we shall see later in this report, not only must they be able to understand security in an all hazards approach (not just about loss of personal data, or loss of economic value as a result of fraud) but also be able to exchange a wide variety of security telemetry across domains. Approaches to persistent security will need to be developed that are valid across multiple competing domains with different security priorities.

We may see an extension of the modus operandi for cyber crime evolve. Just as large volume, low value cyber crime (in the form of phishing) is the favoured modus operandi of choice, exploiting vulnerabilities in the browser, so the possibilities of the IoT may result in the evolution of attacks against diverse endpoints (car, home, etc) be the new targeted endpoint. How will security models from cyberspace (eg cookies, browser security, anti-phishing, anti-spam models) translate, if at all?

At the enterprise level, the security issues become related to the explosion of diverse entities handling data and having a security stake, from service providers (including infrastructural providers) to intermediaries and others for whom the market for data from the IoT has not yet been identified. This means that federated security, made possible through standards-based approaches (such as OASIS but also via eIDM), will become more important, as will achieving inter or cross domain security.[50]

How will the nature of crime change? How will the motivation of cybercriminals change from low value broad mass crime (phishing) to targets where there are more and more diverse types of value to be exploited? Will the browser be replaced by the fridge or the car as the vulnerable point?

Concerns over privacy revolve around whether IoT devices are suitably secure from eavesdropping, whether the possibilities for onward use of data, beyond that which has been 'consented to', are in opposition to the EU legal and regulatory framework governing privacy and data protection. Many concerns revolve around the changes brought along by big data analytics, supported and empowered by the IoT (explored in more detail in Section 2). These concerns include whether consumers will be able to exercise 'control' over their data, or whether they will become the unwitting participant of a world that neither respects nor needs their consent. The issue with the IoT is that the number of organisations that see possibilities of use of personal data is exponential, and impossible to predict *ex-ante*, given the emergent and dynamic possibilities of data analysis.

The efforts of law enforcement will require more holistic linkage between physical and cyber-crime competencies since the implications and targets for those seeking to commit crimes will become all the more diverse and complex.

The complexity of managing the CII shows how difficult it is to coordinate approaches to deal with cyber, physical and personnel risks to infrastructure. It is difficult to say whether the approaches of the Netherlands, where these are separate but linked, or the UK, where they are more centrally harmonised, are more or less effective. The IoT will require a much more joined-up effort with regard to security regulation. Links between the regulators or those with a mandate for security at the national level and those responsible for security in heavily regulated sectors (eg energy, transport) will need to be better understood. The relations that will need to be put in place with the proposed competent authorities foreseen by the Network and Information Security Directive will need to be elaborated if they are to remain valid to tackle IoT-related challenges.

In an IoT world, there may be more opportunities for PETs to be implemented in different forms (physical as well as digital) but also paradoxically less incentive for

[50] EgFor example the work of Creese et al. (2009).

consumers to take them up. Indeed, in addition to technical measures, we may see the evolution of a broader market of privacy agents (either human or automated) that mediate users' privacy and data protection across a range of devices in both physical and cyber space. Such a development is not that far fetched: the Platform for Privacy Preferences (P3P) is essentially trying to do the same thing but requires more intervention and education on the part of the user. In an IoT world with a multiplicity of digital and physical objects, the sheer complexity could well result in market developments of such mediation services or technologies. this will result in even more thorny legal and regulatory questions (can such automated agents be classified as 'data controllers', for example).

4.4. Standards for the IoT

4.4.1. Standards as part of the governance structure of the IoT

Standards are a form of collective intellectual property right. In relation to the IoT we distinguish three different functions:

- Standards provide a basis for the open interoperability that lies at the heart of the IoT value proposition – standards that define technical and logical conditions governing connections and information transfer allow objects to communicate and interoperate.
- The adoption of standards creates explicit or implicit barriers to entry – non-compliant devices will not be able to 'work' with the rest of the IoT and will fail to provide the expected benefits to device owners, limit the functionality of system-level services, create additional vulnerabilities or system risks, and exacerbate congestion and other network problems.
- Standardisation bodies create a platform for the discussion of cross-cutting issues and implementation of coordinated activities including innovation[51] (new standards and new devices, services and so on that employ the capabilities provided by the standards), integrated service provision and organisation of self- and co-regulation.

[51] The standards developed for the IoT necessarily cross existing sectoral boundaries. For example, electronic appliances and large-scale retail trade currently constitute separate industrial sectors, in terms of standards and business models, as well as in terms of the goods and services produced and the firms involved. However, without a set of common technical standards and interfaces (at device and semantic level) to facilitate their interoperation, loT-enabled devices like the smart fridge could not develop.

IoT standards can be applied at different levels in the IoT. These include individual 'things' and their properties; binary interactions and linkages among things;[52] and systems, subsystems and assemblages.

Furthermore, standards can be classified according to the things they control, the items to which they pertain and the connections among them. For instance spectrum standards may control various aspects of IoT applications, including spectral bands used,[53] power, location, other aspects relating to interference, and 'handshaking (eg for agile or cognitive devices).

Within this broad scheme, IoT standards continue to be developed in a range of areas:

- data encoding
- air interface
- testing
- security
- privacy
- application standards
- power use and dissipation.

For RFID standards are developed for:

- working conditions
- label size
- label position
- data elements
- format
- frequency bands, which have implications for operational mode, storage and so on.

Adapting standards an IoT context

Looking ahead, standards developed for RFID, for instance, may need to become broader, more functional and/or less technology or function specific if they are successfully to be applied (taken up, used, open) to broader classes of objects (already visible for NFC). Standards may need to be promulgated above the level of things to encompass fixed or ad hoc assemblages, networks or ensembles of interacting and intercommunicating things. Standards optimised for existing interactions (primarily identification and simple

[52] These are not the same; a linkage is structural or latent, while an interaction (eg remote instruction, query or data exchange) is dynamic and active.

[53] These are obviously related, and may also be expressed in other mechanisms (such as licensing conditions or (tradeable) spectrum use rights.

information-sharing) may need to evolve to support more complex interactions and system functions. By the same token, standards applying to the IoT aspects of internet-capable objects may need to be reconciled to other functions of those objects (in cases where existing standalone devices and objects are brought into the IoT rather than designed to work inside it).

The relationship between standards and other challenges

Standards applying to the IoT (or the IoT implications of other standards) affect the other challenge areas discussed in this document:

- Competition: The competition and other broader policy aspects of standardisation processes (ranging from the standards themselves to the mechanisms for proposing, modifying, approving, promulgating, monitoring and enforcing them) also need to change as the complexity of the objects and their interactions increases. To take a simple example, standards applicable to the technical or communication aspects of devices used to carry out financial transactions or to search for information used to support decisions may be able to exist alongside standards governing those functional aspects, but it may be that the enforcement of technical standards is the best way of handling functional issues or vice versa.
- Identification:Standards can facilitate (as well as prevent) identification and enable egmutual recognition schemes or federated identity, for example.
- Privacy: Standards control the way data are transmitted, recorded, processed, retrieved and shared. Standards relating to processing and the ability of remote systems to trigger software deepen the 'data control' aspects of security, and the interface (eg when activity records are hashed with identifiers).
- Architecture: IoT standards may be used to give concrete form to architectural principles and to design specifications; they may in this sense be useful 'vectors' for spreading such principles. This stands in contrast to egarchitecture and design of egbuildings, for example, which tend to be more autonomous and isolated, competing with other designs or architectures primarily through downstream (uptake) selection.
- Ethics: IoT standards may embed ethical considerations; what kinds of decisions 'things' can make and how they protect people via 'rules' (eg a version of Asimov's Laws) or hardwired functionality (eg privacy, security or information minimisation by design).

- Governance: Standardisation is a form of governance; moreover standards can complement, substitute for or conflict with other forms of control and deliberative, reflective or reactive governance.

4.4.2. Current state of play

A wide range of standards bodies are actively engaged in producing standards for the IoT and in adapting existing standards to cope with IoT specifics. Table 4.1 provides a list of some current IoT standards.

Table 4.1 Sample of current IoT standards

Standard	Objective	Status	Organisation	Comm. range (m)	Data rate (kbps)	Unitary cost ($)
EP	Integration of RFID technology into the EPC framework, which allows for sharing of information related to products	Advanced	GS1	~1	10^2	0.01
GRIFS	European coordinated action aimed at defining RFID standards supporting the transition from localised RFID applications to the IoT	Ongoing	EC, CEN	~1	10^2	0.01
Various	Technical standards: frequencies, modulation schemes, anti-collision protocols	Ongoing	ISO	?	?	?
M2M	Defnition of cost-effective solutions for M2M communications,	Ongoing	ETSI	?	?	?

	which should allow the related market to take off					
6LoWPAN	Integration of low-power IEEE 802.15.4 devices(sensor nodes) into Ipv6 networks	Ongoing	IETF	10–100	10^2	1
ROLL	Defnition of routing protocols for heterogeneous low-power and lossy networks	Ongoing	IETF	?	?	?
NFC	Defnition of a set of protocols for low range and bidirectional communications	Advanced		~10^2	<424	0.1
Wireless Hart	Defnition of protocols for self-organising, self-healing and mesh architectures over IEEE 802.15.4 devices	Advanced		10–100	10^2	~1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced		10–100	10^2	~1
ISO/IEC 18000	Covers data encoding, air interface, testing, applicative	Advanced				

standard in 5
frequency bands
(below
135KHz,
13.56MHz,
2400–
2483.5MHz,
860–960MHz,
433.92MHz)

In addition, IoT-specific standards, internet standards and those that may arise in other domains will either expand or compress the niches within which the IoT may develop. Moreover, standards transposed to the IoT from other domains or arising within it may determine the balance of power and the effective functional, economic and societal performance of the IoT.

4.4.3. Challenges for the future

Taking this context into account, the current development of IoT standards raises a specific set of future challenges:

- Will these separate initiatives and the competition between alternative standards to which they give rise produce the network of standards needed for the most effective technical, economic and societal functioning of the IoT?
- How should IoT standards balance current performance against innovation, interoperability against independent competition, and technological against functional specificity?
- What standardisation bodies and processes are needed in order to permit these standards to emerge – should these bodies be specific to the IoT??
- To what extent will existing standards bodies and the incentives operating on stakeholders distort standards development?[54]
- How can independent, open and 'neutral' standardisation be balanced against and integrated with other modes of governance?

[54] The distortion could lead to standards that have disguised trade barriers and are too light, too proprietary, too difficult to comply with, too easy to violate, too anticompetitive, too harmful to innovation and public service delivery, and too much biased against small enterprises.

PART III Defining the problem

5. Problem statement

From the analysis presented in the preceding sections, we can derive the following problem statements:

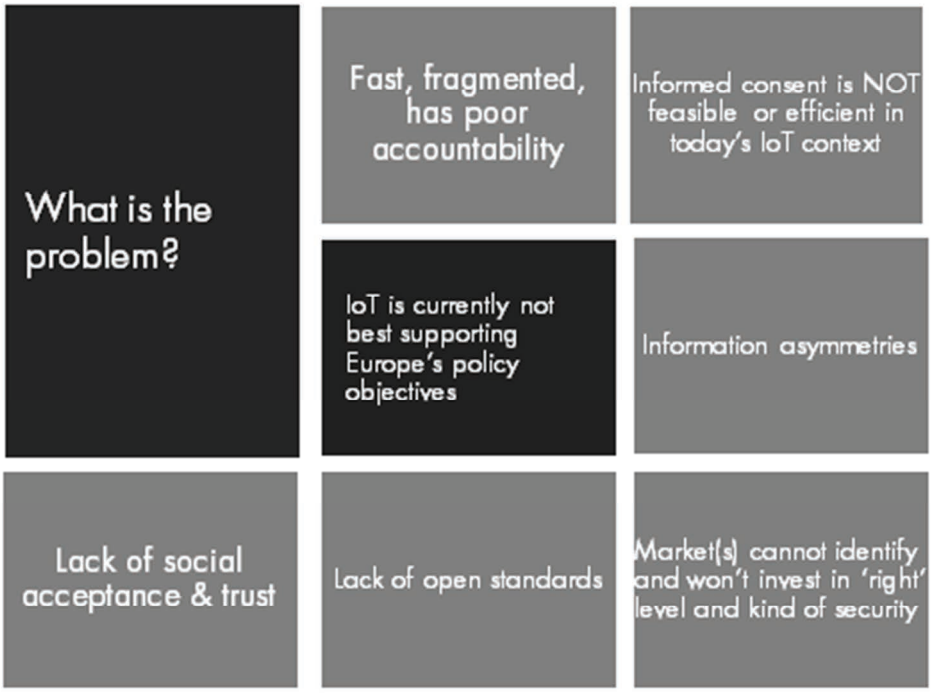
- The IoT currently may not be developing in ways that support Europe's policy objectives, respond to European influence, and can be easily reversed or adjusted once IoT matures.
- Fast and fragmented development could lead to poor accountability: Although the technology is projected to develop fast, the IoT is also fragmented along several lines and the system as a whole often demonstrates a lack of accountability. Although impacts of the technology on citizens and society as a whole can be very significant if the IoT is deployed in key sectors, such as health or energy, there is at present no clear framework for determining responsibilities in IoT settings, where devices are often given co-decision powers. Although so far it has been assumed that individual empowerment was capable of creating self-correcting systems – that expanding the range of choices available to individuals could adequately address any arising problems – the main characteristics of the IoT exclude the possibility of relying on informed choice, which had been the principal tool employed to support individual empowerment.
- Besides, the market for IoT may present several barriers to entry and competition as well as IoT-specific market failures at all levels of the IoT value chain. Market failures come from a variety of sources. It is a result of imbalances of market power due to the legacy of dominant players in internet and data processing and the presence of externalities and public goods such as security, trust and control. Moreover, although security, innovation and market developments interact in a dynamic manner, information asymmetries between consumers, providers and government created by obscure and complex systems could make it more difficult for the market to quantify, price and allocate risk. Therefore, they might impede the IoT market to operate at a societal optimum (compromising Pareto efficiency).
- In addition, a lack of open standards may can create ulterior barriers for SMEs, innovation and platform competition.

In virtue of its particular defining features (as listed in Figure 1.1), the IoT introduces new aspects to pre-existing ethical tensions, for instance questioning the legitimacy of informed consent as a basis for action (beyond responsibility mentioned above) and individual rights related to data use and protection. A possible decrease in the **relevance and reliability of the concept of informed consent** will require joined-up intervention involving business, government and civil society.

Finally, markets have been found **not to incentivise players to invest sufficiently in adequate levels of security**. Safety, social acceptance and trust in the technology so far has not been unequivocal and the operationalisation of ethical principles in an interface-less environment is likely to present further challenges as applications will be rolled out in consumer markets. Therefore it can be concluded that market developments likely cannot be relied on to answer these challenges automatically.

Figure 5.1 sets out some of the potential problems arising for the IoT.

Figure 5.1 Potential problems arising for the IoT



5.1. Key stakeholder perspectives

The previous sections have dealt with the key challenges identified for the European Commission, but it is important to keep in mind that these challenges do not impact in the same way on all stakeholder groups. In order to be able to appraise the impact of eventual EU-level policy interventions (and define recommendations for one that balances the needs of these groups), the relative incentives of stakeholder categories have to be incorporated in the discourse. In the following sections the needs and issues identified

above will be briefly examined from the point of view of four key stakeholder groups: regulators, businesses, the government and individuals.

5.1.1. Legal and regulatory perspective: managing resources and ensuring competition

The IoT brings with it new players and non-traditional markets, changing the landscape within which national and supranational regulatory bodies (eg competition agencies) operate. Anti-competitive behaviour and other sources of market failure must be kept at a minimum. **New strategies may be required to manage common and often scarce resources**[55] better and shelter them from anti-competitive predatory behaviour. **Removing the limits to open and balanced**[56] **competition** in potentially and efficiently competitive layers of the IoT is essential. This may involve a combination of reducing entry and exit barriers (to encourage entrepreneurial rivalry based on the merits of the services offered) and standardisation to ensure that network externalities do not result in excessive 'tipping' towards a dominant provider or technological paradigm. Otherwise, strategic investment, bundling and other practices may enable large firms or cartels to form and abuse market power, particularly if vertical coordination or integration would lead to exclusive or near-exclusive control of the entire supply chain. Ensuring open access to shared infrastructures where this is possible will be important. Note that this suggests measures such as structural separation, 'must carry' or essential facility regulation and so on as well as measures to promote competition.

Similarly, a **balanced approach to access and exploitation of intellectual property rights** in the IoT infrastructure will help thwart market dominance and abuse of market power.

As devices multiply and diversify, and become more critical to sustaining life and livelihood, **legislative requirements for equipment approval** may need to be considered.

Given the ubiquity of information access, storage and delivery, better mechanisms for **protecting citizens** from privacy violations (such as profiling and excessive data retention) are vital. In this context, rules must be enforcement-oriented and corporate accountability and liability reconsidered. Furthermore, an always-on IoT environment will require a review of **universal service provisions**.

---

[55] Such as numbers, addresses and radio spectrum; these are often scarce as a result of the considered and strategic actions of stakeholders, who will invest in scarcity at every turn because it generates rents.

[56] We cannot assume that competition should be preserved and monopoly stamped out in every case: where there are large fixed costs or strong positive network externalities, competition may be inferior to regulated monopoly is preferred; collusion may be as big a problem as monopoly; and competition for markets (extensive competition), which bypasses monopolistic power, may be better (in a Schumpeterian sense) than competition in the market (intensive competition).

Finally, increased emphasis on **cyber crime and cyber security** is needed as cross-border activities continue to increase and new applications rapidly flood the market. Both proactive and reactive mechanisms may be required, and legislation must facilitate enforcement and reduce ambiguity to the largest extent possible.

5.1.2. Business perspective: ensuring efficiency, investment and skills

Market regulation has to enable firms to grow while preserving competition

For an IoT business model to flourish, consistency in policymaking for the creation of sustainable markets and viable businesses is critical. The IoT will be highly dependent on a well-regulated market, but this may not imply that a formal regulator is necessary. To the extent that formal regulation is needed, it should be based on clear principles and focus on promoting (static and dynamic) efficiency and equity rather than on the number or sizes of firms involved. This holds true, and perhaps even more so, for the fast-moving IoT. For example, this concept of 'regulatory fitness' mirrors that behind the current Regulatory Fitness and Performance Programme (REFIT) initiative being implemented across the European Commission.

The playing field for IoT-related markets is not entirely level: some entry and exit barriers and some degree of differential treatment are probably necessary in order to ensure an appropriate mix of static efficiency (low costs, improved value and minimisation of monopolistic or collusive distortions) and dynamic efficiency (the right pace and kind of innovation and investment). This may be correlated with firm size, but it should not be assumed that large (respectively small) firms are inherently less (respectively more) innovative; this will vary by region and 'layer' in the IoT and will reflect framework conditions including regulatory structures and financial markets.

IoT businesses are in need of adequate investment models for growth and innovation

Access to suitably configured venture capital can provide the right incentives for innovation as can government subsidies, targeted public procurement, PPPs, innovation contests or changes to the intellectual property rights (IPR) system, or a greater degree of coordination among policies affecting the IoT *per se* and those affecting 'use case' areas and award programmes for young entrepreneurs at schools and universities. However, such measures are no panacea; they will solve some problems better than others and may easily have perverse consequences.

Building the IoT skillset

Access to the right skills and expertise on the supply and demand (user) side is essential, as is access to technology and infrastructure. Openness of standards and technologies must not be wholly sector-specific, but should – in some cases – cross sectoral boundaries in an IoT world. However, in light of the very real risk that the specific requirements of the most

'important' sector will dominate to the detriment of other sectors with different needs for standardisation (eg around security, integrity and so on), there is a need for a balanced suite of specific and generic standards, just as the architecture should combine generic enablers and specific services, as with the current Future Internet Public Private Partnership (Hoorens et al., 2012), for example the use of standardised RFID meter tags in a wide range of utilities.

Ethical marketing models in an IoT world

In mature markets, businesses need innovative delivery models and unique value propositions to attract and retain customers. One component of such a business proposition that could align competitive forces with the ethical issues discussed in Section 3.2 could be a form of marketing based on 'ethical IoT technology' to enhance branding and increase customer bases, much like the 'green tech' revolution of the last decade. In this context, an understanding by businesses of user apprehension and related needs will foster better brand and service positioning within the **full IoT human interface environment**. This in turn may have positive effects on the ethical content of market innovation and business profits. There is also a deeper advantage – the inclusion of specific and verifiable 'ethical' attributes in IoT-related devices and services (for example suitable interfaces as highlighted in Section 3.2) can also raise the awareness of consumers about these issues. For instance, the right kind of marketing of privacy-friendly capabilities can lead consumers to pay more attention to privacy and behave in more consistent ways; the wrong kind of marketing can displace sensible precautions.

Finally, as noted in Section 2, the scope for regulatory intervention should adapt existing policies to the specific requirements of competitiveness and the need to address IoT-specific forms of market failure stemming from egdistorted competition, limits to consumer sovereignty, abuse of two-sided (platform) market power and collusion, for example.

5.1.3. Government perspective

Protecting citizens and safeguarding the public interest should be a prime concern of government, which in the context of the IoT and big data means **standardising citizen interactions** in the IoT for safety, security and privacy, providing this does not compromise liberty, diversity or effectiveness. It is aided[57] by the **development of an informed, educated and skilled populace** capable of navigating their way through smart connected cities and dealing with autonomous objects in their path. In particular, the development of intuitive interfaces that allow citizens to protect their freedom of

[57] But it must not rely on this; not all citizens will or should be required to reach this standard.

information, freedom of expression, and civil liberties must be ensured.[58] Because of the potential for misuse, citizens' concerns as listed above must be taken into account when providing business incentives, monitoring competition and strengthening the complementarity between competition and consumer protection.

Government can harness the potential of **leading by example**. To this end, it would be valuable for government to provide incentives to its different branches and departments to adopt IoT services for their own activities with a view to developing and perfecting safe and intuitive e-government services. Demand-side instruments are valuable, but should start from a clear definition of **how public IoT services differ from non-IoT services used for the same purposes and how they might overlap** with non-government ones in ways that can 'lift' the offers available to citizens in the market.[59]

This might be best achieved through **partnerships** with the private sector, possibly involving a mix of small and large enterprises providing innovation, enterprise and capital at different points in the value network and a range of public sector service users.

5.1.4. The user–citizen perspective

The user interface and user education

Ordinary IoT users need both the tools and the capacity to realise and benefit from the IoT. For everyone to use and benefit from the IoT, this demands some form of intuitive human interface and educational processes in combination with this, appropriate to the person.

Only these two factors can offer an inclusive IoT world – where all users gain. Campaigns to raise awareness are required and even possibly some forms of digital literacy and re-skilling programs. Without this, the human interface barriers may diminish the benefits of the IoT as a whole. For instance a smart grid with home area networks for smart meters can display temperature or energy consumption and control the heating programme, but the householder must be aware and sufficiently educated to use it. Naturally, there will be more specific citizen needs (eg for the mentally or physically disabled) as distinct from consumer needs, as EU regulators recognise already.

Disability, vulnerability and the IoT

Gaping divides in social inclusion are already visible in today's digital world, illustrated by differences in internet access and skills along socioeconomic, health and other

[58] In ways that do not compromiseeg freedom from terrorist attack, hate crime and fraud, for example.

[59] Governments, businesses and citizens are regulated in different ways; therefore the freedoms or constraints that will develop in a 'launching customer' government use of IoT may not be practicable or appropriate in the market or society more generally.

determinants (European Commission, n.d.).[60] Serious questions are raised concerning the protection of the mentally and physically disabled in a world that demands conformance to models of behaviour imposed externally. At the same time, complete dependence on IoT may demand comprehension of complex concepts and tools for the adherence to such models, and indeed for survival itself.

In accordance with the fundamental values of the European Union, additional effort may be needed in order to prevent the creation of new disparities and to thwart further polarisation. Lack of intuitive interfaces, as mentioned above, combined with a consistent lack of educational programmes may exacerbate societal ills such as deprivation of rights and social isolation, as well as alienation, stress and psychological problems.

User consent

Our legal and regulatory structure and most formal governance is based on informed consent – the implied responsibility of individual users to make up their own minds. However, in an IoT environment, the points at which data, notably elements of data aggregation, and analysis (termed 'mining' or big data) become or cease to be 'personal' is increasingly blurred, if such a distinction can be said to exist at all. Thus, a further area for concern is the ability to provide consent in a meaningful manner to protect personal data against unlawful processing. As highlighted by experts interviewed for this study, policymakers may need to breathe new life into the notion of informed consent.

User delegation and automated decision taking

Delegation or contractual assignment by the user for the reallocation of tasks, activities, decisions, liability and responsibility – sometimes by explicitly agreeing but sometimes not – is one vision of the IoT. Powers of action and accountability may shift away from their original human owners and institutions towards machines. Our European society expects individuals to take responsibility for their own interests. Over-delegation of responsibility for a citizen's quality of life so that it is entrusted to regulators, product designers and so on may lead to inappropriate restriction of human responsibilities. This applies equally to the delegation of interests, which should only be made to suitable parties, with guarantees of appropriate oversight. For example, decisionmaking algorithms built into connected autonomous objects should place the interests of users above those of the IoT services, raising questions about the fundamental purpose and guiding principles of robotics. Furthermore, an environment that relies too heavily on automated decisionmaking risks being at odds with fundamental rights. Evidence and impact of disastrous transfers of responsibility (and rights) would deter the market and users. So any decisions on

[60] This is illustratedeg for example by the Digital Agenda Scoreboard, which tracks progress against the goal of ensuring that 60% of disadvantaged people in the EU use the internet regularly by 2015 – a goal not yet achieved. See European Commission (n.d.).

delegation must recognise the importance of individual freedom rather than being systematically relegated to the lowest levels of the needs hierarchy (eg an object or agent). Automated decisionmaking must not occur without user education, consultation and awareness of its being used through explicit warnings.

The right to be forgotten

The potentially permanent nature of recordings in a digital world, regardless of the anonymising effect claimed for data aggregation (big data), could lead to undesirable and illegal forms of social sorting, discrimination and surveillance. Freedom of information principles respect the right of control by the citizen, plus the right of access to and deletion of details both online and offline. Only with full exploitation of such laws can the 'right to be forgotten' be effective and enforceable, covering both the physical and virtual domains. This right also implies some responsibilities by the individual, and may require clarification of rights and responsibilities of all actors and a new form of 'social contract', one designed for the digital age.

PART IV The case for action

6. Competence and policy objectives

6.1. Competences

The problems and issues arising from IoT development are linked to a wide range of objectives identified in the Treaty on the Functioning of the European Union (TFEU).[61] Some of these involve areas of exclusive EU competence:

- the functioning of the internal market
- common commercial policy
- protection of fundamental rights, with particular reference to the protection of privacy and personal data
- potentially, in view of the global scope of the IoT and the potential benefits of international alignment on IoT governance, the conclusion of an international agreement when this is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as such a conclusion may affect common rules or alter their scope.

In this sense, the competence to act to ensure the functioning of the internal market seems to justify EU policy initiatives on the IoT. Without EU intervention, national policies may develop in diverging ways, including by introducing varying legal requirements for IoT operators and end users, and creating barriers to the correct functioning of the internal market. To ensure an integrated market that operates homogeneously (and thus stimulates development of the European IoT market) and to ensure high levels of consumer protection, policy intervention at the EU level may be necessary and proportionate, as these are objectives that a Member State and the market could likely not achieve without EU policy intervention. Other objectives examined in this report involve areas of shared competence:

[61] Consolidated Version of the Treaty on the Functioning of the European Union, 2008, OJC 115/47.

- social policy, for the aspects defined in the Treaty (eg labour conditions[62] and occupational health and safety,[63] which may be affected by workplace use of IoT devices and systems)
- consumer protection (especially informed consent when subscribing to IoT services or using them to make purchases)
- transport (to the extent that IoT applications are used to identify or control vehicles, eg driverless cars)
- trans-European networks and energy (especially in conjunction with smart meters and grids.

In view of the (currently) fragmented and dynamic nature of the IoT and its defining potential to support the ubiquitous interoperability of a wide range of 'untethered' devices, action at Community level may be necessary and have the potential to deliver European added value that could not be achieved by Member State action alone, more specifically:

- The potential problems raised by the IoT (see Section 5) potentially cannot be dealt with satisfactorily by Member State action alone because of the global scope of the IoT sector, IoT-enabled markets and the IoT-derived information flows and the fact that national markets and systems (eg telecommunications systems) are open to low-level and fragmented penetration by devices and software coming from the entire globe.
- Actions by Member States alone or the lack of Community action might conflict with Treaty requirements by increasing the risk of market fragmentation or discriminatory treatment of specific stakeholder groups (ranging from small firms to socially marginalised groups).
- Actions by Member States alone or the lack of Community action might significantly damage the interests of Member States if standards, access restrictions or traffic management measures restricted the free circulation of goods – particularly the 'roaming' movement of devices and data.
- Action at Community level could produce clear benefits compared with action at the level of Member States by virtue of scale effects. European action could deliver these benefits through a larger installed base of interoperable devices, better opportunities for integration with other layers of the Single Market and reaching critical mass in innovation. Increased connectivity could enable in enhance device and data mobility and thus ubiquity of access to the whole spectrum of IoT-provided benefits.

[62] Article 153 of TFEU.

[63] Article 156 of TFEU.

> Finally, extending the scope of the technology could enable the rich variety of use cases and business models arising in different national contexts to be fruitfully generalised or localised to other regions. Action at Community level should also be more effective than action at Member State level because of the greater reach and power of pan-European monitoring and enforcement, and the potential of policy along the lines indicated in Section 8 to create a common 'floor', which would enable competitive forces and collaborative partnerships to produce integrated changes in the IoT *per se*, IoT-using markets[64] and legal, regulatory, standards and financial[65] framework conditions.

6.2. Policy objectives

In view of the rapidly changing, global nature of the IoT and its complex linkages across sectors, regions and stakeholder domains, it would be premature and possibly counterproductive to design elaborate, direct, immediate and targeted interventions. Indeed, as noted in Section 6.1, many aspects of the problems identified above lie in areas of shared competence and may ultimately be addressed by some combination of Member State action, private market initiative, civil society or citizen activism, and multi-stakeholder co-regulation and other forms of joint action. But this does not automatically mean that the Community should simply wait for an opportunity to contribute by its own actions or through harmonisation. Several stakeholder participants in the workshops held as part of this study and others interviewed coming from government, business and civil society stressed the detrimental effects of uncertainty, and suggested that a combination of leadership and commitment was essential. To frame the discussion of possible policy interventions, therefore, we begin by discussing general objectives derived from the problem statement and the case for action. In view of the breadth of the issues involved, these should be seen as characteristics of the desired 'landing place' for the IoT rather than specific or operational objectives, which will necessarily differ with the specific measures, issues, policy domain and key actors involved.

The desiderata for the IoT represent valid policy objectives in the sense that its current evolution suggests that they might not be achieved without intervention and that such intervention should be undertaken at Community level (see Section 6.1).

6.3. Strategic objectives for IoT policymaking

In this section, we will elaborate on the strategic policy objectives identified by experts interviewed for this study: accountability, interoperability, inclusivity, ethical soundness,

---

[64] Goods, services, business models and market structures.

[65] Including the ability to spread risk across approaches, sectors, firms and regions.

safety, openness, and effective and efficient competition and competitiveness (see Figure 6.1).

Figure 6.1 Strategic objectives for policymaking for the IoT

6.3.1. Accountability

General objective: the IoT should be accountable to all its stakeholders, in order to ensure that their choices and activities are consistent with their interests and common European objectives. To attain this, stakeholders at all points of the value chain should have access to relevant, meaningful, accurate and trustworthy information that enables them to make meaningful choices.

Specific objective: to clarify stakeholder responsibilities and liabilities in order to ensure that their decisions are aligned with collective interests.

Operational objectives:

- to ensure that the monitoring of compliance with regulations and societal norms is comprehensive, effective and accurate and to take steps necessary to ensure that rules and obligations are enforced; for example, the effective application of privacy rules to the IoT requires data subject notification in the event of breaches, but further clarity is required regarding the actions different IoT stakeholders must take in order to screen for potential breaches, identify the extent and parties involved, and notify the affected parties and authorities; this is more complicated in the IoT than on the internet per se, because data may be lost or collected by devices or ad hoc

assemblages rather than single systems or organisations; likewise, the roles of data controllers, data processors and the competence of data protection authorities to detect non-compliance and take appropriate action may be weakened; at least, the cost and adverse performance consequences of the protections available on the internet per se may outweigh their benefits

- to ensure effective and efficient allocation of liability and responsibility to devices and human–device interactions, for example, in the event of decisions or actions by such entities that lead to harm, whether 'intentional' or not; in this case, it may not be possible to define a responsible 'owner' of the IoT entity and legally justifiable or efficient to hold such an owner responsible under criminal, contract or tort law[66]
- to align accountability where possible with the obligation to provide understandable information on IoT products and services and with the power to act, for example by substituting disclosure obligations and other 'informational remedies' for inflexible and possibly unenforceable formal obligations, or at least by attaching such informational obligations more clearly to IoT product or service provisioning.

6.3.2. Interoperability

General objective: to ensure appropriate levels and kinds of interconnectivity and interoperability among the myriad devices and systems comprising the IoT.

Specific objective: to engage with architectural and standardisation processes and entities whose decisions will determine the potential for interoperability and to ensure that actual interconnection and interoperation are consistent with other policy objectives.

Operational objectives:

- to assess the value of a coherent architecture policy that guarantees interoperability across all vertical sector domains[67] and take steps to support its implementation
- to harmonise initiatives towards technical interoperability among IoT devices and enterprise or organisational interoperability
- to develop tools and methods for assessing the positive and negative impacts of interoperation and devising appropriate remedies[68]

---

[66] This is particularly problematic when no single device can be found that caused the harm – when harm arises 'in the system.'

[67] While at the same time ensuring adequate safety, security and privacy are built in to any instances of any architecture and minimising market foreclosure or the use of interoperation to facilitate collusion.

- to assess the expected impacts of interventions on the volume market for low-cost interconnection that the business case for the IoT requires.

6.3.3. Inclusivity

General objective: to improve social inclusion by removing barriers to participation and enhancing ubiquitous digital skills.

Specific objectives: to ensure that citizens and consumers alike are informed, educated and empowered to optimise benefits and manage risks and to ensure that citizens are not 'locked into' or 'locked out of' the IoT.

Operational objectives:

- to support the development of inclusive[69] software, hardware and systems approaches to improving access to the IoT
- to support the development and deployment of IoT solutions to problems of internet and societal access and inclusion
- to strengthen digital skills through education and awareness-raising, thus increasing the number of end users who can responsibly use IoT solutions and benefit from them in an optimal way
- to assess and where necessary take steps to strengthen the availability of finance at all levels in order to facilitate the creation of an IoT-enhanced next generation private or public infrastructure for services of general public interest (including energy supply, health services, care of the aged and infirm, transport, cities and water supply).

6.3.4. Ethical soundness

General objective: to ensure that the development of the IoT and any policy interventions undertaken to improve it are consistent with the EU Charter on Fundamental Rights.

Specific objective: to develop the theory and practice of ethics by design in order to protect against inadvertent breach of fundamental rights, and ensure that such breaches are visible and that appropriate levels of trust are supported.

Operational objectives:

- to ensure that fundamental values and norms are properly transposed to the IoT

---

[68] The point here is that low-level interoperation and information exchange may facilitate collaborative innovation and service delivery or collusive market manipulation and exclusion. Standard legal remedies (eg prohibiting certain kinds of coordination or communication) and processes are inappropriate for the scale and speed of the IoT.

[69] EgFor example, accessible, easy-to-use and inclusive-by-design are common features of inclusive technologies, eg in AAL.

- to take steps to ensure that protections are proportionate and balanced, and cover the full range of rights affected by the IoT, including social inclusion and human rights
- to facilitate an effective mix of technical and compliance approaches to ethics by design
- to encourage appropriate levels[70] of trust eg by designing suitable mechanisms and interfaces in order to stimulate take-up and social learning about the specificities of trust in the IoT.

6.3.5. Safety

General objective: to ensure that the IoT is a safe environment in which users and other participants are not exposed to undue, non-transparent and unmanageable risks without due consent.

Specific objective: to influence the development of the IoT in a way that identifies and minimises safety risks specific to the IoT domain and confounding effects on risks in other areas (eg health, transportation, commerce).

Operational objectives:

- to ensure that adequate safety, security and privacy are built in to (any) instances of any IoT architecture
- to encourage development of a shared model for security risk identification and governance encompassing emergent and dynamic physical and electronic risks (as well as hazards)
- to facilitate an effective mix of technical and compliance approaches to privacy by design and security by design and an effective means of balancing privacy and security
- to facilitate knowledge sharing and coordination with regulatory actors in other sectors that will be affected by IoT
- to avoid over-reliance on automatic, generic and systemic safety measures that might be (or become) unreliable or 'crowd out' user precautions.

6.3.6. Openness

General objective: to ensure that the IoT remains open to new hardware, software, services, business models, market and contractual forms and stakeholders.

[70] This does not assume that more trust is always better, that trust in machines and systems is the same as trust in human beings or that trust developed in other contexts (eg the internet at large) should always be transferred to the IoT.

Specific objectives: to support the development of open and common protocols, standards and architectures and to favour multi-stakeholder governance wherever possible.

Operational objectives:

- to provide clarity and improved methods to reconcile international data transfers with fundamental rights and obligations in order to reduce current levels of uncertainty and enhance the spread of European approaches to privacy, security and data use
- to reduce regulatory, legal, technological and market uncertainties that are frequently cited obstacles to investment, innovation and participation, particularly where these uncertainties encourage development of 'closed' intellectual property, technological and business models
- to develop spectrum 'commons' (eg by expanding licence exempt bands) in order to encourage innovation and deployment of a myriad of future IoT applications with their varied operating conditions[71]
- to reduce barriers to entry by reducing unnecessary administrative burdens and strengthening harmonisation to create predictable rules and expectations and reduce the costs and risks associated with pan-European operation.

6.3.7. Effective and efficient competition and competitiveness

General objective: to ensure that the economic potential of the IoT is optimised as regards employment, innovation, economic growth and the elimination of inequality in general and as regards the European Single Market.

Specific objectives: to ensure that industrial, economic development and innovation policy are 'IoT-aware' and that competition policy is able to cope with the specific challenges arising from the IoT.

Operational objectives:

- to assess the value of active policy measures to remove barriers to entry, exit and commercial success across all domains without concentrating market power either via specific product codes or use of mobile cellular application of SIM card to market controls of numbering plans
- to ensure the strength and competitive health of linkages between the IoT sector, its upstream and downstream value chain, and financial markets

[71] This offers broader benefits, as use of low cost and open radio over the coming decades is expected to reduce current dependence on licensed spectrum and the MNOs that control it.

- to enforce competition law principles to limit distortions in the IoT sector, vertical foreclosure of IoT-using sectors and market failure via two-sided market power.

7. Normative framework and gap analysis

If the IoT represents an extension and expansion of the traditional internet to include physical objects, any legislation applicable to the internet will likely be applicable to the IoT, at least to some extent. The questions before us then are: what other issues does the IoT raise that would require specific normative provisions which do not yet exist, and which existing normative provisions are insufficient in their current form?

The present legislative and regulatory overview has been structured into nine thematic sections, covering the various legal areas that may require further policy attention from an IoT perspective:

- competition law
- equipment approval and compliance certification
- privacy, data protection and data ownership
- data retention and lawful interception
- human dignity, reputation, and freedom of expression
- universal service and e-inclusion
- cyber crime
- cyber security
- fair market practices and e-commerce.

Each thematic section will identify and assess:

- key gaps in existing or proposed legislation
- effectiveness of the existing or proposed legislation.

7.1. Competition law

- EU TFEU, Part 3: Union policies and internal actions, Title VII: Common rules on competition, taxation and approximation of laws; Articles 101-106
- EU TFEU, Part 3: Union policies and internal actions, Title VII: Common rules on competition, taxation and approximation of laws: Articles 107, 108, 109
- Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (the Framework Directive)
- European Parliament resolution of 17 January 2013 on state aid modernisation
- WTO Agreement on Basic Telecommunication, Annex to 4th Protocol to the General

Agreement on Trade in Services, Regulatory Reference Paper, 1997, Article 1 (Scope), Article 8 (Monopolies), Article 9 (Business Practices)

- EU guidelines for the application of state aid rules in relation to the rapid deployment of broadband networks, 5 January 2013

7.1.1. Gap analysis

Although competition law is firmly entrenched in the European institutional and legal frameworks, and embedded in the TFEU, notably in Articles 101 and 102, it is a daunting task to define markets relevant to the IoT, let alone the traditional internet itself. This is exacerbated by the fact that these markets will most likely grow and evolve to encompass the entire ICT and consumer electronics industry. Many observers are concerned that monopolies will naturally emerge for the IoT, like for the search engine market and for domain name allocation. Should such monopolies develop, close monitoring and possibly corrective action may be required.

Another important issue is the use in the mobile world of SIM cards and the control exercised over IMSI by public mobile operators. Suggestions have been made about liberalising and opening access to SIM cards and their Machine Identification Module counterparts, including giving users additional control. This would facilitate competition in M2M roaming (as there would be more players) and enable smaller players to enter the IoT market (eg OECD 2012).

7.1.2. Legislative effectiveness

It is unclear at this stage how the IoT market will develop, and in particular whether it is a market that will sustain more than a relatively small number of very large players (comparable to the internet search market cookies or online advertising markets, which are dominated by a few large enterprises). In general there is increasing merger activity in the industry. It is unclear whether a largely reactive role of competition authorities, limited solely to reacting to specific instances of market dominance, will be sufficient in the future without encompassing a proactive approach to fostering competitive market and rapid innovation. It should be noted that existing state aid provisions (eg Article 107 of the TFEU) underline the need for targeted aid that does not distort competition or increase public spending, while creating an environment conducive to innovation.

7.2. Equipment approval and compliance certification

- Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standards
- Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (the R&TTE Directive). This is currently under review and may be replaced by the proposed revisions (see http://ec.europa.eu/enterprise/sectors/rtte/documents/legislation/review/index_en.htm).

7.2.1. Gap analysis

There is currently no generic legislative requirement to approve electronics equipment in the EU. Instead, a set of standards or benchmarks has been adopted which is used for the assessment of equipment in different industries (eg radio and telecommunications terminal equipment, low-voltage equipment, electromagnetic compatibility, toy safety), following the 'new approach' mechanism: essential requirements are established via minimal legislation, and more non-binding detailed norms are developed separately from the legislative process through standardisation bodies. As an example, Directive 1999/5/EC (the R&TTE Directive) establishes a regulatory framework for placing on the market and putting into service radio equipment and telecommunications terminal equipment, and would apply to at least some IoT products. Third-party certification is not usually required. 'Old approach' directives require third-party testing and approval against technical standards that are directly adopted by public authorities. However, the 'new approach' directives currently adopted follow a different format and place more obligations on the manufacturer to make sure that the product meets appropriate requirements, which are not included in the directives themselves.

Given the unique characteristics of the IoT, it is advisable that the general normative framework for equipment conformity and approval should be revisited and vetted for IoT business cases. An expanded use of 'compliance marking' (certificates and marks of conformity issued by a third party) should be considered for sensitive IoT use cases, eg in health care or the transportation sector, or to attest to data protection compliance. In an IoT environment, it may be necessary in exceptional cases, such as where critical applications are involved, to move beyond voluntary and self-regulatory mechanisms. Any such efforts should carefully balance the impact on innovation and investment incentives.

7.2.2. Legislative effectiveness

As indicated above, the current legislation focuses on conformity requirements but does not normally mandate equipment approval, conformity or third-party testing.

7.3. Privacy, data protection and data ownership

- UN Universal Declaration of Human Rights, 1948, Article 12
- UN International Covenant on Civil and Political Rights, 1966, Article 17
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This is currently under revision and may be replaced in the future by the proposed General Data Protection Regulation and the proposed Law Enforcement Data Protection Directive (see http://ec.europa.eu/justice/data-protection/law/index_en.htm)
- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Article 7 (spam)
- Directive 2002/58/EC on the processing of personal data and the protection of privacy (the Privacy and Electronic Communications Directive)
- Draft regulation on electronic identification and trusted services for electronic

transactions in the internal market, 4 June 2012, Chapter II (electronic identification)

- UN International Telecommunication Regulations, 2012, Article 5b (unsolicited communications)

Non-legislative recommendations, norms, guidelines, opinions:

- Commission recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by RFID
- EU Article 29 Data Protection Working Party, Opinion 5/2010 on the industry proposal for a privacy and data protection impact assessment framework for RFID applications
- EU Privacy Impact Assessment Framework for RFID applications, 12 January 2011
- Opinion 26 of the European Group on Ethics in Science and New Technologies to the European Commission
- OECD Privacy Guidelines
- The Asia-Pacific Economic Cooperation (APEC) Privacy Framework
- UN, World Summit on the Information Society (WSIS), Action Line C10 (Article 25): Ethical dimensions of the information society (eg Article 25c, privacy and data protection)
- UN, WSIS 2005 Tunis Agenda, Article 42 (spam, privacy, data protection, freedom of expression), Article 46 (privacy)

7.3.1. Gap analysis

The legal framework for data protection in the European Union is currently undergoing revision. These revisions are, *inter alia,* addressing an important gap in the area of privacy and data protection, regarding liability for privacy violations. As the impact assessment to the proposed revision explains (European Commission, 2012b), the current Data Protection Directive is not uniformly effective in ensuring the accountability for violations of data protection laws. However, the newly proposed General Data Protection Regulation calls for fines up to €1m or up to 2percent of the annual worldwide turnover of enterprises. While this proposal has been criticised in some quarters for being too onerous and may therefore not be retained as written in the final text, it demonstrates a broader move towards greater accountability.

It is important to note that accountability is determined by not only the size of a fine, but also enforcement mechanisms. There is a key gap in the legislative framework in this area, because harm to individual victims is often too minimal in the grand scheme of things to make it worthwhile for these individuals to take legal action. As a result, even widespread incidents that cause significant harm can go unchecked. Joint enforcement actions, such as European variants of class actions, might be desirable. This will be especially important in an IoT environment, where big data concerns will be exacerbated because of the scale at which data on all aspects of the lives of everyday citizens will be collected, aggregated and reused.

7.3.2. Legislative effectiveness

Although much effort has been put into the development and refinement of a data protection and privacy framework at the European level, many Member States have found it difficult to implement and enforce these laws at the national level, primarily because violations of the requirements of the Directive are so frequent. Furthermore, in the more serious cases, servers or service providers are often not located in the jurisdiction of the victim, making it even more costly to enforce any rights that data protection laws have foreseen. Both these issues will only be exacerbated in an IoT environment.

Other issues that hamper the effectiveness of current data protection legislation include:

- *The meaning of 'personal'*: Data protection rules are triggered or become applicable when data becomes 'personal'. However, in an IoT context, it can be next to impossible to determine exactly when data become 'personal'. Certain data, which may seem innocuous or even anonymous at the time of collection, may become highly sensitive early on in the aggregation or mining process. This begs the question as to relevance of the notion of 'personal'. The criterion of data being capable of identifying a natural person directly or indirectly (also retained in the newly proposed regulation) may therefore be hard to apply in an IoT context.
- *The 'purpose' of data*: Another risk is that IoT data might be aggregated too rapidly in real time to allow for the identification of a clear purpose and may be easily reused for purposes for which they were not originally intended. The obligation to process data solely for particular known purpose(s) may therefore be increasingly ineffective in an IoT environment.
- *Who is 'liable'*: The liability of actual data controllers is becoming more and more difficult to identify in an IoT environment, where data can be exchanged and reused quickly and infinitely. More importantly, the actuating capabilities of IoT devices (in which devices can make important decisions on how to process or respond to data themselves) raises fundamental challenges: will devices themselves be considered as data controllers, or will liability rest with owners, manufacturers, programmers, licensors and end users, all of whom may be different persons?
- *What is 'consent'*: In an IoT environment, when can a user be deemed to be providing legitimate consent to the data controller (likely but not necessarily via the device itself)? The complexity of providing legally valid consent in an IoT context may result in other grounds of legitimacy to

take a stronger role than consent, which may erode the role and impact that data subjects have on the processing of their personal data.

7.4. Data retention

- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF)

7.4.1. Gap analysis

Data retention became a part of EU telecommunications policy via Directive 2006/24/EC, which established an obligation for telecommunications service providers to retain certain key electronic communications data for a certain amount of time, for the purpose of the investigation, detection and prosecution of serious crime. The Directive has been controversial throughout its lifespan, drawing steady criticism and legal challenges about its compliance with fundamental human rights (European Commission, 2010a).

In an IoT environment, certain IoT service providers could become subject to a similar data retention obligation, triggering further human rights concerns as interventions in individuals' personal sphere are no longer restricted to the virtual sphere of their electronic communications, but intrude into their physical realities through tangible IoT objects. It should thus be ensured that data retention rules are kept fully in line with fundamental privacy rights and the data protection principles of the European Union. As currently drafted, EU data retention legislation is likely to broad to satisfy this goal, and will thus need reigning in before it could be applied to an IoT context.

7.4.2. Legislative effectiveness

The effectiveness of data retention legislation is contested (European Commission, 2012a), because of the need of costly retention of very large volumes of personal information for an uncertain future potential use (big data). An extension of this model to an IoT context, which would involve an even greater volume of data to be stored with even greater privacy challenges, is not advisable without further consideration.

7.5. Human dignity, reputation and freedom of expression

- UN Universal Declaration of Human Rights, 1948, Articles 1 (dignity) and 3 (liberty)
- UN International Covenant on Civil and Political Rights, 1966, Article 19 (freedom of expression) and Article 17 (privacy, honour and reputation)
- UN International Covenant on Economic, Social and Cultural Rights, 1976, Article 15 (cultural life)
- ITU Constitution of the International Telecommunications Union, Article 33 (right of public to use telecoms)
- Treaty on European Union, Title I: Common provisions, Article 3 (freedom, security, justice, respect among peoples)

Non-legislative recommendations, norms, guidelines, opinions:

- Opinion 26 of the European Group on Ethics in Science and New Technologies to the European Commission
- UN, WSIS, Action Line C10 (Article 25): Ethical dimensions of the information society (eg Article 25a, freedom, equality, solidarity, tolerance, shared responsibility, and Article 25c, prevention of human trafficking)

7.5.1. Gap analysis

A number of international covenants and treaties exist to protect human dignity, honour and reputation. At the EU level, the European Charter of Fundamental Rights is a relatively recent (2000) example. These treaties are generally technology-agnostic, and their application in electronic contexts such as the internet (and future IoT) develops organically through case law.

There are no explicit gaps in existing fundamental rights texts.

7.5.2. Legislative effectiveness

While legal gaps are unlikely, it will need to be considered whether abstract treaty rights are concrete enough to result in effective protection in an electronic world in which human beings may be treated as one of the 'objects' in an IoT environment.

A new understanding of human dignity in an electronic world may be required, encompassing fundamental subjects such as self-determination (including the right to opt out of an electronic world), freedom of expression and self-development (which are only viable in a world without continuous monitoring and profiling), and electronic identity and reputation management (which require some control over our data, including as it is perceived and processed by others). As these examples illustrate, this area is closely related to other policy areas, such as data retention, privacy and the right to be forgotten in the new emerging data protection framework.

7.6. Universal service and e-inclusion

- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (the Universal Service Directive)
- EU Communication on Universal Service in E-communications: Report on the Outcome of the Public Consultation and the Third Periodic Review of the Scope in Accordance with Article 15 of Directive 2002/22/EC

Non-legislative recommendations, norms, guidelines, opinions:

- EU Communication 'Towards an accessible information society', 1 December 2008
- EU Communication 'European i2010 initiative on e-inclusion – to be part of the information society', 8 November 2007
- EU Communication on E-accessibility, 13 September 2005
- EU Riga ministerial declaration on e-inclusion of 11 June 2006

7.6.1. Gap analysis

Universal service is a part of the EU telecommunications package; it ensures that at least some measure of communications connectivity is available to all citizens of the EU. Given

the impact of the internet on the development of society and the fundamental importance that online connectivity has on citizens' capability to participate in the information society, it is high time that universal service provisions are expanded to include access to broadband internet. This is especially important for the development of the IoT as the IoT is going to require universal internet access.

Furthermore, the provisions of universal service currently do not emphasise scalability and adaptability, and do not consider evolutions in bandwidth requirement and availability. There is currently no mandated and periodic review process of the definition of universal service enshrined in universal service legislation.

It should be noted that this issue was identified as early as 2008 (see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the second periodic review of the scope of universal service in electronic communications networks and services in accordance with Article 15 of Directive 2002/22/EC), but it has so far not been resolved adequately.

7.6.2. Legislative effectiveness

Current universal service rules do not cover broadband internet access.

7.7. Cyber crime

- Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Articles 2-5 (crimes), Article 10 (jurisdiction); this is urgently under revision, and may be replaced in future by the proposal for a directive on attacks against information systems (see http://europa.eu/rapid/press-release_MEMO-10-463_en.htm)
- Council of Europe, Convention on Cybercrime

7.7.1. Gap analysis

The current legal framework in the EU is largely agnostic towards specific technologies, and should therefore not contain any substantial gaps. It is worth noting that the ongoing revision of the Framework Decision includes expanded rules to cover the use of botnets and identity theft incidents more effectively, which should also facilitate the application of these rules to criminal IoT uses, as these may be similar in operation to botnets because of their networked nature.

7.7.2. Legislative effectiveness

While the legal framework does not contain any significant gaps, the effectiveness of existing laws as a tool to combat cyber crime is questionable. This is largely because law enforcement is still essentially a national affair, and the cross-border nature of cyber crime complicates rapid intervention and effective investigations. This may be more serious for IoT-enabled crimes, as IoT devices may have actuating characteristics (raising the question

of who should bear criminal liability) and may be mobile (thus further complicating the issue of determining national competences and applicable law).

Furthermore, there is an ongoing trend of criminalising the design, manufacturing, distribution and ownership of devices (including software) intended to commit criminal offences. This trend was already captured by the current Framework Decision, which contains provisions to this effect, and will be further reinforced by the proposed directive. This approach can be problematic in cases where devices have been created for security testing, as such devices can have both beneficial (eg pen testing) and harmful (eg criminal hacking) uses. The same issue will apply to IoT scenarios as well, as devices such as monitoring equipment (including cameras, mobile phones or drones) will have similar characteristics. Ambiguous legislation on this point can stifle the development of this market.

7.8. Cyber security

- Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- Cybersecurity Strategy of the EU 2013 (including new directive on internet security: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity)
- UN International Telecommunication Regulations, 2012; Article 5a (security)

Non-legislative recommendations, norms, guidelines, opinions:

- UN, WSIS 2005 Tunis Agenda, Articles 42, 45, 57, 58, 68

7.8.1. Gap analysis

The need to protect crucial electronic infrastructure against terrorism and other threat vectors has increasingly manifested itself at EU level in recent years, including through the European Programme for Critical Infrastructure Protection (2006), followed by the Critical Infrastructure Directive 2008/114/EC, and the recently proposed cyber-security strategy, which included a proposed Internet Security Directive. These initiatives are closely linked to the aforementioned cyber-crime framework, but whereas the latter focuses more on combating specific criminal incidents, the former has a stronger emphasis on protecting general societal interests. Cyber security is a relatively young policy area, and as a result the legal framework suffers from there having been few clear challenges, including the difficulty of delineating the concept of critical infrastructure, establishing harmonised policies across the Member States to ensure that incidents do not spill over across borders, and aligning the legal frameworks so that the obligations and liabilities of critical infrastructure providers are clearly and homogeneously defined.

The introduction of IoT in this policy domain will raise new challenges. The IoT is not formally defined in current legal initiatives, and it is therefore not unambiguously covered or exempted under existing legislation, including the CIIP Directive and the proposed

Internet Security Directive; this depends on whether a specific IoT service qualifies as critical infrastructure, respectively as an information society service or other product or service offered by a market operator. There is thus a risk of a legal and policy gap, in which decentralised or community-based IoT services may not be subject to cyber-security obligations. This issue will have to be monitored in future to ensure that no major gaps are allowed to exist.

7.8.2. Legislative effectiveness

The effectiveness of the current legal framework is difficult to assess as it is still young and current experiences with significant incidents are thus scarce, even in a non-IoT context. However, it is clear that challenges may result from the way the IoT is impacted by current legal initiatives, as the responsibilities and liabilities of IoT service providers (or users) can be unclear or differ from Member State to Member State. For instance, IoT incidents would result in an obligation for market operators to file breach notifications, which will be effective for cases in which a clear market operator can be identified, but not necessarily for others. This can become an important issue if IoT networks are entrusted with tasks that are fundamental to the correct functioning of vital parts of society (eg mobility, health care and energy).

Similarly, hardware manufacturers and software developers are exempted from the risk management and reporting obligations of the proposed Internet Security Directive, as are certain specific sectors such as the water and food supply industries. While this can be acceptable to the extent that safety in these sectors is regulated by other EU initiatives, the same is not necessarily true for the IoT. The safety of IoT devices thus may not be adequately ensured or validated by independent parties. A post-hoc approach that addresses incidents after they occur may not be sufficient in an IoT environment, and emerging use cases will thus need to be monitored to ensure that comprehensive security is ensured in all key IoT sectors.

7.9. Fair market practices and e-commerce

- Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market; amending Council Directive 84/450/EEC; Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council; and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive)
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce)

7.9.1. Gap analysis

The EU has taken significant steps in ensuring that consumers are protected against unfair market practices on the internet, including via the Unfair Commercial Practices Directive

2005/29/EC and the Electronic Commerce Directive 2000/31/EC. Both of these are technology neutral, but their applicability in an IoT environment will likely not be trivial.

7.9.2. Legislative effectiveness

Legislative challenges in this area are related to the fact that these directives are focused mainly on traditional communications mechanisms. For instance, it may not be straightforward to inform citizens of the identity and location of service providers in an IoT environment where devices may not have been equipped with video screens or other communication channels that are easily understandable for human users. Furthermore, actuating devices may not have appropriate communication routines available to them to communicate choices to end users. As a result, it may be difficult to ensure transparency towards citizens on how IoT devices and services in their environment impact them.

The issue of liability is also of concern: the Electronic Commerce Directive provides specific and conditional liability exemptions for hosting, caching and mere conduit service providers. These provisions may also become applicable to some IoT applications, egfor example in use cases that consist partially or entirely of information aggregation. The extent to which these provisions are appropriate for an IoT world will need to be monitored, in particular whether they strike an appropriate balance between supporting innovative IoT use cases and establishing effective protection for end users.

7.10. Standards

7.10.1. Gap analysis

Standards affect the structure, efficiency and effectiveness of the IoT in a variety of ways. Chief among these is the provision of a common framework for interaction among a wide range of devices, necessary to preserve the openness and 'bring your own device' character that is widely regarded as crucial to the continued evolution of the IoT. There are a range of tensions arising from this function, including that between openness and proprietary standards; potential conflict between technical and operational standards; balancing standards against market forces, regulations and other forms of governance; and the dual aspect of standards that exclude non-compliant devices and processes from the IoT and create a protected space within which competition and cooperation can operate.

Standards are used to control a wide range of aspects of the IoT, from technical standards relating to physical devices and use of electromagnetic spectrum to standards for information encoding and protocols for communication among devices. Many of them are inherited from or also apply to other domains within which these devices operate – this in turn creates the potential for conflicting objectives of standardisation and incompatible procedures for defining, agreeing, enforcing and monitoring standards. In this respect, the most important discussion is over the need for an IoT-specific suite of standards, with

specific standards initiatives having been created to incorporate and adapt existing standards and to complete the portfolio with additional standards.

Comparison of existing and proposed standards reveals other types of fragmentation, for instance the existence differentiation by frequency and spatial range.

Another source of potential gaps in coverage derives from the self-created and often self-certified nature of standards. At present, standards applicable to the IoT are produced by a range of bodies. Interviews with representatives of standards bodies suggest that the process of standards creation and refinement combines cooperation within a specific standards body) with a competitive phase (between different standards). Especially in the case of standards for communication and interoperability, the initial choice of a (set of) standards (often equivalent to choosing a standards body) may limit contact with users of competing standards, and thus affect the overall development and coherence of the set of available standards.

This potential for 'structural holes' in the portfolio of available standards can be reinforced by the uneven pace of standardisation in different areas – the tendency to standardise early (again, particularly for communication standards) has the potential to affect technological and service development, raising the risk of 'lock-in' to solutions that may not be the most effective in the long run. This risk has been observed before in other ICT-related technologies where interoperability or economies of scale give rise to strong first mover advantages and the creation of a 'compatibility pool'.

The standards bodies themselves also tend to represent particular parts of the IoT value network. This can bias development away from tightly integrated solutions – there is no evidence that this is inefficient (at this stage of IoT development), but there is some risk of technology specificity (eg with the difficulties encountered in adapting RFID standards to the range of technologies currently under development for NFC). However, interviews suggest that industry players are aware of the potential positive impacts of specificity in providing economic returns to intensive competition and full development of particular technologies that might otherwise be abandoned 'too early'.

7.10.2. Legislative effectiveness

Standards are not laws, so the interpretation of their effectiveness must be balanced with an appreciation of their evolutionary and often voluntary character and the lack of formal institutions to reconcile different standards with each other and other governance mechanisms.

At this early stage of development, it is not clear how uniformly standards are applied or enforced, or even how strictly they should be enforced. One interviewee likened the current standards landscape to a beauty contest, whose most useful output would be a greater degree of agreement as to which elements of the IoT should be standardised and

how standardisation should be organised. There are no clear or authoritative data showing the number of firms or devices bound by specific standards, or the degree to which standards adoption is reversible.

There is another sense in which effectiveness can be gauged: the degree to which standards are explicitly recognised in law, regulation and procurement specification. Existing public procurement rules, for example, make explicit provision for tender specifications to mandate compliance with named standards 'or equivalent performance'. Other forms of policy support for industrial and service development can adopt similar endorsement strategies, or explicitly recognise certification activities associated with specific (families of) standards.

Most IoT standards to date have been created by industry-led bodies, with an engineering orientation and relatively little public sector or civil society (lay) representation. This may limit their adoption by 'downstream' users and effectiveness in realising societal benefits, but there is no hard evidence to support this in the IoT domain. However, some of those interviewed expressed concern over the potential competitive implications of standardisation driven by industry. This is not a new concern; many have drawn attention to the potential for standards driven by dominant firms to foreclose competition, especially vertically (eg by limiting the ways individual devices could interact with and over common platforms), but this might occur less in the IoT context where important interactions are self-organised for M2M or peer-to-peer rather than client–server communication.

7.11. (Internet) governance structure

As highlighted in our definition in Section 1, the IoT builds out from today's internet, but also differs from the internet in several aspects (further detailed throughout the report). As an extension to the internet, the IoT is largely subject to internet governance issues.

As noted in Section 1.5, on internet governance, the world is currently split between countries that look primarily at multi-stakeholder organisations to take care of important aspects of the internet, like ICANN (DNS and IANA) and IETF (development of standards), and others which place their trust in more government-driven institutions like the ITU.

The IoT itself is on the agenda of the informal talks at the Internet Governance Forum. The Dynamic Coalition on IoT (DC IoT) was set up, which had its first inaugural meeting in Nairobi, October 2011. DC IoT reports that there are still great controversies about the basic understanding and definition of IoT governance: while one group sees IoT governance as a special separated issue, others define IoT as 'another application' on top of the DNS (next to other internet applications such as e-mail, social networks and so on) (IGF, 2011). There are also controversies about the understanding of the ONS (in

comparison with the DNS), and allocation policies for identifiers, including IPv6 addresses (IGF, 2012).

The IoT Expert Group, set up by the European Commission and with several members of the DC IoT, agrees that for the time being the general internet governance principles as laid down, *inter alia*, in WSIS Tunis Agenda (2005) and the ICANN Bylaws give enough guidance for the further development and deployment of new IoT services and applications. They emphasise that future IoT policy initiatives should be user oriented, market driven and need to enhance privacy of end users, security and fair competition. They state that, most importantly, nothing should be done which could prevent further innovations (European Commission, 2013).

In essence, most stakeholders seem to believe that a new, dedicated IoT governance framework is not needed. Experts interviewed for this study – in line with reports produced by the IoT Expert Group and DC IoT – believe that if IoT-specific policy issues will be identified they can be dealt with in the framework of the existing internet governance platforms and that the ongoing IoT multi-stakeholder process taking place in existing platforms like the Internet Governance Forum (IGF) would be the right place to deal with it, for now.[72]

[72] See also: Recommendations on a European Strategy for the Internet of Things (IoT), endorsed by Center of European National Top Level Domain Registries, European American Business Council, GS-1, TechAmerica Europe and the European Telecommunications Operators' Association, 1 November 2012.

8. Consideration of policy options

8.1. Policy options

As discussed in Section 6, the breadth, global scope and dynamism of the IoT itself, the complexity of the Community mandate for action, and the intricate linkages among the many issues raised by the current and likely future development of the IoT militate against the elaboration of tightly focused and specific policy interventions. It seems more appropriate to adopt instead a strategic approach that can be used to group and structure more detailed potential interventions while remaining 'future-proof' and providing internal and external stakeholders with a consistent basis for individual and collective action at a more instrumental and detailed level.

In this section, we present three overarching policy options or stances defined by the project team:

- *Option 0, do nothing*: more accurately, not changing any policies currently under way and assuming other parties will do the same
- *Option 1, soft law*: initially using measures other than changes to laws and regulations[73] to stimulate development and mitigate problems in some areas and observing other areas, possibly leading to later action
- *Option 2, hard law*: making a mix of changes to existing laws and regulations (harmonisation, integration, new provisions and/or deregulation) with greater or improved enforcement of existing laws and the implementation of new formal (co-)regulatory actions (again with statutory underpinning).

We should note at the outset that these are not simple global once-and-for-all decisions. Each of these stances involves a balance of pro-activity and adaptability, acting rapidly where sufficient evidence and commitment are available while retaining flexibility to gather

[73] Especially – but not exclusively – such quasi-legal instruments as communications, codes of conduct and guidelines used within areas of EU competence.

further support and information before acting. In implementing any of these approaches, we expect that specific policies will change. In particular, it seems likely that the implementation of any of these options will involve a changing mix of actions that take the form of IoT-specific initiatives and measures to adapt other (existing and new) policies to the specificities of the IoT. In some cases, IoT-specific measures will form an interim measure intended to bridge the gap between the IoT and the broader internet, economy or society; these may be necessary[74] but would be accompanied by review and transition provision to permit them to be absorbed into more general areas of governance (competition, privacy, consumer protection etc) as convergence proceeds and evidence accumulates. In other cases, general 'light touch' measures may be needed until it is known whether the IoT requires and can support special treatment.

In a similar fashion, while these measures are discussed from the Community perspective, they necessarily involve action by many parties; it may well happen that roles shift as the IoT develops and responds to policy, eg by transferring responsibility from formal regulation to co-regulation or self-regulation or vice versa.

Finally, the policy options may be used in sequence. There is a case to be made for starting soft and broad and moving to hard law where it appears necessary (once we know more), but also a case for starting with hard law to create a framework of certainty to encourage innovation, which can be relaxed as the IoT becomes increasingly self-governing. Indeed, it is most realistic and appropriate to think of the soft law option as starting with quasi-legal and non-legal measures (see Section 8.1.2) and proceeding to legal changes only when the scope for such measures clarifies, while the hard law option starts with adjustments to the legal framework conditions, and uses other measures to fit specific circumstances and fine tune the intervention once the framework changes have been implemented.

8.1.1. Option 0, do nothing

The simplest policy option, which must always be considered, is to take no (further) action. This does not mean that no actions will ever be taken in Europe to address the issues and problems associated with the IoT or to influence its development – external stakeholders (including business, citizens and consumers and Member State and foreign governments) will continue their activities. Indeed, actions may be taken at European level that influence and respond to the IoT, insofar as the IoT would evolve in directions that naturally bring it within the scope of existing policy initiatives. These include ongoing programmes of regulatory evaluation and reform in general (REFIT) and in specific areas (eg privacy and the Telecommunications Regulatory Policy Framework). Moreover, public

[74] Because the IoT and non-IoT aspects of a problem are currently very different – eg automated data collection or because the IoT aspects are changing too fast for modification of other laws, regulations and so on.

procurement and public support for research will continue to influence the demand for and supply of IoT-relevant innovations and services. However, the distinguishing characteristic of this policy option is that there will be no dedicated intervention in the development of the IoT market, no EU-level investment in the IoT *per se*, no specific research and deployment programmes aimed at the IoT, and no modification to existing or emerging rules and regulations centred around the IoT.

Under this option, the development trajectories discussed in previous sections can be expected to continue.

8.1.2. Option 1, soft law policy options

This option involves a range of non-legislative activities. As discussed above, this does not involve changes to statute law or formal regulation, but does entail use of the other quasi-legal measures (eg communications, guidelines and codes of conduct) within its areas of competence, together with non-legal actions such as procurement, participation in standardisation and governance bodies, international negotiations, research and innovation support, financial support (eg for infrastructure, research and innovation (R&I) and economic development), monitoring and data analysis and dissemination, recommendations and support for self- and co-regulatory initiatives including eg certification. Some of the specific measures that could usefully be included are described in Table 8.1, grouped under three major headings:

- *watching brief*: a largely reactive option based on monitoring and targeted intervention based on the observations made
- *innovation policy*: a proactive option in which the IoT is stimulated actively to develop in directions that align most closely with EU socio-political values and preferences
- *industrial policy*: a proactive option in which there is active intervention in the technical development and governance of the IoT, again aiming to ensure that development aligns with EU values and preferences.

Table 8.1 Aspects of soft law options

Area	Policy sub-option
WATCHING BRIEF	
Architecture	Monitor and assure open and equal 'fair' access to the IoT infrastructure Collect and document architectural proposals and standards, and instances of their implementation
Economic aspects including competition, investment	Collect data on the structure, conduct and performance of IoT sector players Monitor macroeconomic and (especially IoT-intensive) sectoral indicators
Ethics, education and values	Monitor ethical contributions of IoT implementation (eg via ethical monitoring and horizon scanning, and extension of fundamental rights indicators)
Governance	IoT is in its early phases, and needs space for innovation and growth, as well as stability from a regulatory perspective; monitor self-regulation, rather than pre-empting this with formal regulation Pay attention to IoT-specific subjects in a range of policy areas, as it is merely a specific aspect of the internet; IoT is not a governance area in itself but touches on several, mostly but not solely those on the internet Monitor development of the IoT into a critical infrastructure in order to prepare for potential change in basis for regulatory intervention
Security and privacy	Monitor and assess suitability and applicability of 'informed consent' and meaningful choice Monitor the incidence and prevalence of security threats by liaison with relevant industry and international organisations
Technical aspects including spectrum management	Add data on M2M traffic to existing indicators of network use
INNOVATION POLICY INCLUDING RESEARCH SUPPORT	
Architecture	Support R&I – with vertical sector demonstrators in expected key sectors where significant societal IoT benefits could be realised (health care, mobility, environmental protection, etc), as well as more basic R&D

Area	Policy sub-option
Economic aspects including competition, investment	Support productive R&I aimed at building and supporting clusters Foster cluster development through support (direct, indirect, in-kind, demand-side) for infrastructures needed to develop IoT-themed clusters Support development, deployment and interconnection of local communications and related infrastructure necessary to provision ubiquitous IoT capability Expect evolution of identification schemes to come from industry – policy should be to coordinate industry bodies and ensure no abuse of significant market power (SMP), moving to open identifiers as and when possible
Ethics, education and values	R&I as a tool for encouraging deeper ethical reflection; continue promotion of and learning from third-party ethical audits in EU-funded ICT research Provide guidance (eg based on identified best practices)on development or use of the IoT in accordance with EU fundamental values, including on privacy, human dignity, freedom of thought, expression and assembly or association, and non-discrimination Take advantage of existing EU flagship programmes to support Digital Agenda for Europe's (DAE) social policy targets Stimulate development of an ethical perspective in research and design (eg via ethical impact assessments and/or promotion of corporate social responsibility)
Governance	Provide 'charter' recommendations for adoption and extension of IoT devices, systems and services Support collaboration actions to build flexible vertical industry-wide norms using ISO- or EU-level standardisation activities
Security and privacy	Help players understand implications of emergent risks (eg via Horizon 2020 programme) Provide guidelines on conducting risk assessments or privacy impact assessments for IoT products or services
Technical aspects including spectrum management	R&I encouragement of modern sharing techniques such as White Space Devices (WSD), Cognitive Radio (CR), Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS)

INDUSTRIAL POLICY	
Economic aspects including competition, investment	Consider multiple investment models as part of an EU-wide industrial policy (eg as appropriate, use public sector only, mixed public-private programmes and for medium/short-term fairly low-risk, private sector only
	For the main IoT shared infrastructure, major sums are involved – so consider public sector finance only, prudently mixed with PPP in selected cases
	Channel industrial policy activities (procurement, development funding and financial support) specifically towards rivalries, new entrants and technologies, services and business models that compete with or complement incumbents
	Endorse open IoT standards through demand-side instruments.[75]
	Consider an 'IoT first' presumption for targeted parts of public procurement[76]
	The full range of financial measures ranging from state aids to risk capital participation and underwriting can, in principle, be employed to provide incentives for development of the IoT by private and public bodies
	Investment support could be targeted throughout the value chain
	Provision of suitable communications infrastructures (eg low-cost radio access) and the development of devices may be as important as the creation of integrated systems (eg driverless cars) that use these devices and infrastructures
Governance	Encourage rapid and appropriate standardisation by participation in standards bodies and inclusion of standards in public policy
	Strengthen certification regimes by recognition and cross-linking to public data and registries
	Participate in international IoT governance and represent IoT considerations in international internet governance
Security and privacy	Provide better guidance for market players to conduct risk assessments across hazards and security (holistic risk model for physical and virtual spaces), and facilitate compliance certification and trustmarking schemes

[75] The procurement directives make explicit provision for the inclusion of named standards, providing the tender also allows 'equivalent performance' – for which the evidence required must be stronger. Thus these tools both reinforce existing standards and facilitate their continual improvement because successful variants may in turn give rise to new standards.

[76] This would be analogous to the 'cloud first' strategy implemented in the US and would embed IoT specifics in procurement specifications and evaluation criteria.

	Expand spectrum sharing with strong EU drive on both regulation for licence exempt bands and R&I encouragement of modern sharing techniques such as WSD, CR, DSSS and Frequency-Hopping Spread Spectrum (FHSS)
Technical aspects including spectrum management	Use EU fora (Conference of Postal and Telecommunications Administrations; CEPT, and Radio Spectrum Policy Group; RSPG) and Member State national regulatory authorities (NRAs) to prepare for a global approach (World Radio Communication Conference; WRC) to licence exempt band releases especially for DD2 and liberal use of existing international mobile subscribers with relaxation of limits
	More practical guidance for data controllers and data processers on important IoT aspects like informed consent; accountability and transparency

8.1.3. Option 2, hard-law policy options

A more formal and explicit option is to tackle IoT-related policy issues by means of new or changed statutory and regulatory law and/or through improved or reengineered enforcement of existing laws. The overall intention is to establish appropriate legal norms and enforce them against violations. This may include extensions of existing regulations and laws to cover IoT players. In doing so, considerations of feasibility and proportionality are paramount.

Changes in the legal framework

Several possible routes are feasible:

- Improve legal harmonisation to make sure that existing legislation in a range of policy areas implicated in the IoT effectively addresses its specific problems and does not conflict with other legislation or create undesirable unintended consequences. Examples include revisions and possibly amendments of the Electronic Commerce Directive, Electronic Privacy Directive and Data Retention Directive in order to clarify their applicability to the IoT, addressing the concerns identified in Section 7. Similarly, make ongoing legislative revisions and proposals (such as the contemplated General Data Protection Regulation, Directive on Network and Information Security and Directive on Attacks against Information Systems) 'IoT aware', ensuring that their new provisions are in line with the specific characteristics of the IoT.
- Enforce legal harmonisation by amending directives or regulations in key areas, possibly making provision for the use of Commission decisions, delegated or implementing acts in order to keep pace with new developments while retaining overall coherence, effectiveness and stability. For example, adopt specific acts within the context of the General Data Protection Regulation, for example to support privacy by design in IoT devices or services.

- Encourage legal unification by replacing directives with European regulations in areas strongly affected by aspects of the IoT where national differences in implementation are particularly damaging to the implementation of the Single Market or other treaty obligations. The contemplated replacement of the Data Protection Directive by the General Data Protection Regulation is a clear example; similar evolutions are conceivable, for instance in the Telecommunications Regulations or the Electronic Commerce Directive, if there would be sufficient consensus among Member States on the benefits of such an approach..
- Give legal force to international agreements, thus ensuring their legal authority and enforceability in practice. The Safe Harbor arrangement in the context of data protection is a viable example, as an agreement between the European Commission and the US Department of Commerce was strengthened and further validated through a formal Commission Decision (Decision 520/2000/EC). Similar approaches could be applied in relation to the mutual recognition of security assessment against protection profiles by national conformity assessment bodies.
- Provide formal legal backing for self-regulation in cases where its outputs are seen to be appropriate, generalisable, fair, reasonable and non-discriminatory, and consistent with existing law and policy (co-regulation). This option was also used within the data protection framework, where the codes of conduct established by the Federation of European Direct and Interactive Marketing (FEDMA, n.d.) were ruled explicitly to be compliant with EU data protection law by the Article 29 Working Party (European Commission, 2010b), thus increasing its legal standing and value to marketing associations.
- Support the use of specific standards by ensuring that compliance with those standards is considered to be proof of compliance with more broadly phrased legal requirements; this method of operation is commonly used in New Approach Directives.

The examples above assume that existing rules are amended or implemented in ways that support the IoT. An alternative would be to adopt separate legislation that specifically addresses the needs of the IoT, eg in the form of an IoT directive or regulation. This would offer the benefit of providing a single legislative tool that groups all legal needs of the IoT into a single instrument, which is a policy option that is sometimes used for new technologies that have very specific technical needs (such as egthe recent Electronic Money

Directive[77]). However, this approach also risks creating divergences with other legal frameworks, when obligations established in an IoT specific framework are no longer in line with generic rules (eg IoT liability or transparency requirements would be more or less strictly defined than for e-commerce in general), which may or may not be justified. Thus, such sector specific approaches that essentially isolate the IoT as a separate field of policy and law making are not without risks.

Generally speaking, the creation of sustainable markets and viable businesses is highly dependent on a well-regulated market (which does not imply there is a formal regulator) and on consistency in policymaking. To the extent that formal regulation is needed, it should be based on clear principles and focus on promoting (static and dynamic) efficiency and equity rather than on the number or sizes of firms involved. This concept of 'regulatory fitness' is consistent with the REFIT initiative being implemented across the European Commission, which provides a vehicle and a basis for the reconsideration of existing Regulations – *inter alia* in light of the IoT.

The scope of laws and regulations involved is documented in Section 7. In most of these areas, while IoT-specific measures might be implemented, it is too soon to identify the areas in which they may be needed.

Changes in enforcement

The analysis above has identified a range of areas where enforcement of existing laws and regulations struggles to keep cope with the IoT. These include many of the areas highlighted in Section 7, and especially privacy (Section 7.3) and security (Section 7.8), consumer protection (Section 7.9), competition (Section 7.1) and cyber crime (Section 7.7). In addition, there may be challenges to the effective enforcement of telecommunications regulatory policy, though this may need to be addressed by legal change; even the status of the internet in relation to the Telecommunications Regulatory Policy Framework is unclear and to our knowledge none of its provisions have yet been applied to the IoT *per se*. This policy option therefore not only implies that revisions or extension of legal rules are considered, but also that the effectiveness of enforcement mechanisms (eg through traditional court systems, national supervisory bodies, consumer protection bodies or alternative dispute resolution mechanisms) is monitored and strengthened where needed.

[77] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

8.2. Assessment of policy options

In this section, we consider the differential impacts of the policy options as compared to the base case ('do nothing') option whose impacts are analysed above.

8.2.1. Soft law

Architecture

A coherent architecture adapted to the IoT might emerge under the 'do nothing' option, but is unlikely to be optimal. In contrast, because the soft law option makes specific provision for monitoring, discourse and exploration of architectural principles, it is far less likely to risk being overwhelmed by inappropriate legacy elements derived from the internet *per se* or from other domains whose specific requirements might limit the generality, openness, functional effectiveness and innovation-friendliness of the IoT. This visibility and engagement with architecture also reduces the risk – present under the 'do nothing' option – that no coherent architectural principles emerge and that instances of the IoT, while formally interoperable at device level, may not work together at system level.

Also, this approach is likely to end the current trend towards fragmented standards coming from a range of different standards bodies and thus reflecting the conflicting objectives of many parties. Under the soft law option, standards are monitored, public bodies actively participate in standards bodies, and standards are reinforced through recommendations and inclusion in economic stimulus measures (on the demand side through inclusion in public tender requirements; on the supply side through mandated engagement with standards bodies by projects in receipt of public funding). Such standards are less likely to slow or distort the development of the IoT and more likely to lead to the emergence of common architectural principles needed to ensure short-run effectiveness and preserve interoperability, openness, security and other desirable characteristics against future development.

One particular benefit is that interoperability is likely to be enhanced; because of the multi-stakeholder nature of the soft law approach it should be able to avoid problems like that observed in relation to RFID, where concern over the protection of proprietary information limited the utility of tags beyond their original purpose (Schindler et al., 2012).

Economic aspects including competition, investment

The internet itself faces economic challenges; while the levels of output, value creation and employment associated with the internet economy are large, many of those estimates

depend on strong assumptions and controversial attribution techniques.[78] The provision of the soft law option – including the collection and sharing of data and pro-competitive industrial policy – mean that these challenges are less likely to spill over to the IoT. As a beneficial consequence of the broad and diversified support for IoT developments that both increase value and minimise risk, limitations on access to capital that have restrained the growth of the internet and the IoT alike may ease.

The soft law option will also minimise regulatory burdens and deadweight losses associated with inappropriately targeted industrial policy.[79] In principle, the IoT will have a better chance to contend with other areas of economic development and will attract capital and build market share to the extent that it succeeds in delivering value to customers and capturing enough of this value to provide the supply side with adequate returns.

The extent to which this optimistic expectation is realised will depend on other aspects of policy. Though a full analysis goes beyond the scope of this report, it is useful to note a few areas where the cross impact will be particularly strong. The large data flows associated with the IoT will be subject to regulation under existing EU rules, and their utility will depend on the capacity of the communications infrastructure (especially the wireless portion) to carry this traffic and availability, affordability, quality and suitability of computation resources needed to process, store and make these data available. If the development of high-speed communications infrastructures differentially favours wired connections, asymmetric provision (faster download then upload) or fixed locations, many promising IoT applications will not be able to fulfil their promise. If the data collected cannot be handled cheaply, only a subset of the applications, services and business models envisaged by many stakeholders will come to fruition. In addition, if the provision of computing and communications infrastructures remains dominated by large players and incumbents, the development of the IoT may not produce the degree of innovation and atomistic competition that the underlying technological possibilities (cheap interoperable devices providing a decentralised and self-organising ocean of sensors and actuators for a cloud-like information system operating over an open, reliable, secure and affordable network).

---

[78] For instance, these involve attributing to the internet the bulk of value created by businesses that use the internet, without considering whether the same value might be created in other ways, differentiating between internet services *per se* and (eg communication) services that are currently conducted in whole or in part over the internet, but which might be provisioned in other ways without much loss of value. Such estimates also tend to take optimistic approaches to overcome the difficulties involved in separating the 'internet' parts of the profitability of large diversified companies and distinguishing between economic value creation and rents created by market power or a favourable regulatory environment, for example.

[79] Including the distortions associated with traditional policies that 'pick winners' whether in the form of incumbent firms or specific technologies (Aghion et al., 2012).

Thus the coordination of IoT-related policies with policies in other areas may be particularly important. To this end, the soft law option provisions for using the IoT as a platform for policy discourse and coordination and for working through existing programmes are particularly useful.

The economic and market challenges facing IoT development come from the specifics of the technology – this has already been noted in relation to the cloud, where the placement of storage and processing resources in data centres can potentially lower entry barriers to cloud users. They gain access to state of the art functionality through thin clients and are therefore much less likely to be locked in to specific suppliers. In turn, those providing services over such platforms have immediate access to a critical mass of users, which sharpens the efficiency-enhancing effects of innovation competition. But this loss of traction is resisted by those providing access and those who provided computation services according to closed or walled garden models. To preserve their market power, they tend to use strategies such as traffic shaping, device tethering, exclusive subscriptions and use limitations that greatly weaken the societal returns and the economic advantages to the 'ends' of the market.[80] The same factors apply to the IoT, as the platform-based market structure is very similar; in addition, the destinies of the cloud and the IoT are linked: the former provides computation and storage for the data generated by the latter, while the sensors and actuators of the IoT offer enhanced functionality to cloud-based entities and services.

Ethics, education and values

In this domain, the soft law option can facilitate but not enforce progress in meeting the ethical objectives. Much will depend on the outcome of current initiatives to reform the data protection and privacy rules. Beyond this, pressures on government and industry scrutiny, retention and processing of 'near-personal' data may come to affect the rights of those using the IoT. If they can engage with government on the basis of open data sharing and multi-stakeholder dialogue, these risks may be averted. But this is not guaranteed; to the extent that they become aware of these forces, significant swathes of users may opt out and thus lose the benefits of the IoT and may even suffer weakened societal inclusion. In addition, the erosion of the effective significance of informed consent is likely to continue, which may limit the alignment between user choices and user interests, reduce the extent to which consent can be used to signal or reinforce trust among participants and even selectively distort the ability of society to infer progress towards the protection of fundamental rights by analysis of data relating to the use of the IoT. Finally, the provision of privacy protections 'up the stack' in designed or automated form may encourage

[80] A more complete analysis can be found in Cave et al. (2012)

complacency and crowd out individual vigilance and continual refinement of the policy understanding of individual rights.

Governance

The governance of the IoT will continue to be contested between different interest groups, modalities of control and decision fora. While the interconnected and multi-stakeholder governance approach of the soft law option can mitigate this fragmentation, it cannot overcome it entirely. There is thus a risk that the mix of technical, economic, legal and informal rules may not strengthen IoT development. To the extent that effective self- and co-regulatory arrangements spring up in or extend into the IoT, they may be vulnerable to capture or mission creep. Much will depend on the convergence of these processes – if a reference body or set of rules emerges the IoT can avoid further fragmentation of governance and the prospect that only those issues that can be handled by standards or mediated through market mechanisms are effectively dealt with.

Security and privacy

The soft law option makes indirect provision for addressing issues of security and privacy. However, this may prove effective; especially in the privacy domain, the provision of reliable and relevant information should allow users effectively to negotiate with suppliers or to allow certification mechanisms to emerge that align market forces with valid privacy interests. In addition, the support for research and experimentation envisaged in this option will improve public understanding of the risks, enable users to take more effective precautions and even allow financial markets to analyse and price risks associated with specific devices, technologies, business models and the practices of specific firms.

Security may not be as effectively addressed by this option, not least because incremental improvements to which it is expected to lead in the short run may not compensate for the potentially severe consequences of breaches. Breach notification will be extended to the IoT, but such provisions have proven ineffective or even counterproductive troubling in the past (eg Schwartz and Janger, 2007; Dimick, 2010; Kierkegaard, 2013).[81]eg There is also a risk that users will not be able to associate a breach with a responsible or accountable party. Indeed, the prevalence of small scale breaches may be so high, and the consequences so hard to define, that users may become insensitive to them. Certainly, the ability of users to prevent breaches will be limited, and the capability and incentives of device manufacturers or network service providers to compensate for this will be limited.

[81] These problems reflect both the proportionality of breach notification requirements, the ability of those notified to take steps to mitigate past harms or avoid future harms (especially in view of the inherently indefinite nature of the information provided) and the uneven impacts and potentially perverse consequences of the market incentives provided by the 'reputational' risk to firms for potential losses that may be only partially under their control. See for example Kierkegaard (2013), Dimick (2010) and Schwartz and Janger (2007).

Technical aspects including spectrum management

The soft law option does not make explicit provision for redrawing the legally defined boundaries of licensed spectrum, changing licence conditions or implementing new methods of spectrum allocation suited to making spectrum IoT-friendly, but is consistent with spectrum sharing and recontracting. Paradoxically, this informal mechanism for gaining access to spectrum may be more efficient that improved licensing, especially as far as innovation is concerned.

8.2.1. Hard law

The impacts of the hard law option will depend on the elements of law to be changed, the specific changes to be made, the 'route' taken (see Section 8.1.3), the extent and distribution of compliance and the costs associated with compliance and non-compliance. In addition, the hard law option will inevitably involve quasi-legal and non-legal actions[82] (at least in the medium term). Therefore, we shall consider the impacts from a more general perspective.

We consider actions taken under the hard law option as:

- concrete and explicit
- subject to detailed scrutiny by accountable bodies
- approved by relevant government institutions
- subject to mandatory assessment as to effectiveness, efficiency, 'regulatory fitness' and consistency with other policies including other changes proposed changes under this option
- subject to judicial (rather than market or technical) review, interpretation and modification, at least in the short to medium term.

They also have an unambiguous character and fixity that can provide a reliable commitment or signal of future conditions. In this sense, they can enhance actions by other stakeholders along the lines identified in assessing the impacts of the soft law option.[83] The legal and regulatory certainty provided is likely to stimulate development of the European IoT sector. This stimulus will come from investment encouraged by

[82] In this connection, we note that the Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Internet of Things (an Action Plan for Europe) (COM (2009) 278 final) created the basis for initiating dialogue on a range of IoT-connected issues (eg the 'silence of the chips') that could lead to hard law measures. This impetus was strengthened in the area of security by the accompanying recommendation, which outlined measures by Member States to make national legislation for RFID compliant with the EU Data Protection Directives 95/46, 99/5 and 2002/58 (No. 2).

[83] These are in architecture; economic impacts including competition and investment; ethics, education and values; governance; security and privacy; and technology including spectrum management.

reducing undiversifiable, unpredictable and non-tradable risks. It will also reflect collaboration within a reliable and clear legal framework for contractual negotiation. Looking to the future, the fixity afforded by legal measures is likely to stimulate innovation in the sense of generating and making available new inventions – by producing a solid framework for individual and collective property rights. It is also likely to stimulate 'soft' (business model, service and business process) and co-created or collaborative innovation by clarifying the rights of for example users, suppliers and other stakeholders to the IPR, revenue and service benefits of new IoT devices, services and business models and market arrangements. In addition, legal measures at EU level are likely to encourage other governance measures, including efforts by the Member States to eliminate harmful disparities in the way existing rules are implemented, together with self- and co-regulatory measures by industry and civil society organisations.

On the other hand, this same fixity, authority and explicit character may have some drawbacks. Legal measures are slow and cumbersome to change, especially when important stakeholders disagree. In some cases, the delays involved may be very costly – for instance if the rules do not reflect late-breaking developments, or if the initiation of legal processes forestalls swifter and possibly more finely tuned action by other stakeholders.

This potential drawback applies differently to the routes identified in Section 8.1.3; in particular, directives may be (and often are) implemented differently in Member States. While the directives establish clear boundaries for such variations, their significance in relation to market development and the effectiveness of consumer or citizen protection, for example, may depend as much on the profile of approximations across the Member States as it does on the specifics of implementing legislation in each Member State. This creates a tension between the advantages of a common framework, the potential costs of inappropriate homogeneity and the spill-over effects within different national legal regimes. For this reason, hybrid ('new comitology') measures – which offer additional advantages in level of detail and speed of creation, implementation and modification – may be particularly valuable.

Finally, it should be mentioned that the basis for any intervention, particularly for legal intervention, needs to take account of subsidiarity and proportionality. As discussed above (in Section 6.1), the subsidiarity case seems strong, especially in light of the functioning of the internal market.

Proportionality is more nuanced; at the level of generality at which the hard law option is expressed, it can be linked to a specific set of criteria – some of which may need detailed assessment for specific measures within this option:

- The risk that the option goes beyond what is necessary satisfactorily to achieve the objectives can be minimised by the multi-stakeholder nature and explicit scrutiny provisions built into the hard law processes.
- In general, it cannot be guaranteed the scope of action is limited to those aspects that Member States cannot achieve satisfactorily on their own, and where the Union can do better, because the boundaries in some areas are not wholly clear and may be changing.
- The financial or administrative cost for the Union, national governments, regional or local authorities, economic operators and citizens should be minimised and commensurate with the objective; again, this should always be considered, but it is important to recognise that changes in the IoT itself may change the magnitude and incidence of these costs.
- The range of routes identified leaves Member States with the greatest possible scope for national decision while achieving satisfactorily the objectives set. In addition to the 'new comitology' aspect discussed above, it is reasonable to expect that some of the objectives (especially accountability, competition, ethical soundness and inclusivity) are difficult to ensure by pan-European measures alone; therefore the satisfactory achievement of these objectives by legal means depends on locally appropriate legal action crafted and implemented by local – and locally accountable – authorities. In this way, the hard law option's mix of directives and regulations will respect both Community law and well-established national arrangements and special circumstances.
- Because the option is intended to work as far as possible along 'IoT-aware' rather than 'IoT-specific' lines – revising and amending existing legal frameworks, rather than implementing IoT specific legislation, at least until more evidence and experience have been accumulated – the form of Community action will be as simple as possible and coherent with satisfactory achievement of the objective and effective enforcement.[84]
- Finally, the inclusion of a co-regulation route (route 6 in Section 8.1.3) will help ensure that whatever route is chosen will have a solid justification; indeed, in view of the dynamic (albeit fragmented) nature of stakeholder governance action in or affecting standardisation of the IoT, for example (see Section 4.4), the impact assessment for any legal measure should take continuing self- and co-regulation into explicit account as part

[84] In particular, the REFIT initiative should provide a framework and political justification for the hard law option.

of the baseline assessment and (following route 6) as an option in its own right.

8.3. Comparison of options

8.3.1. Effectiveness

Formally, effectiveness refers to 'the extent to which the options achieve the objectives discussed' (Impact Assessment Guide, 2009, p. 48), as discussed in Section 6.3. We start with an overall characterisation of the options before comparing the effectiveness of each objective.

The *laissez-faire* approach of Option 0 implies that no IoT-specific actions are undertaken at the EU level. Developments in the IoT sphere will thus follow the preferences of market actors and/or Member State governments and are likely to be fragmented along national, policy area and/or sectoral lines. There is no guarantee that these would be entirely in line with EU policy objectives or European values, nor would the problems identified above necessarily be addressed. In other words, the 'do nothing' option offers no assurances with respect to effectiveness.

The soft law approach of Option 1 (including each of the three main streams of action – watching brief, innovation policy and industrial option) is more likely to be effective. It ensures that the objectives will be reached; compliance with the goals established by the soft law options is not binding on IoT market participants. However, wide participation in formulating soft law objectives and measures should produce a high degree of buy-in and internalise trade-offs among different interests. Assuming that the guidance provided by the soft law option offers sufficient incentives for adoption and compliance (eg by facilitating compliance with existing legislation, improving quality of products or services, or stimulating IoT uptake by providing consumers with sufficient trust), the effectiveness of this option can be very high.

Finally, the hard law option (Option 2) can be highly effective, given that compliance with requirements imposed through legislation is mandatory. The effectiveness of this option is thus only bounded by the ability of legislators to codify the objectives into law, and by the ability to enforce the resulting legislation on the relevant market players. However, the legislative evaluation and scrutiny process can be cumbersome, and is not easily restarted; thus the hard law option carries some risk of unintended negative consequences or rigidities that inhibit the response of the IoT to new developments.

The effectiveness of the three options in relation to the strategic objectives described in Section 6.3 is summarised in Table 8.2.[85]

Table 8.2 The extent to which the different options are likely to attain objectives

Objective	Option 0, do nothing	Option 1, soft law	Option 2, hard law
Accountability	Fragmented, ad hoc accountability; little involvement of accountable bodies	Informal accountability reinforced by market and political forces (voting with one's feet)	Highest level of accountability ensured by formal legal and legislative processes
Interoperability	Primarily directed towards existing value affiliations and the formation of competing closed clusters	Mutual agreement will end trend towards non-interoperable standards	Some standards and forms of exchange can be legally enforced, but flexibility and adjustment may be compromised
Inclusivity	Trend to include and serve the most commercially attractive social groups matched with the most remunerative services	Self-organising and self-regulatory inclusion reinforced by support for multistakeholderism including lay representation	Formal legal barriers to participation will be removed, but may be replaced by less obvious informal ones (eg exclusionary standards, non-neutrality)
Ethical soundness	Ongoing and unresolved conflict between ethical, commercial and political agendas; development of 'ethics by design' inhibited by lack of value proposition	Alignment of soft-law policies can encourage ethical business models and services, but some risk of lock-in (eg privacy attitudes and behaviour unable to drive new technology)	Explicit incorporation of ethical norms in legal and regulatory frameworks; recasting of eg security and privacy to reflect IoT specifics

[85] Red cells – objective likely to be a compromise; yellow cells – little improvement or substantial uncertainty; blue cells – modest progress towards objective; green cells – best outcome from this perspective.

Objective	Option 0, do nothing	Option 1, soft law	Option 2, hard law
Safety	Only monetised elements of safety provided; no liability rule adjustment	Bargaining across policy and interest domains and adoption of binding codes of conduct or certification	Legal underpinning for safety improves trust, but may be cumbersome and discourage innovation
Openness	Current tussle between players at different point in value chain persists; hard to predict equilibrium	Adoption of openness as an architectural principle across many policy and action domains enhances 'right kind' of openness (including open innovation)	Legal enforcement for eg neutrality principles and open competition rules, but potential for preventing access restriction as an incentive device or inhibiting innovation
Competitiveness, competition	Current tendency towards tipping and foreclosure reinforced by predatory behaviour of globally dominant players and legacy incumbents; potential for double marginalisation	Tussle allows balance of market and non-market competition; strengthens position of SMEs and flexible networks; provides testbed for new global IoT governance arrangements	Competition laws create level playing field – but within existing market boundaries may create 'high-cost' IoT that weakens competitiveness (or lead way to global balance)

Key:

	Objective likely to be a compromise
	Little improvement or substantial uncertainty
	Modest progress towards objective
	Best outcome from this perspective

8.3.2. Efficiency

Efficiency refers to 'the extent to which objectives can be achieved for a given level of resources/at least cost (cost-effectiveness)' (Impact Assessment Guide, 2009, p. 48). Option 0 *may* achieve some of the objectives (eg interoperability, inclusivity and openness) but there are no guarantees. While it is efficient from the perspective of market players (who would be free to develop their IoT products and services as they see fit), it seems likely that

the costs of doing so will be shifted to others (eg customers or other parts of the value chain) who may not be the most effective actors in meeting these objectives.[86] Alternatively, the actions needed to make progress towards the objectives may be provided by the most efficient parties, but in exchange for excessive payments reflecting their unique advantages. Further inefficiencies may arise from country fragmentation, duplication and coordination problems.

The multi-stakeholder negotiation that underpins the soft law option should enable inefficiencies arising from national fragmentation to be negotiated away, but may suffer additional costs and other distortions due to issue fragmentation and 'stovepiping' among the players. National differences should be limited because the objectives can be more or less clearly (compared with Option 0) reflected in soft law measures at EU level. There may be additional advantages relative to the hard law option, because market players still retain some freedom in assessing how best (or whether) to comply with these measures. In other words, the soft law option provides incentives for compliance with policy objectives, but allows market players to assess the socioeconomic efficiencies of compliance – or at least those parts that they can monetise and those elements they are compelled to incorporate by norms and informed consumer choice.

The hard law option provides greater assurance of progress towards those objectives for which there is a legal basis. This may not be enough to guarantee an attractive cost–benefit ratio. There may be inefficiencies stemming delay, costs, excessive burdens and potentially inappropriate or inflexible provisions. Moreover, for cases where legal evidence is hard to obtain and remedies difficult to enforce, levels of compliance may actually be lower than they are under a soft law approach. Generally, the hard law option is only likely to be efficient in a broad sense (taking external impacts into account) if legislators can ensure that they impose – or retain – only those obligations which are strictly necessary to achieve the objectives. For the IoT this is not a trivial requirement, given the current uncertainties in the anticipated evolution and adoption of the IoT.[87] Any regulation therefore risks overburdening IoT service providers, imposing obligations that do not match future market developments or missing problems that significantly impair the legal position of European consumers. Given the cost of correcting such errors (redrafting dysfunctional

---

[86] For example, inclusivity, ethical protection or safety may be provided by service providers under eg universal service obligations in exchange for favourable regulatory treatment at Member State level, for example, but this may crowd out 'by design' solutions or fail to deliver uniform benefits across market segments and regions.

[87] For instance, data breach disclosure requirements, which are burdensome and arguably of ambiguous benefit in many current settings (eg cloud computing), may be replaced by technical or standards approaches of greater effectiveness at lower – and better-allocated – cost; see for example Cave et al. (2012).

legislation and compensating service providers), hard law options are less likely to prove optimally efficient, at least not until market developments are clearer.

8.3.3. Coherence

Coherence refers to 'the extent to which options are coherent with the overarching objectives of EU policy, and the extent to which they are likely to limit trade-offs across the economic, social, and environmental domain' (Impact Assessment Guide, 2009, p. 48). The *laissez-faire* option 0 offers little assurance of either consistency with existing law or useful trade-offs. As shown in Section 7, the current trajectory of development of the IoT market is in many ways out of step with EU policies set out in linked areas (such as e-commerce, electronic communications or cyber security). Moreover, existing legal and policy frameworks drawn up in relation to a pre-IoT world may not be future-proof; for instance, the emergence of autonomous systems and the implied transfer of authority away from end-users, service providers and even infrastructure providers may reduce the coherence of existing rules as applied to the IoT. On the other hand, the perpetuation of existing boundaries between jurisdictions and legal instruments may effectively prevent the recognition and optimisation of trade-offs (eg the degree to which societal or environmental objectives could be reached by recasting privacy rules to protect only essential interests or to improve the ability of data subjects to authorise information transfers).

A soft law approach is likely to fare better as regards coherence, as the guidance provided to the IoT market and other multi-stakeholder fora can take into account existing policies, regulations and practices in such ancillary policy areas. The open terms of soft law policy coordination may be particularly friendly to trade-offs and the joint optimisation of economic, societal and environmental objectives.

A hard law approach can similarly be highly effective when the focus is on revising and possibly amending existing legislation, since coherence with existing policies is then the basis for legislative action. Entirely new and ad-hoc initiatives on the other hand (adopting new and IoT specific legislation) risks endangering policy coherence, as the IoT may become subject to isolated specific obligations that differ significantly from choices made in related EU policy areas.

PART V Proposal for action

9. Policy recommendations

As the description of the policy options and the comparative analysis in Section 8.3 makes clear, these options entail many sub-options and constitute policy approaches or strategies rather than specific actions. This is appropriate in view of the dynamism and uncertainty of IoT development and of the broader policy, technology, societal and economic contexts within which it operates. Therefore, these options may best be regarded as portfolios or as real options.[88] From this perspective, the soft law option is recommended over the others; it does not preclude inaction or even withdrawal in situations where this is warranted, or hard law measures when warranted, but it also provides for realignment of responsibilities and liabilities, gathering further information and widening participation by key stakeholders in order to balance potentially divergent objectives. In addition, as noted in Section 8.1, it makes explicit provision for switching between elements of *laissez-faire* and hard law as circumstances change.

It offers an attractive balance of effectiveness and flexibility, as shown in Section 8.2, with optimal effectiveness in four of seven options and near-optimal effectiveness in the others.

It is also more likely to be cost-effective in a broad sense. Compared with Option 0, Option 1 has a greater ability to ensure that external costs are internalised when negotiating and enforcing soft-law options; compared with Option 2, Option 1 allows costs and burdens to be realigned to match stakeholder objectives and powers of action – this diversifies costs and optimises compliance. As regards coherence, it is weaker in the short run at ensuring consistency with pre-existing overarching goals than Option 2, but creates a platform for identifying and attaining beneficial trade-offs among those objectives and – in the long run – providing a basis for increasing the internal consistency of the set of overarching policy goals.[89]

---

[88] A real option is having the right – but not the obligation – to choose between alternative courses of action arising as a result of a prior decision. Its value or impact thus derives from the future decisions that it makes possible (or prevents) rather than its immediate or certain consequences.

[89] This refers to the fact that some existing tensions – eg between open standards and security – may disappear in the face of the kind of technological, commercial and societal evolution that the IoT promises to enable.

These options are not simply means for addressing 'problems' created by the emergence of the IoT. As has become clear from our analysis, the IoT domain is 'new' and needs the space to evolve. While IoT specific legislation at this point may be superfluous or premature, the European Commission maintains an important role in guaranteeing fundamental rights and values in all settings, including that of the IoT. Therefore, it is necessary to consider a potential role for DG CONNECT and IoT policy in coordinating different policy areas and ensuring healthy and efficacious **societal debate on IoT**-specific issues across all areas concerning emerging technologies. The preferred policy option offers the greatest potential for this to develop, because it neither prescribes nor precludes this form of governance brokerage.

At a more general level, attention and suitable soft law actions are needed to:

- create space for IoT development
- address gaps in the legal and regulatory framework
- monitor for the emergence of specific IoT-related issues.

In addition, a number of 'soft law' policies can accelerate or improve the development of the IoT market:

- support R&I
- share knowledge
- provide meaningful digital literacy programmes
- raise awareness of IoT
- create a European 'ethical tech' brand
- encourage more broad-based participation and competition through governance experiments
- provide financial support
- provide more general oversight
- create an ethical charter.

Our policy recommendations are described below.

1 Create space for IoT development

The discussion in Section 7[90] in particular demonstrates the potentially adverse consequences of fragmented decisionmaking and lack of coherence across sectors and policy areas. To encourage the 'self-repair' of these gaps, the EU can usefully act to:

[90] Especially sections 7.1, 7.3, 7.4, 7.8 and 7.10.

- coordinate policy dialogue across sectors and continue the IGF debate with all stakeholders on global level in order to ensure a common and dynamic understanding of the issues related to IoT
- stimulate development of global standards by the stakeholders, through participation in standardisation activities by the EC itself and by members of EU-sponsored research and technology development (RTD) and deployment projects, and by incorporation of standards in public procurement, especially in relation to public e-services
- consult on the broader development, adoption and implementation of corporate social liability rules, making industry aware of need for self-regulation ('good citizenship').

2 Address gaps in the legal and regulatory framework

The analysis in Section 7[91] also highlights the existence of gaps, duplications and inconsistencies in the framework of regulations affecting or affected by the IoT. To improve regulatory fitness in relation to the IoT within the soft law framework, the EU can usefully continue to test IoT developments against relevant existing and emergent legislation (eg by incorporating IoT and soft law options explicitly within ReFit analyses and impact assessments) in order to provide clarity where necessary, and help to ensure that regulation (including at Member State level) is minimised and kept flexible unless and until it proves to be necessary to address otherwise intractable problems and/or to allow innovation to flourish.

3 Monitor for the emergence of specific IoT-related issues

For example, these might arise in relation to big data, 'spectrum availability' or 'autonomous actuators'.[92]

4 Support R&I

Support and promote research and validation projects for identification, privacy and ethics in IoT environments (eg future and emerging technology, the Competitiveness and Innovation Programme (CIP) and Horizon 2020), in addition to research and validation projects aimed at future internet such as trusted infrastructures, security and resilience, interoperability and so on. Within the future internet R&I roadmap a specific focus on IoT seems to be in place – to be related to the different environments in which IoT deployment seems to be promising – the roadmap could also make specific links to

[91] Especially sections 7.1, 7.2, 7.3, 7.4, 7.6, 7.7 and 7.9.

[92] See for example sections. 3.1, 4.3.2, 4.4.3, and the stakeholder perspectives in Section 5.1.

ongoing and planned initiatives. One example is provided by the Future Internet Public–Private Partnership[93] (FI-PPP) – there are strong links between its generic enablers and the IoT and possibly new use case requirements to ensure that the FI-WARE[94] core architecture serves the IoT properly.

5 Share knowledge

There is scope for exchange of experiences with the development and deployment of IoT environments for specific applications, such as AAL, environmental care, road safety, domotics and so on. More actively, there is scope for R&I initiatives that could provide platforms for developing 'horizontal' IoT capabilities that jointly support the implementation of AAL, e-health and so on.

6 Provide meaningful digital literacy programmes

These should be aimed at developers, making IoT developers aware of the legal and ethical framework they are working in, so as to empower self-regulation.

7 Raise awareness of IoT

Introduce initiatives aimed at making citizens aware of the existence of IoT, how it may affect their lives and what they may do to optimise these effects.

8 Create a European 'ethical tech' brand

Encourage innovators and providers to develop ethical technology in line with market and used needs. This could be an important way for businesses to add value to their brand, and would also allow consumers to determine which companies hold ethical principles in high regard. The objectives would be to foster a value-added strategy much like what has happened for green tech over the last decade.

9 Encourage more broad-based participation and competition through governance experiments

The IoT is not simply a technology employed by suppliers to improve service delivery and profitability. Much of its disruptive potential comes from its ability to subvert (or invert) power relationships by giving owners of untethered devices the power to interact in

---

[93] The FI-PPP is a Digital Agenda initiative intended to facilitate the evolution of the future internet in ways that advance overarching European objectives. It combines three essential elements: a technology foundation (the FIWARE Core Architecture and generic enablers), a set of specific use cases, and a capacity-building component. For more information, see https://ec.europa.eu/digital-agenda/en/future-internet-public-private-partnership.

[94] FI-WARE is the cornerstone of the FI-PPP programme, a joint action by the European industry and the European Commission delivering the core platform for the future internet.

powerful and relatively uncontrolled ways with others and with systems. Therefore, the business and service models that could arise on the IoT may not fit well within existing approaches and may be actively resisted (through attempts to lock down standards, competition and information as discussed elsewhere in this report) by today's incumbents. Suitable interventions could enable more broad-based participation and competition. Especially helpful in this respect would be a 'sandbox' initiative in which commercial, public sector and civil society stakeholders could 'play' with different arrangements in an environment that is (by design) trusted, secure and capable of capturing innovations.[95]

10 Provide financial support

Although not directly analysed here, some specific forms of venture capital support could address potential roadblocks to the commercial development of the IoT. Specifically, vertical impediments may arise because the IoT will produce even greater volumes of time-sensitive, highly dispersed and possibly highly differentiated data whose value is not easy to capture because the data come from individual, independent devices and semi-autonomous systems (who cannot be charged) while the value comes from the collective or aggregated analysis and re-use of those data. This will put further pressure on (hard and soft) internet infrastructure investment models. 'Data neutrality' rules to preserve openness may only make this worse. At least the struggle for bandwidth between different providers and users of content or communications pits like against like. A struggle between people and machines for use of the internet is much more unequal, and might result in human users being asked to subsidise ever-greater volumes of M2M traffic. To preserve investment capital that matches expected demand for capacity, forms of partnership investment could be devised that combine the partnership style of working and extended time horizons of venture capital with the flexibility of value co-creation and monetisation forms found in modern internet business models (eg search-based value networks). The public stake would provide risk underwriting and a component of assured demand (via public procurement) in exchange for co-regulatory responsibility sharing (shared governance) and options on jointly produced IP.

11 Provide more general oversight

Beyond monitoring for IoT issues in specific application domains (Recommendation 3) there is a need for a more general oversight or observatory to assess foreseeable and emergent risks. For instance, it may become necessary to develop new policy in an area concerned with autonomous decisions taken by machines. The question of who is or should be liable may challenge existing regulatory assumptions – the chain of causation

[95] A similar mechanism was used to explore 'data mashing' – recombinant reuse of public information in connection with the UK's Data Grand Challenge.

may stretch back from the operators and owners of communicating machines to the suppliers or even designers. The problem is not wholly new; deaths have been caused by robots in industrial environments since 1979. But the IoT changes the problem and may facilitate novel solutions. This could start at a fundamental or systemic level by ensuring that principles of good protective governance to preserve human safety are embedded in the architecture of the IoT. To illustrate this shift, consider autonomous vehicle technologies and advanced driver assistance systems; because these technologies increasingly perform driving functions, they require a shift in responsibility from the driver to the vehicle itself – its design and the architecture of the traffic systems in which these 'driverless' or 'assisted-driver' vehicles operate.

12 Create an ethical charter

In a similar vein, soft law actions to promote 'ethical branding' (Recommendation 8) could be extended to support the creation of an ethical charter that would safeguard vital interests of consumers in IoT environments, offer guidance to developers of IoT environments and services (even ethical impact assessments before development).[96] The development and implementation of such a charter is one potential consequence of a continuing programme[97] of research and debate on the ethical, legal, social and environmental aspects of ICT, specifically as regards the IoT.

[96] We note that this recommendation did not receive consistent support among those responding to the EC public consultation on the development of the IoT. This was because of a division among those who felt the proposals did not go far enough, those concerned about its feasibility and those who doubted that it could work without a stronger overarching governance structure, rather than a repudiation of the principle. See http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.

[97] Such a programme is recommended by the European Group of Ethic's Opinion 26 published in February 2012 and recent statements by Commissioner Kroes. These call for broad societal debate on trade-offs among comfort, security and privacy in order to promote a conscious development of an IoT world people would want to live in.

10. Implementation and monitoring strategy

10.1. Introduction

The policy interventions recommended in this report reflect the state of development and evolving character of the IoT, thus it would be premature to specify precise implementation and monitoring strategies. However, it is appropriate to anticipate some aspects that apply both to specific measures and more generally to policy responses and policymaking with regard to the IoT.

10.2. Implementation

As mentioned before, the IoT overlaps with the internet, which in turn overlaps with telecommunications, innovation and other ICT-related policy and regulatory domains. Therefore, **there is a need to develop and implement policy in conjunction with those other contexts**. This requirement applies as well to *ex ante*, interim and *ex post* assessment.

Beyond these overlaps within the ICT domain, the IoT evolves in a wider context of policies relating to cross-cutting issues such as privacy, data protection, security and consumer protection. Not all of these areas lie specifically within the internet domain, or indeed fall under the remit of traditional entities such as telecom regulators, ministries of communications or DG CONNECT. There are many policy areas outside the remit of DG CONNECT in which the IoT is (or will be) an essential part of the problem and/or may be crucial to solving policy problems. One of the more troubling challenges is to find a useful *modus vivendi* between those stakeholders who are 'internal' (to the Commission) – with their deep knowledge of specific policy areas – and DG CONNECT – with its deep knowledge of the impacts (societal, technical, but also economic) of those technologies and the forces that drive their adoption, adaptation and impacts. Without a relationship built on partnership and complementarity (rather than rivalry) the problems will not be addressed effectively and the potential of the technologies not fully realised. One approach to this problem of constructive engagement involves a three-fold initiative:

- to develop a method to identify and prioritise such areas
- to conduct a set of 'deep dive' investigations to begin building a network of collaborators and demonstrate the concept

- to develop an evidence base, toolkit and strategy for engagement.

This is not just a matter for the future. The 'policy footprint' of the IoT goes beyond abstract policy areas. There are many existing and pending legal instruments (ranging over directives, regulations and delegated acts) that may need to be modified in light of the IoT to ensure their continued effectiveness or to withdraw from areas where technological and socioeconomic developments associated with the IoT substantially weaken the case for intervention or change the associated administrative burdens. This suggests the inclusion of an **IoT component in progress under the REFIT initiative**.

10.3. Monitoring and evaluation

10.3.1. Measure-specific indicators

There are obviously specific indicators associated with particular policy measures: key success factors; critical risks; measureable indicators of progress towards specific and implementation objectives; inputs; outputs; and outcomes. These should be developed in conjunction with DG CONNECT's 'Metrics' initiative.

10.3.2. IoT development indicators

The range of uses to which IoT devices and services are put should be mapped by measuring the intensity of such use (**using adoption data**) against a fixed set of application areas and a standardised set of functionalities (refining a division between data capture or sensing, data exchange, data processing, actuators).

This should be complemented by **tracking data on the use of 'non-IoT' means of providing similar functions**. Where IoT devices (eg in the form of sensor nets or swarms) are specifically used to provision systemic functions (eg traffic or energy routing, logistic flows and so on) **panel data** (over time and across regions, sectors and entities) can be captured **to support impact modelling**.

Commercial data on payments and costs can be collected from existing data sources (eg Amadeus) and used to support return-on-investment analysis of investment in IoT infrastructures and IoT services.

These examples relate to a need for better data on the 'footprint' and impacts of the IoT. These requirements are summarised in Table 10.1.

Table 10.1 Indicators for the IoT, their sources and how they are collected

Data item	Indicator of	Who collects (sources)	How
M2M traffic	Volumes, structure (network pattern of flow by origin, destination, time and volume); particular focus on cross-border flows (a separate indicator based on data retention information if available)	Internet service providers and network operators	Inclusion of standardised headers
IoT service availability	Indicators of IoT services available on subscription or commercially (terms, functions, tariffs) and of the distribution and ownership of IoT devices For each service, an indicator of cross-border availability and roaming charges or function and capacity limits (if any)	NRAs, business databases, monitoring organisations (eg SamKnows, NetIndex)	Electronic market surveillance, crowd-sourced end-user reporting
IoT value network	Stakeholder connections and relations, value creation and capture (costs and payments)	Business databases	Analysis of corporate reports and disclosure statements
IoT market development	Number and size (revenues, turnover, market share) of device, service, suppliers, integrators, end-users (count of devices)	Business registries (eg Datastream, AMADEUS)	Electronic search of public records
Importance or necessity of IoT	Potential demand, elasticity of substitution, opportunity cost of development	Surveys, business consultancies (eg Cullen, IDC),vice-chancellors, academics	Market studies, econometric studies, meta-analysis
Innovation associated with IoT	RTD expenditures Patents and renewals Joint ventures Mergers and acquisitions	Patents, Community Innovation Statistics data, alliance databases (eg Merit-CATI)	Text-based search of records of patents, joint venture agreements
Competitiveness and competition	National map of IoT provision and use	Based on traffic, availability and pricing data	Geographic information system representation

10.3.3. IoT observatory

For the potential (good or bad) impacts foreseen in this document but not directly measured (especially ethics, privacy, security and other 'challenges' noted in Section 9) an observatory should be created to create an evidence base for possible future policy change (including hard law action when needed) and research. This would capture such easily available data as:

- legal and regulatory 'mentions' of IoT based on electronic searches of identified authoritative sources
- examples of progress towards and effectiveness of implementation drawn from the logical frameworks and evaluation and monitoring strategies of specific initiatives, identified by electronic surveillance of official websites
- standards relating to or specifically about the IoT based on periodic progress reports and publications of the main standards bodies
- national (government), industry and third sector initiatives based on a network of industry, civil society and government entities, identified through participation in IoT-themed conferences, workshops and 'grey' literature.[98]

[98] This last element is indicative, and therefore should strive for coverage rather than comprehensiveness or statistical representativeness.

Reference list and bibliography

Aarts, E. and Grotenhuis, F. 'Ambient Intelligence 2.0: Towards Synergetic Prosperity', in *Proceedings of the European Conference on Ambient Intelligence*, Berlin: Springer, 2009, pp.1–13.

Aghion, P., Dewatripont, M., Du, L., Harrison, A. and Legros, P. *Industrial Policy and Competition*. National Bureau of Economic Research, 2012.

Alam, S., Chowdhury, M. M. R. and Noll, J., 'Interoperability of Security-Enabled Internet of Things', *Wireless Personal Communications*, Vol. 61, 2011, pp.567–86.

Anderson, R. and Moore, T., 'The Economics of Information Security', *Science*, Vol. 314, No. 5799, 2006, pp.610–13.

Andrade, N., 'Future Trends in the Regulation of Personal Identity and Legal Personality in the Context of Ambient Intelligence Environments: The Right to Multiple Identities and the Rise of the Aivatars', in Muller, S., Zouridis, S., Frishman, M. and Kistemaker, L. (eds) *The Law of the Future and the Future of Law*, FICHL Publication Series, No. 11, Oslo: Torkel Opsahl, 2011, pp.567–85.

Andrade, N., 'Oblivion: The Right to Be Different from Oneself: Reproposing the Right to Be Forgotten', paper given at VII International Conference on Internet, Law & Politics: Net Neutrality and Other Challenges for the Future of the Internet, *IDP. Revista de Internet, Derecho y Política*, 2012, pp.122–137.

Arabo, A. and El-Mousa, F., 'Security Framework for Smart Devices', paper given at Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) International Conference, 2012.

Ars Technica. 'Insecure Routing Redirects YouTube to Pakistan', 25 February 2008. Available at: http://arstechnica.com/uncategorized/2008/02/insecure-routing-redirects-youtube-to-pakistan/ (accessed 1 April 2013).

Assaf, D., 'Models of Critical Information Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, Vol. 1, 2008, pp.6–14.

Babar, S. et al., 'Proposed Embedded Security Framework for Internet of Things (IoT)', paper given at Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) 2nd International Conference, 2011, pp.1–5.

Balmaseda, M. A., Trenbert, K. E. and Kallen, E., 'Distinctive Climate Signals in Reanalysis of Global Ocean Heat Content', *Geophysical Research Letters*, 25 March 2013.

Bao, F. and R. Chen, 'Trust Management for the Internet of Things and its Application to Service Composition', paper given at World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium, 2012, pp.1–6.

Batchelor, R., Bobrowicz, A., Mackenzie, R. and Milne, A., 'Challenges of Ethical and Legal Responsibilities When Technologies' Uses and Users Change: Social Networking Sites, Decision-Making Capacity and Dementia', *Ethics and Information Technology*, Vol. 14, No. 2, 2012, pp.99–108.

BIS, *Information Security Breaches Survey 2013: Technical Report*, London: Department for Business, Innovation and Skills, 2013, https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report (accessed 23 May 2013).

Bohn, J., Coroamă, V., Langheinrich, M,. Mattern, F. and Rohs, M., 'Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing', in Weber, W., Rabaey, J. and Aarts, E. H. L. (eds) *Ambient intelligence*, Berlin: Springer, 2005, pp.5–29.

Boyatzis, R. E., Stubbs, E. C. and Taylor, S. N., 'Learning Cognitive and Emotional Intelligence Competencies Through Graduate Management Education', *Academy of Management Learning & Education*, Vol. 1, No. 2, 2002, pp.150–62.

Bradley, J., Barbier, J. and Handler, D., *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, CISCO, 2013, available at http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf (accessed 23 May 2013).

Brown, I. and Adams, A. A., 'The Ethical Challenges of Ubiquitous Healthcare', *International Review of Information Ethics*, Vol. 8, No. 12, 2007, pp. 53–60.

Cáceres, R. and Friday, A. 'Ubicomp Systems at 20: Progress, Opportunities, and Challenges', *Pervasive Computing, IEEE*, Vol. 11, No. 1, 2012, pp.14–21.

Cadzow, S. W. 'Privacy – The Forgotten Challenge in Sensor and Distributed Systems', paper given at IET Conference on Wireless Sensor Systems (WSS 2012), 2012.

Califf, M. E. and Goodwin, M., 'Effective Incorporation of Ethics Into Courses that Focus on Programming', *ACM SIGCSE Bulletin*, 2005, pp.347–51.

Callaghan, V., Clarke, G. and Chin, J. 'Some Socio-Technical Aspects of Intelligent Buildings and Pervasive Computing Research', *Intelligent Buildings International*, Vol. 1, No. 1, 2009, pp.56–74.

Casagras. *Final Report*, 2011.

Cave, J., Marsden, C. and Simmons, S., *Options for and Effectiveness of Internet Self- and Co-regulation*, RAND Technical Report TR-566-EC, Santa Monica, CA: RAND, 2008.

Cave, J. et al., *Does It Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy*, final report, European Parliament, 2011, available at http://www.europarl.europa.eu/committees/fr/studiesdownload.html?languageDocument=EN&file=65871 (accessed 23 May 2013).

Cave, J., Robinson, N., Kobzar, S. and Schindler, R., *Regulating the Cloud: More, Less or Different Regulation and Competing Agendas*, 2012, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031695 (accessed 29 May 2013).

Cave, M., 'Encouraging Infrastructure Competition via the Ladder of Investment', *Telecommunications Policy*, Vol. 30, 2006, pp.223–37.

Chen, Y., Paxson, V. and Katz, R. H., *What's New About Cloud Computing Security?*, University of California, Berkeley Report No. UCB/EECS-2010-5, Vol. 20, No. 2010, 2010, pp.2010–15.

Chui, M., Löffler, M. and Roberts, R., 'The Internet of Things', *McKinsey Quarterly*, Vol. 2, 2010, pp.1–9.

Cochran, P. L., Tatikonda, M. V. and Manning Magid, J., 'Radio Frequency Identification and the Ethics of Privacy', *Organizational Dynamics*, Vol. 36, No. 2, 2007, p.217.

COMREG, 'Numbering for Machine-to-Machine Communications', Commission for Communications Regulation, Ireland, ComReg 13/33, 28 March 2013.

Connolly, R. W., 'Beyond Good and Evil Impacts: Rethinking the Social Issues Components in our Computing Curricula', *Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education*, 2011, pp.27–9.

Courtois, N. T., 'The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime', presented at the Workshop on RFID Security 2009 (RFIDSec 09), 2009.

Creese, S., Hopkins, P., Pearson, S. and Shen, Y., 'Data Protection-Aware Design for Cloud Services', *Proceedings of the First International Conference on Cloud Computing*, 2009, pp.119–30.

Dark, M. J. and Winstead, J., 'Using Educational Theory and Moral Psychology to Inform the Teaching of Ethics in Computing', *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, 2005, pp.27–31.

Daskala, B., *Looking Through the Crystal Ball – Identifying Future Security, Privacy and Social Risks in a Prospective IoT Scenario*, 2010, available at https://www.nics.uma.es/seciot10/files/ppt/daskala_seciot10.pdf (accessed 29 May 2013)..

De Hert, P. *A Right to Identity to Face the Internet of Things?* 2008a, available at http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf (accesssed 30 May 2013).

De Hert, P., 'Identity Management of e-ID, Privacy and Security in Europe: A Human Rights View', *Information Security Technical Report*, Vol. 13, No. 2, 2008b, pp.71–5.

de Leusse, P., Periorellis, P., Dimitrakos, T. and Nair, S. K., 'Self Managed Security Cell: A Security Model for the Internet of Things and Services', *Advances in Future Internet, 2009 First International Conference*, 2009, pp.47–52.

DiBiase, D., Goranson, C., Harvey, F. and Wright, D., 'The GIS Professional Ethics Project: Practical Ethics Education for GIS Pros', paper presented at the 24th International Cartography Conference, Santiago, Chile, 2009.

Dimick, C., 'No Harm Done? Assessing Risk of Harm under the Federal Breach Notification Rule', *Journal of AHIMA*, Vol. 81, No. 8, 2010, pp.20–5.

Dodge, M. and Kitchin, R., 'Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting', *Environment and Planning B*, Vol. 34, No. 3, 2007, pp.431–45.

Doukas, C. et al., 'Enabling Data Protection Through PKI Encryption in IoT M-Health devices', paper given at the Bioinformatics & Bioengineering (BIBE), IEEE 12th International Conference, 2012, pp.25–9.

Edwards, C., 'Smart Dust, Engineering and Technology', *Engineering & Technology*, Vol. 7, Issue 6, 2012.

EGE, *Ethics of Information and Communication Technologies*, European Group on Ethics in Science and New Technologies to the European Commission, February 2012, available at http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ict_final_22_february-adopted.pdf (accessed 30 May 2013).

Eloff, J., Eloff, M., Dlamini, M. and Zielinski, M., 'Internet of People, Things and Services: The Convergence of Security, Trust and Privacy', paper given at 3rd CompanionAble Workshop, Brussels, 2 December 2009.

Emiliani, P. L. and Stephanidis, C., 'Universal Access to Ambient Intelligence Environments: Opportunities and Challenges for People with Disabilities', *IBM Systems Journal*, Vol. 44, No. 3, 2005, pp.605–19.

ENISA, *Flying 2.0: Enabling Automated Air Travel by Identifying and Addressing the Challenges of IoT and RFID Technology*, European Network and Information Security Agency, 2010, available at http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2 (accessed 23 May 2013)

Ess, C. M, 'Trust and New Communication Technologies: Vicious Circles, Virtuous Circles, Possible Futures', *Knowledge, Technology & Policy*, Vol. 23, Nos. 3–4, 2010, pp.287–305.

EUR-Lex, *A Digital Agenda for Europe*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2010, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT (accessed 23 May 2013).

Europa, 'Digital Agenda: Commission Consults on Rules for Wirelessly Connected Devices – the Internet of Things', press release, IP/12/360, 12 April 2012, available at http://europa.eu/rapid/press-release_IP-12-360_en.htm (accessed 23 May 2013).

European Commission, IoT_Privacy_201206.doc from the IoT EG portal (restricted access).

European Commission, 'Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive)', 2002, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF (accessed 23 May 2013).

European Commission, *Impact Assessment Guidelines*, 2009, available at http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf (accessed 30 May 2013).

European Commission, 'Article 29 Data Protection Working Party', press release, 14 July 2010, 2010a, available at http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf (accessed 23 May 2013).

European Commission, 'Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing', 0065/2010/EN, 2010b, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_en.pdf (accessed 23 May 2013).

European Commission, 'Data Retention', 2012a, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/review-of-data-retention-directive/index_en.htm (accessed 23 May 2013).

European Commission, *Impact Assessment*, SEC (2012) 72 final, 2012b, available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf (accessed 23 May 2013).

European Commission, *Report on the Public Consultation on IoT Governance*, DG for Communications Networks, Content and Technology, 16 January 2013.

European Commission, Digital Agenda for Europe, 'Scoreboard', n.d., available at https://ec.europa.eu/digital-agenda/en/scoreboard (accessed 23 May 2013).

Evans, P. C. and Annunziata, M., *Industrial Internet: Pushing the Boundaries of Minds and Machines*, General Electric, 2012, available at http://www.ge.com/docs/chapters/Industrial_Internet.pdf (accessed 24 May 2013).

Expert Group on the IoT, Factsheets set, 2012.

FEDMA, 'Self-regulation', Federation of European Direct and Interactive Marketing, n.d., available at http://www.fedma.org/index.php?id=56 (accessed 23 May 2013).

Fleisch, E., 'What is the Internet of Things? An Economic Perspective', *Economics, Management, and Financial Markets*, No. 2, 2010, pp.125–57.

Floridi, L., 'A Look Into the Future Impact of ICT On Our Lives', *The Information Society*, Vol. 23, No. 1, 2007, pp.59–64.

Garfinkel, S. L., *Security and Privacy*, Center for Research on Computation and Society, Harvard University, 2005, available at http://www.oecd.org/dataoecd/18/53/35473108.pdf (accessed 23 May 2013).

Gersch, M., Lindert, R. and Hewing, M., 'AAL-business Models: Different Prospects for the Successful Implementation of Innovative Services in the First and Second

Healthcare Market', *Proceedings of the AALIANCE European Conference on AAL*, Malaga, Spain, 11–12 March 2010.

Gheorghiu, R. and Unguru, M., 'Beyond Connectivity: Future Challenges for E-Inclusion Policies', *Romanian Journal of European Affairs*, Vol. 9, No. 2, 2009.

Grandison, T. and Sloman, M., 'A Survey of Trust in Internet Applications', *Communications Surveys & Tutorials*, Vol. 3, No. 4, 2000, pp.2–16.

Green, M., Drew, S., Carter, L. and Burnett, D., 'Submarine Cable Network Security', a presentation to APEC, Submarine Cable Protection Information Sharing Workshop, Singapore, 13 April 2009, International Cable Protection Committee, available at http://www.iscpc.org/information/Openly%20Published%20Members%20Area%20Items/Submarine_Cable_Network_Security_PDF.pdf (accessed 23 May 2013).

GRIFS, *RFID Standardisation, State of the Art*, Global RFID Interoperability Forum for Standards, 2010, available at http://www.grifs-project.eu/index.php/downloads/en.

Gumzej, N., 'Protection of Data relating to EU Consumers in the IoT Age', paper given at Software, Telecommunications and Computer Networks (SoftCOM), 20th International Conference 2012.

Gutwirth, S., 'Beyond Identity?', *Identity in the Information Society*, Vol. 1, No. 1, 2009, pp.122–33.

Haller, S. and Magerkurth, C., 'The Real-time Enterprise: IoT-enabled Business Processes', paper given at IETF IAB Workshop on Interconnecting Smart Objects with the Internet (March 2011).

Haller, S., Karnouskos, S. and Schroth, C., 'The Internet of Things in an Enterprise Context', in *Future Internet–FIS 2008*, Berlin: Springer, 2009, pp.14–28.

Haller, S., Magerkurth, C. 'The Real-time Enterprise: IoT-enabled Business Processes', paper given at IETF IAB Workshop on Interconnecting Smart Objects with the Internet, SAP Research Center St Gallen/Zürich SAP (Switzerland) Inc., March 2011.

Halperin, R. and Backhouse, J., 'A Roadmap for Research on Identity in the Information Society', *Identity in the Information Society*, Vol. 1, No. 1, 2008, pp.71–87.

Haselsteiner, E. and Breitfuß, K., 'Security in Near Field Communication (NFC)', paper given at Workshop on RFID Security, RFIDSec, 2006.

Heesen, J. and Siemoneit, O., 'Opportunities for Privacy and Trust in the Development of Ubiquitous Computing', *Ethical Challenges of Ubiquitous Computing*, Vol. 8, 2007, p.47.

Herrera-González, F., 'How Many Ladders of Investment?', *New Economic Papers*, 2011, available at http://econpapers.repec.org/paper/zbwitse11/52148.htm (accessed 30 May 2013).

Hildebrandt, M., 'Profiling and AmI', in *The Future of Identity in the Information Society*, Berlin: Springer, 2009, pp.273–310.

Hildebrandt, M., 'The Dawn of a Critical Transparency Right for the Profiling Era', in Bus, J., Crompton, M., Hildebrandt, M. and Metakides, G. (eds) *Digital Enlightenment Yearbook 2012*, Amsterdam: IOS Press, 2012.

Hochleitner, C., Graf, C., Wolkerstorfer, P. and Tscheligi, M., 'uTRUSTit: Usable Trust in the Internet of Things', in *Trust, Privacy and Security in Digital Business*, Berlin: Springer, 2012, pp.220–21.

Hofkirchner, W., 'How to Design the Infosphere: The Fourth Revolution, the Management of the Life Cycle of Information, and Information Ethics as a Macroethics', *Knowledge, Technology & Policy*, Vol. 23, No. 1–2, 2010, pp.177–92.

Hofkirchner, W., Tscheligi, M., Bichler, R. and Reitberger, W., 'Ambient Persuasion for the Good Society', *IRIE*, Vol. 8, 2007, pp.42–6.

Holzinger, A., Struggl, K. H. and Debevc, M., 'Applying Model-View-Controller (MVC) in Design and Development of Information Systems: An Example of Smart Assistive Script Breakdown in an e-Business Application, e-Business (ICE-B)', *Proceedings of the 2010 International Conference on 26–28 July 2010, Inst. of Inf. Syst. & Comput. Media (IICM), Tech. Univ. Graz, Austria*, 2010.

Hoorens, S. et al., *Towards a Competitive European Internet Industry: A Socio-Economic Analysis of the European Internet Industry and the Future Internet Public-Private Partnership*, European Commission, 2012.

Hussain, M. and Abdulsalam, H., 'Secaas: Security as a Service for Cloud-Based Applications', *Proceedings of the Second Kuwait Conference on e-Services and e-Systems*, 2011, p.8.

IGF, Transcript of the Annual Meeting of the Internet Governance Forum, 2011, available at http://www.intgovforum.org/cms/2011-igf-nairobi (accessed 23 May 2013).

IGF, *Dynamic Coalition on the Internet of Things*, Internet Governance Forum, 2012, available at http://www.intgovforum.org/cms/component/content/article/118-dynamic-coalition-proposals/1217-dynamic-coalition-on-the-internet-of-things (accessed 23 May 2013).

Internet of Things Architecture, IoT-A Project Deliverable D1.2 – Initial Architectural Reference Model for IoT, 2011.

Internet of Things Architecture, IoT-A Project Deliverable D1.3 – Updated reference model for IoT v1.5, 2012.

Internet of Things Architecture, IoT-A Project Deliverable D6.2 – Updated requirement list, Jan 2011

ITU, *ITU Internet Reports 2005: The Internet of Things, Executive Summary*, International Telecommunication Union, 2005, available at http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf (accessed 23 May 2013).

ITU, *The International Identification Plan for Public Networks and Subscriptions*, ITU.212, International Telecommunication Union, 2008, available at http://www.itu.int/rec/T-REC-E.212/en (accessed 23 May 2013).

Jensen, M., Schwenk, J., Gruschka, N. and Lo Iacono, L., 'On Technical Security Issues in Cloud Computing', in *Cloud Computing: 2009 IEEE International Conference on Cloud Computing*, IEEE Computer Society, 2009. pp.109–16.

Juels, A. and Weis, S. A., 'Defining Strong Privacy for RFID', *ACM Transactions on Information and System Security (TISSEC)*, Vol. 13 Issue 1, 2009.

Kalra, N., Anderson, J. and Wachs, M., *Liability and Regulation of Autonomous Vehicle Technologies: California PATH Program*, Berkeley: Institute of Transportation Studies, University of California at Berkeley, 2009.

Katz, M. and Shapiro C., 'Product Introduction with Network Externalities', *Journal of Industrial Economics*, 40, 1992, pp 55–83.

Kende, M., *Impact of Radio Spectrum on the UK Economy and Factors Influencing Future Spectrum Demand*, London: Department of Business, Innovation and Skills, and Department for Culture, Media and Sport, 2012.

Kierkegaard, S., 'Data Insecurity: Scams, Blags & Scalawags', in Krüger, J., Nickolay, B. and Gaycken, S. (eds) *The Secure Information Society: Ethical, Legal and Political Challenges*, Berlin: Springer, 2013, pp 117–34.

Kim, C. H. et al., 'The Swiss-Knife RFID Distance Bounding Protocol', 2008, available at http://perso.uclouvain.be/fstandae/PUBLIS/60.pdf (accessed 29 May 2013).

Køien, G. M, 'Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context', *Wireless Personal Communications*, Vol. 61, No. 3, 2011, pp.495–510.

Könings, B., Wiedersheim, B. and Weber, M., 'Privacy & Trust in Ambient Intelligence Environments', in Heinroth, T. and Minker, W. (eds), *Next Generation Intelligent Environments*, Berlin: Springer, 2011, pp.227–52.

Krasner, G. E. and Pope, S. T., *A Description of the Model-View-Controller User Interface Paradigm in the Smalltalk-80 System*, ParcPlace Systems, Inc., 1988.

Laing, C., Badii, A. and Vickers, P. (eds) *Securing Critical Infrastructure and Critical Control Systems*, IGI Global Hershey, PA, 2012.

Lee, G. M., The Internet of Things – Concept and Problem Statement, 2011, available at http://tools.ietf.org/html/draft-lee-iot-problem-statement-00 (accessed 23 May 2013).

Lehtonen, M., Staake, T. and Michahelles, F. 'From Identification to Authentication: A Review of RFID Product Authentication Techniques', in Cole, P. H. and Ranasinghe, D. C. (eds) *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Counterfeiting*, Springer, 2008, pp.169–87.

Leister, W. and Schulz, T., 'Ideas for a Trust Indicator in the Internet of Things', paper given at SMART 2012, The First International Conference on Smart Systems, Devices and Technologies, 2012, pp.31–4.

Libenau, J., Elaluf-Calderwood, S. and P. Karrberg, P., 'Strategic Challenges for the European Telecom Sector: The Consequences of Imbalances in Internet Traffic', *Journal of Information Policy*, Vol. 2, 2012, pp.258–72.

Liu, J., Xiao, Y. and Chen, C. L., 'Authentication and Access Control in the Internet of Things', in *Distributed Computing Systems Workshops (ICDCSW)*, 2012, pp.588–92.

Luger, E. and Rodden, T., 'Terms of Agreement: Rethinking Consent for Pervasive Computing', *Interacting with Computers*, 2013.

Ma, H. D., 'Internet of Things: Objectives and Scientific Challenges', *Journal of Computer Science and Technology*, Vol. 26, No. 6, 2011, pp.919–24.

Machina Research, 'The Connected Life: A USD4.5 Trillion Global Impact in 2020', 2012, available at http://connectedlife.gsma.com/wp-content/uploads/2012/02/Global_Impact_2012.pdf (accessed 23 May 2013).

Malik, G. and Kretsis, M., 'Challenges and Success in Teaching Legal, Ethical, Social And Professional Issues To Computing Undergraduates', in *Proceedings of the 15th Annual INSPIRE Conference*, British Computer Society, London, March 2010.

Markets and Markets, *Internet of Things (IoT) & Machine-To-Machine (M2M) Communication Market – Advanced Technologies, Future Cities & Adoption Trends, Roadmaps & Worldwide Forecasts (2012–2017)*, September 2012.

Marx, G. T, 'Ethics for the New Surveillance', *The Information Society*, Vol. 14, No. 3, 1998, pp.171–85.

Mathieson, K., 'Towards a Design Science of Ethical Decision Support', *Journal of Business Ethics*, Vol. 76, No. 3, 2007, pp.269–92

Mayordomo, I. et al., 'Emerging Technologies and Challenges for the Internet of Things', paper given at the Circuits and Systems (MWSCAS) IEEE 54th International Midwest Symposium, 2011.

Meints, M. and Gasson, M. 'High-tech ID and Emerging Technologies', in Rannenberg, K., Royer, D. and Deuker, A. (eds), *The Future of Identity in the Information Society: Challenges and Opportunities*, Berlin: Springer, 2009, pp.130–89.

Michelfelder, D. P, 'Philosophy, Privacy, and Pervasive Computing', *AI & Society*, Vol. 25, No. 1, 2010, pp.61–70.

Mitrokotsa, A., Rieback, M. R. and Tanenbaum, A. S., 'Classification of RFID Attacks', in *Proceedings of the 2nd International Workshop on RFID Technology*, 2008.

Monteleone, S., *Ambient Intelligence and the Right to Privacy: The Challenge of Detection Technologies*, EUI Department of Law Working Paper, 2011.

Narayanan, A. and Shmatikov, V., 'Robust De-anonymisation of Large Sparse Datasets', in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, Washington, DC: IEEE Computer Society, 2008, pp.111–25.

Newton-Evans, *Market Trends Digest; Executive Summary of Findings From EMS*, SCADA, DMS Study, Ellicott City, Maryland: Newton Evans Research Company Inc, 2008.

NIC, *Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025*. Conference Report CR 2008-07, National Intelligence Council, 2008a, http://www.fas.org/irp/nic/disruptive.pdf (accessed on 9 March 2012)

NIC, *Global Trends 2025: A Transformed World*, National Intelligence Council, 2008b, http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf (accessed 23 May 2013).

NIC, 'Who We Are', National Intelligence Council, n.d., http://www.dni.gov/index.php/about/organization/national-intelligence-council-who-we-are (accessed 23 May 2013).

Nissenbaum, H., 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', *Law and Philosophy*, 17, 1998, 559–96.

OECD, 'Machine-to-Machine Communications: Connecting Billions of Devices', *OECD Digital Economy Papers*, No. 192, 2012.

Ohm, P., 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review*, Vol. 57, p.1701, 2010.

Oualha, N. and Olivereau, A. 'Sensor and Data Privacy in Industrial Wireless Sensor Networks', paper given at Conference on Network and Information Systems Security (SAR-SSI), 2011, available at http://www.twisnet.eu/ (last accessed on 23 March 2013)

Pagallo, U., 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law', in Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (eds.) *European Data Protection: In Good Health?*, Springer Netherlands, 2012.

Palm, E. and Hansson, S. O., 'The Case for Ethical Technology Assessment (ETA)', *Technological Forecasting and Social Change*, Vol. 73, 2006, pp.543–58.

Palmer, M., 'Telecoms Place High Hopes on M2M Talk', *Financial Times*, 25 February 2013.

Pfleeger, C. P. and Pfleeger, S. L., *Security in Computing*, Prentice Hall PTR, 2006.

Polk, T. and Turner, S., 'Security Challenges for the Internet of Things', paper given at workshop Interconnecting Smart Objects with the Internet, 2011, p.50.

Prins, C., 'Digital Diversity: Protecting Identities Instead of Individual Data', in Mommers, L., Franken, H., Van den Herik, J., Van der Klaauw, F. and Zenne, G.-J. (eds) *Het Binnenste Buiten*, 2009, p.291, available at https://openaccess.leidenuniv.nl/bitstream/handle/1887/15206/LiberCompleet.pdf;jsessionid=C544849ED5FBD31094D779A2A7AAD881?sequence=2 (accessed 29 May 2013).

Rainey, S. G., *P. ETICA Governance Recommendations Project Report*, ETICA EU Project, Deliverable D 4.2, 2011.

Ramachandran, A., Singh, L., Porter, E. and Nagle, F., 'Exploring Re-identification Risks in Public Domains', *Proceedings of the Tenth Annual International Conference on Privacy, Security and Trust (PST)*, 2012, pp.35–42, 2012.

Rannenberg, K. and Royer, D., 'Open Challenges: Towards the (Not So Distant) Future of Identity', in Rannenberg, K., Royer, D. and Deuker, A. (eds), *The Future of Identity in the Information Society: Challenges and Opportunities*, Berlin: Springer, 2009, pp.391–99.

Ratto, M., 'Ethics of Seamless Infrastructures: Resources and Future Directions', *International Review of Information Ethics*, Vol. 8, 2007, pp.21–7.

Ristenpart, T., Tromer, E., Shacham, H. and Savage, S., 'Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds', in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009, pp.199–212.

Robinson, N., Botterman, M., Valeri, L., Ortiz, D. S., Ligtvoet, A., Shoob, R. and Nason, E., *Security Challenges to the Use and Deployment of Disruptive Technologies*, Santa Monica, CA: RAND Corporation, TR-406-EC, 2007, available at http://www.rand.org/pubs/technical_reports/TR406 Robinson, N. et al Strengths and Weaknesses of the EU Data Protection Directive 95/46/EC (accessed 4 April 2013).

Robinson, N. et al., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, RAND Technical Report TR-933-EC, Santa Monica: RAND, 2010.

Rogers, M., 'Understanding Deviant Computer Behavior: A Moral Development and Personality Trait Approach', *Canadian Psychological Association Abstracts*, Summer 2003.

Roman, R., Najera, P. and Lopez, J., 'Securing the Internet of Things', *Computer*, Vol. 44, No. 9, 2011, pp.51–8.

Sarma, A. C. and Girão, J., 'Identities in the Future Internet of Things', *Wireless Personal Communications*, Vol. 49, No. 3, 2009, pp.353–63.

SCF Associates Ltd, *A Helping Hand for Europe: Competitiveness in Emerging Robot Technologies (CEROBOT): The Opportunities in Safety and Robots for SMEs*, 2010, available at http://www.eurosfaire.prd.fr/7pc/doc/1290673085_eu_robotics_industry_jrc61539.pdf (accessed 29 May 2013).

SCF Associates Ltd, *The Strategic Implications of the Second Digital Dividend*, Policy Tracker, 2012, available at http://www.policytracker.com/research-services (accessed 23 May 2013).

Schindler, R. et al., Smart Trash: Study on RFID Tags and the Recycling Industry, RAND Technical Report TR-1283, Santa Monica: RAND Corporation, 2012, http://www.rand.org/pubs/technical_reports/TR1283.html (accessed 23 May 2013).

Schlatter, J. and Chiadmi, F., 'The Ethics of RFID Technology', in Turcu, E. B. D. C. (ed.) *Deploying RFID – Challenges, Solutions, and Open Issues InTech*, 2011, available at http://www.intechopen.com/books/mostdownloaded/deploying-rfid-challenges-solutions-and-open-issues (accessed 30 May 2013).

Schneier, B., 'Will Giving the Internet Eyes and Ears Mean the End of Privacy?', *Guardian*, 16 May 2013, http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google?INTCMP=SRCH (accessed 23 May 2013).

Schrammel, J., Hochleitner, C. and Tscheligi, M., 'Privacy, Trust and Interaction in the Internet of Things', in Keyson, D., Maher, M. L., Streitz, J., Cheok, A. D. et al. (eds) *Ambient Intelligence*, Berlin: Springer, 2011, pp.378–9.

Schwartz, P. and Janger, E., 'Notification of Data Security Breaches', *Michigan Law Review*, Vol. 105, 2007, p.913.

Smith, I. G. (ed.) *The Internet of Things 2012: New Horizons*, 3rd edition of the Cluster Book, available at http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf (accessed 30 May 2013).

Soraker, J. H. and Brey, P., 'Ambient Intelligence and Problems with Inferring Desires from Behaviour', *International Review of Information Ethics*, Vol. 8, 2007, pp.7–12.

Spiekermann, S., 'About the "Idea of Man" in System Design: An Enlightened Version of the Internet of Things?', in Uckelmann, D., Harrison, M. and Michahelles, F. (eds) *Architecting the Internet of Things*, Springer, 2011, pp.25–35.

SRI Business Consulting, *Disruptive Technologies Global Trends 2025*, 2008.

Stahl, B. C., Heersmink, R., Goujon, P., Flick, C., van den Hoven, J., Wakunuma, K., Ikonen, V. and Rader, M., 'Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method', *International Journal of Technoethics*, Vol. 1, No. 4, 2010, pp.20–38.

Swift, A. G., 'Locating "Agency" Within Ubiquitous Computing Systems', *International Review of Information Ethics*, Vol. 8, 2007, pp.36–41.

Tan, Y., 'Persuasive Technology in Motivating Household Energy Conservation', 2009, http://www.im.ethz.ch/education/FS09/iot_2009_slides/persuasive_energy_awareness (accessed 30 May 2013).

Tapscott, D., *Grown Up Digital: How the Net Generation is Changing Your World*, McGraw-Hill, 2008.

Tech Exclusive, 'India Faces Disrupted Internet Service Due to Undersea Cable Issue', 27 April 2010, http://www.tech-exclusive.com/india-faces-disrupted-Internet-service-due-to-undersea-cable-issue/ (accessed 23 May 2013).

Tene, O. and Polonetsky, J., 'Big Data for All: Privacy and User Control in the Age of Analytics', *Northwestern Journal of Technology and Intellectual Property* , 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364 (accessed 30 May 2013).

Thanki, R., 'The Power of the Unlicensed Economy', July 2012, available at http://allthingsd.com/20120710/the-power-of-the-unlicensed-economy/ (accessed 29 May 2013).

Van Beijnum, I., 'Inecure Routing Redirects YouTube to Pakistan', ArsTechnica, 25 February 2008, http://arstechnica.com/uncategorized/2008/02/insecure-routing-redirects-youtube-to-pakistan/ (accessed 23 May 2013).

Van Blarkom, G. W., Borking, J. J., Olk, J. G. E., *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*, 2003, available at http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf (accessed 29 May 2013).

Van Dijk, N., 'Property, Privacy and Personhood in a World of Ambient Intelligence', *Ethics and Information Technology*, Vol. 12, No. 1, 2010, pp.57–69.

Van Kranenburg, R., Anzelmo, E., Bassi, A., Caprio, D., Dodson, S. and Ratto, M., 'The Internet of Things', paper given at 1st Berlin Symposium on Internet and Society, 2011, pp.25–7.

Vesset, D. et al., *Worldwide Big Data Technology and Services 2012–2015 Forecast*, 2012, available at http://www.idc.com/getdoc.jsp?containerId=233485 (accessed 23 May 2013).

Weber, R. H., 'Accountability in the Internet of Things', *Computer Law & Security Review*, Vol. 27, No. 2, 2011, pp.133–8.

Weber, S. G., Martucci, L. A., Ries, S. and Mühlhäuser, M., 'Towards Trustworthy Identity and Access Management FOR The Future Internet', in *Proceedings of the 4th International Workshop on Trustworthy Internet of People, Things & Services (IoPTS)*, 2010.

Whalen, M. W. et al., 'Your "What" Is My "How": Iteration and Hierarchy in System Design', *IEEE, Computing Now*, Vol. 30, No. 2, March/April 2013, pp.54–60.

Wiegerling, K., Capurro, R., Britz, J., Hausmanninger, T., Nakada, M. and Apel, M., 'Ethical Challenges of Ubiquitous Computing', *International Review of Information Ethics*, Vol. 8, 2007.

Witten, I. H, Frank, E. and Hall, M. A., *Data Mining: Practical Machine Learning Tools and Techniques: Practical Machine Learning Tools and Techniques*, Morgan Kaufmann, 2011.

Wolf, M., 'Why the World Faces Climate Chaos', *Financial Times*, 14 May 2013.

Wright, D., 'Structuring Stakeholder E-inclusion Needs', *Journal of Information, Communication and Ethics in Society*, Vol. 8, No. 2, 2010, pp.178–205.

Wright, D., 'A Framework for the Ethical Impact Assessment of Information Technology', *Ethics and Information Technology*, Vol. 13, No. 3, 2011, pp.199–226.

Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M. and Moscibroda, A., 'Privacy, Trust and Policy-making: Challenges and Responses', *Computer Law & Security Review*, Vol. 25, No. 1, 2009, pp.69–83.

Xinhua News Agency and Booth, R., 'A Report from "Investment in IoT: Are We Ready?", Internet of Things Special Interest Group Conference, Google Campus, Open Innovation Connect, 29 Nov 2012.

Yan, L., Rong, C. and Zhao, G., 'Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography', *Cloud Computing*, 2009, pp.167–77.

Yorita A. et al., 'Cognitive Development in Partner Robots for Information Support to Elderly People', *IEEE Transactions on Autonomous Mental Development*, Vol. 3, No. 1, March 2011.

Zhou, L. and Chao, H. C., 'Multimedia Traffic Security Architecture for the Internet of Things', Network, IEEE, Vol. 25, No. 3, 2011, pp.35–40.

Annex A. Methodology

The study, conducted between January and June 2013, utilised a number of methods.

A.1. Background research

Desk research was used to establish the state of the art in evaluating the effectiveness and impacts. It covered scientific, industry and 'grey' (policy) literature, relevant publicly available data referenced in the literature, and non-public, confidential material provided by the European Commission.

The initial literature review was followed by a Rapid Evidence Assessment exercise with a focus on ethics, privacy and security. We developed a search strategy, using a multi-tiered Systematic Literature Search (SLS) technique to search research evidence. This included defining search terms by sequentially testing variants of successful search terms, and included suggestions from interviewees. For the purpose of this work, we aimed to include relevant databases covering disciplines such as psychology and social sciences, economics, law, technical/experimental social sciences and business administration. We included scientific databases such as ACM Digital Library, JStor, IEEE, and Google Scholar and grey literature.[99] All queries were conducted between January and March 2013. Overall, the systematic review process generated a library containing 122 documents, which were subsequently reviewed for usefulness and quality.

Overall, we collected information on: the analysis of the issues and challenges; the range of impacts considered and methods for measuring and/or estimating them; the contents, quality, coverage and relevance of data sources; the models and parameters that have been estimated (and the conclusions drawn).; and the scope, context and findings of related

[99] In our context, grey literature includes reports and research by think tanks, government departments, international organisations, professional associations, and other published and unpublished research. Furthermore, it must be noted that for grey literature, we used Google and Google Scholar search engines because individual organizations' websites were not consistently structured and not easily searchable. Google hits served as a starting point and provided useful background information.

Impact Assessments (eg those addressing RFID, spectrum and Internet governance policies by various levels of government).

A.2. Framing methods

The most important methodological requirements come from the self- and co-regulatory nature of IoT governance. Evidence relating to internet governance clearly demonstrates the wide range of issues addressed, instruments used,[100] variety of forms governance organisations take and the apparently close connections between these forms and sectoral, issue or national specificities. Second, because the IoT and the bodies concerned with its functioning arise and/or operate at least partially outside government control,[101] the assessment of IoT governance options required the inclusion of third-party actions and actions; this departs in three ways from the normal context of an impact assessment:

- The stakeholder bodies through or in conjunction with which IoT governance options must operate were not necessarily designed to advance particular public objectives, which may thus be achieved as a by-product of their defining *raison d'être*.[102]
- Such bodies often need to rely on voluntary self-interested behaviour for participation and compliance, which differentiates their command of resources, scope (who is bound by them) and effectiveness from those of similar formal regulatory initiatives.[103]
- These players do not have exclusive power within an integrated legal framework, and thus may compete, overlap or collaborate with other self-governance, co-governance and formal governance bodies, or face patchy legal underpinnings across their geographic sphere of activity.[104]

To take these considerations into account, the framing of the study also provided a stakeholder analysis to map the key players in the IoT and current (formal and informal) regulatory bodies, presented in Annex E and Annex F.

As a result of the partially self-organising and autonomous nature of IoT governance, and the powerful overlaps between IoT governance issues and steps taken to address the same

[100] For example, standards, codes of conduct, contracts and monitoring.

[101] Governments participate in many inter-governmental bodies, but often only as observers.

[102] For example, interoperability as a by-product of IETF design principles.

[103] An example is the voluntary approach of the RFID Bill of Rights proposed by Simon Garfinkel (2005) compared with the co-regulatory approach adopted by the US FTC in relation to the Fair Information Principles (and, in the internet domain, the Safe Harbour Agreement).

[104] For example industry-led hotlines for illegal content or Safe Harbour privacy provisions.

issues in other domains, familiar elements of the logical framework such as design and relevance, efficiency, effectiveness and sustainability required careful interpretation, especially when comparing governance alternatives. To do this we built on the guidance developed in Cave, Marsden and Simmons (2008) to specify:

- the options – in particular the baseline Option 0 in which no further action is taken by the EU, but where other industry, government[105] and civil society initiatives continue
- the intervention logic associated with the options
- the criteria to apply at each stage
- evidence and measurable indicators
- relevant economic, social and other impacts and affected parties
- additional risks or external factors most likely to affect the assessment.

A.3. Additional evidence-gathering and validation

Once we completed the rapid evidence assessment, we identified areas where further clarification was needed, mapped subjects to areas and developed a protocol for semi-structured interviews, which we conducted for the most part as telephone interviews.

To complete the evidence base for the study, validate the methodological steps and emerging findings, and ensure that the scenario analysis, description of options and impact identification were complete, balanced and consistent, we conducted a series of key informant interviews with industry, government and civil society stakeholders involved in the IoT itself and those concerned with specific issue areas (eg privacy advocates, service providers and others involved with privacy and security issues, and participants in internet governance). Interviewees were selected on the basis of their expertise (as referenced in the literature or suggested by others) or the stakeholder group they represent (industry, government, civil society), including former members of the European Commission's IoT Expert Group (2010-2012). In order to ensure that all sides of the debate are heard regardless of their relative policy influence, a particular effort was made to seek input from European entrepreneurs, SMEs and European key stakeholder as well as dominant industry players.

Table A.1 lists the interviewees, excluding those who requested to respond anonymously, respecting the Chatham House Rule.

[105] Including those directed at internet governance *per se.*

Table A.1 List of persons interviewed for study[106]

Name	Organisation
Benoit Abeloos	European Commission
Eric Barbry	Alan Benoussan Avocats
Rudolf van den Berg	OECD
Dan Caprio	McKenna Long & Aldridge LLP
Prof. Brian Collins	UCL Centre of Engineering policy
Marc de Colvenaer	Flemish Living Lab Platform
Alain Dechamps	CEN
Ralph Droms	IETF
Kathleen Gabriels	Vrije Universiteit Brussel
Patrick Guillemin	ETSI
Mark Harrison	University of Cambridge
Ayesha Hassan	International Chamber of Commerce
Prof. Mireille Hildebrandt	University of Nijmegen
Prof. Jeroen van den Hoven	TU Delft
Prof. Sotiris Ioannidis	Foundation for Research and Technology
Dr Stig Johnsen	SINTEF
Olaf Kolkman	NL net labs
Tobias Kowatsch	Institute of Technology Management, St Gallen
Rob van Kranenburg	Waag
Christoper Kuner	Hunton and Williams
Christoph Luykx	Intel
Massimiliano Minisci	GS1
Ludovic le Moan	Sigfox
Gerrit Muller	Embedded Systems Institute
George Roussos	Birkbeck, University of London
Rogelio Segovia	European Commission
Marc Sel	PriceWaterhouseCoopers
Prof. Berndt Carsten Stahl	De Montfort University
Mark Townsley	IETF
Prof. Guido van Steendam	KU Leuven
Peter Walters	Department for Business, Innovation and Skills, UK
Dr Rolf Weber	University of Zurich
Tijman Wisman	University of Amsterdam

[106] Excluding those who were interviewed anonymously.

A.4. Legal analysis

To make a comparative analysis of the current relevant legislation and the regulatory measures implemented worldwide, at European level and in particular Member States, we conducted a comparison between key legislation and legislator measures. We focused on the current legislative framework for the IoT and the pressing legal challenges for the future, notably as they relate to consumer protection priorities. We provided an overview of the current legislation in force, its applicability to the IoT, and the major gaps and lacunae. Related jurisprudence that might be applicable to future IoT landscapes was highlighted when relevant.

A.5. Assessing Impacts

We assessed non-quantitative impacts on the basis of analyses drawn from the scholarly literature, consultation with experts and the interactive methods used to explore the scenarios.

A.6. Workshops

The study was informed by a team-internal scenarios-based workshop. We extended and tested our findings and conclusions at an open stakeholder workshop held on 30 April 2013 at the European Commission's premises in Brussels.

The workshop attracted European innovators and entrepreneurs and brought together a diverse set of stakeholders involved in the policy formation regarding the IoT: civil society and consumer representatives; industry stakeholders who provide, support and/or use IoT devices, applications and services; and academics. The workshop served as a means to validate and refine research findings, explore their implications and policy options with the audience, and obtain suggestions about how the European Commission and other interested stakeholders might proceed. Table A.2 lists the participants at the workshop.

Table A.2 List of participants at stakeholder workshop

Name	Organisation
Kristina Aleksandrova	ANEC
Alessandro Bassi	Bassi Consulting
Souheil Ben Yacoub	Verisign
Aileen Byrne	Transatlantic Council
Rodolphe Frugès	Sigfox
Kathleen Gabriels	Vrije Universiteit Brussel
Eric Gaudillat	European Commission
Mark Harrison	University of Cambridge
Finn Myrstad	BEUC

Philippe Lefebvre	European Commission
Christoph Luykx	Intel
Massimiliano Minisci	GS1
Gerrit Muller	Embedded Systems Institute
Stephen Pattison	ARM Holdings
Isabelle Roccia	US Mission to the EU
Kostas Rossoglou	BEUC
George Roussos	Birkbeck, University of London
Rogelio Segovia	European Commission
Prof. Guido van Steendam	KU Leuven
Petra Wilson	CISCO

Annex B. Managing autonomous decision engines in the IoT

B.1. The IoT and decisions by object that could affect everyday life

One of the key difficulties in widespread uptake if the IoT, if it is to reach its full potential, is the requirement for an approach to safety for machines that may make autonomous decisions. This is not a new problem. It has been studied over the last three decades, largely in various robotics research projects, and in a very simplified form for human control and intervention in diverse web-based implementations, using a particular architectural construct (Krasner and Pope, 1988).

This dilemma presents a significant new dimension in the IoT, of there being possibly very large numbers of machines, which may also have agents or proxies acting for them, or for human users of the IoT. Their effect on society risks being harmful, unless there is some way of limiting any extreme behaviour.

Protection against this danger should form part of policy, to ensure that autonomous machines always exhibit safe and rational behaviour in line with pre-set safety guidelines. This would require examining outcomes in real time from decision-taking machines or agents to detect anomalies. It might also be necessary to employ predictive techniques to detect the early onset of abnormality. The actual policy itself should be structured with the principle of holding safety of life and the environment as the highest priority, as the industrial robotics sector has done for more than a decade.[107]

B.2. Such a mechanism has various system requirements

To be implemented in the IoT any such mechanism needs specific attributes:

- It must be capable of distinguishing with precision between normal and aberrant behaviours in the autonomous decision-taking system.

[107] See SCF Associates Ltd (2010), which explores safe robotics and policies for safety in the robotics industry, including Asimov's Laws (1950).

- It must be low cost to create and integrate, with low performance overheads when in operation.
- It needs to be inviolate, a difficult characteristic which is implementation-dependent, but separation from the IoT object supervised is evidently a first step.
- It must be possible to add it to existing systems quickly and easily.
- It should be compatible with all types of real-time system such as Supervisory Control and Data Acquisition (SCADA), transaction-based systems, autonomous robotic equipment, as well as internet and web-based systems that act in deferred time.
- It should be implementable either locally (with or even within the object supervised) or remotely, or partially remotely with only what is necessary for capturing data and actuating change placed locally (as a thin client, with the major elements on a remote server).

B.3. Anticipating potentially unsafe autonomous decisions

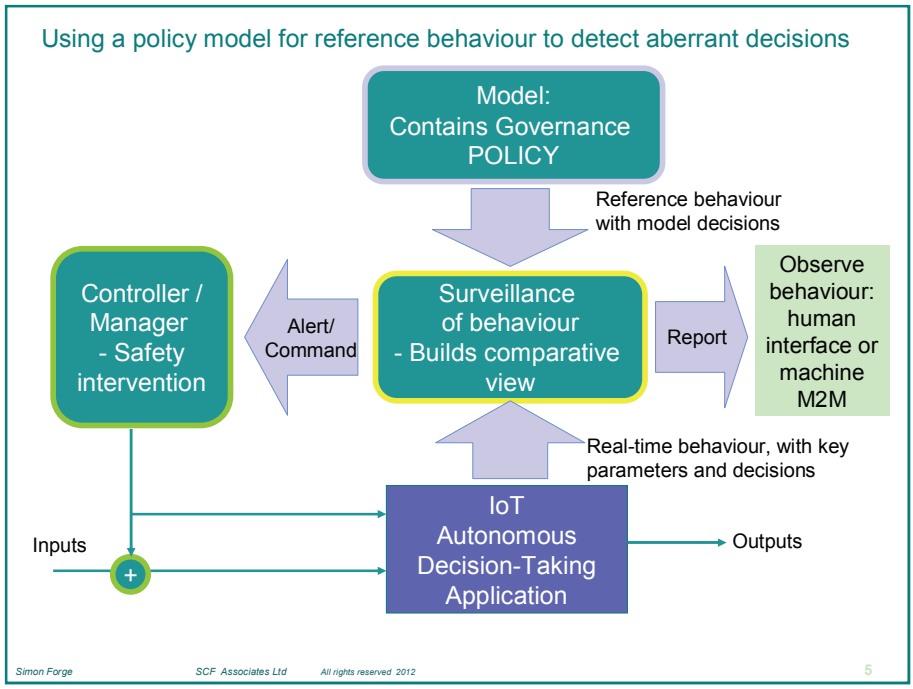
The approach used in robotics, and in industrial process control for some years, has been a simple comparison with a pre-set policy, coupled with identification of the key parameters for aberrant behaviour. In an autonomous decision-taking system, however, this may be far more complex than simple drift from pre-set process parameters.

Decision-taking could involve an intricate state situation and deviations from this may not be evident. The standard solution to this is a comparative model of normal behaviour under all conditions. That may be quite sophisticated and involve cognitive analysis of multiple machine's behaviour, to understand what is happening and whether it is changing, and then what exactly is causing the change in that behaviour, so the appropriate a remedial action can be applied.

This requires an intelligent comparison in real time of the decisions reached, perhaps before they are implemented. In addition the components of an ideal-model and a controller would implement a corrective process following the pre-set policy that ensures compliance with safety security and privacy. Existing web-based constructs, usually for human control, as in the model view controller pattern (Holzinger, Struggl and Debevc, 2010), may not be suitable for the IoT in an automated situation, although the basic pattern may be augmented for the IoT with some basic modifications.

One suggestion for this is shown in Figure B.1. The concept of comparison of behaviour, in its abstract form through models (Yorita et al., 2011), is an approach often used in this domain.

Figure B.1 Supervisory system to anticipate failure in decision-taking objects



The basic design uses three elements – a policy reference model, a surveillance and comparison component, and a controller or manager that supervises the subject IoT machine's inputs and operational parameters. Optionally, there may be a human interface, or machine external observer to view and follow what is occurring. Differences in behaviour patterns of the IoT object in its decisions are detected by the comparator in the surveillance element as soon as possible. This construct expects purely machine intervention, although overrides to manual control may well be required. Checks on decisions against the model are performed before they are executed if possible.

B.4. Policy impacts-defining the problem

At a policy level it may be necessary for IoT systems that have safety of life risks in their decision-taking to mandate that some form this type of supervisory system are present.

B.4.1. Defining the problem statement for the governance of the architecture revolves around two main questions

The real challenge is to identify a type of architecture that would meet the demands of all possible concrete IoT implementations, within the budget and timeframe available. Ensuring attention to the security and privacy aspect is crucial – its incorporation must be in the founding principles and implementations of the architecture, not left to be an afterthought added later on top of what has been built.

When considering governance with reference to the architecture for the IoT, two sides of the problem arise.

First, **is governance is necessary, for the architecture itself**? And if so – how should that governance be effected? Who should do it and how? The internet has enshrined its architecture's governance in various institutions, most notably the IETF and the IGF, to hear the views of various stakeholders – technical communities, end users, governments and the private sector. It has the Working Group on Internet Governance, which initially called for the IGF before it was formally set up in 2006 by the UN.

This leads us to the second consideration on architecture and governance – which is **to identify the architecture needed to implement the policy options for governance of the IoT**. The aim of the architecture is to protect the liberty and security of all users while at the same time carrying out the networked functions of an IoT in a robust and secure manner, which is as efficient and flexible as possible. This is increasingly difficult as it must:

- take into account the requirements of all stakeholders, regarding governance
- anticipate the need for future developments in governance, in the flexibility for adaptability of the architecture
- make a place at the start for the core needs of privacy, security and safety so they are not added afterwards – as in the internet.

Thus the IoT's very design in the key foundations of its structure (and the working behaviour that implicitly induces) would inherently enact the governance policies and rules. Forms of various standards can be involved here also, for instance in common architectural reference models that express the semantics of interactions used to implement specific architectural principles, for example around security to enforce these principles, as has happened in highly successful ICT markets such as for the web-server–web-browser design paradigm.

In consequence, for the consideration of a problem statement, for a policy analysis for an IoT architecture within a global and a European context we start by summarising the key policy level questions. Then we state the problem for policy in these areas, more specifically whether there is a possible role for European institutions, and if so what that is:

- Is there a clear need for an IoT (specific) architecture(s)?
- If so, is there a real need for a **common** IoT architecture – and what would need to be done to achieve its commonality, in the context of a multi-stakeholder community?
- Do any of the questions above demand action from a central governance body? How would an IoT architecture be governed?
- If some form of IoT architecture governance is required, what is the role of the EC? (Or is it neutral, just allowing industry and standards

committees to proceed normally, without any EC encouragement, initiatives or intervention?)

- If action from the EC is required – what is it?
- And importantly, in parallel, how could an IoT architecture express the governance principles that a needs analysis of the IoT overall reveals?
- How should architecture(s) be coordinated with other governance mechanisms, processes and constraints?

To address the core questions, the future potential IoT architecture may be examined across five key areas:

- infrastructure – the basic principles
- stability and resilience of an IoT architecture
- identification
- security and privacy
- standards, that define the technical architecture.

B.4.2. The architecture of the IoT Infrastructure – basic principles

Any architecture should respond to a needs analysis and it is crucial that its principles, the major components and their active behaviour correspond to these requirements in the design foundations (Whalen et al., 2013).[108] For implementation, these functions collectively may be termed the framework or infrastructure on which real application systems are built.

Thus an architecture in this context is defined as a framework for the specification of any implementation, as a networked system's **logical and physical** components and their functional organisation and configuration, with the operational principles and procedures, protocols, semantics of information and data formats used in its operation.

B.4.3. Is there a clear need for an IoT specific architecture?

Will the current internet architecture we have used since 1971, with increments such as the web in 1994, be enough for the IoT? It has naming and addressing for hierarchical fixed network addressing, a peer-to-peer model of working, with no centralised locus of control, and was originally aimed at large file transfer, inter-process communications for coordinated computing and e-mail exchanges. Its address space has just been expanded with the move from IPv4 to IPv6 and its can now cope with the 100 billion IoT objects expected in coming decades.

[108] Requirements and architectural design should be more closely aligned than they currently are: requirements models must account for hierarchical system construction, and architectural design must better support requirement specifications for system components.

The current key application on top of the internet communications layer, the web, developed various publish-and-subscribe functions, using a thin client and server model. This is implemented with the browser and its responding web server sites, using various document formatting or mark-up languages. The internet is open to all to join and its infrastructure has no IPR constraints.

However, the internet corresponds to a set of fairly limited needs compared with the IoT, although its architecture is 'stretchable' in many ways. It is based on a single processing, communications and storage model, most usually aimed at publishing globally and accessing information globally – often for non-real-time delivery, in a sheltered environment (home, street, office or data centre).

The IoT is some ways very different to the existing internet. An overview of the pertinent main points in an assessment of its requirements (see Box B.1) highlights a range of quite diverse operational demands compared with the internet. Its architecture must be scoped to be an extension of the physical infrastructure that society uses far more than the internet has been. As IoT systems must respond to real-world events, typically the change of state of a monitored parameter, so the architecture must be event-driven. Thus it has to be fairly different from the standard internet architecture, in order to control energy grids, manufacturing and processing plant, urban environments, smart buildings, homes and hospitals as well as monitor environmental parameters on land and sea efficiently and safely.

Thus the requirements and scope of IoT architecture are far wider than those of the internet in their physical implementations. While the internet has a single identification scheme with its DNS design, for example, an RFID-tag-based identification architecture (using a tree naming mechanism) may be very dissimilar, while control systems for a process plant with a sensor-based network and programmable logic control may again require a different architecture in which the internet could be used, but is not ideal. Thus for the IoT architecture, some strong differences pertain. The attributes of an IoT architecture, showing the more difficult capabilities to encompass within the current internet and web architectures with mark-up languages (although perhaps not entirely impossible), are shown in Box B.1.

Box B.1 Attributes for an IoT architecture – key requirements to meet

- *It is event driven* – by 'things' – triggered by signals indicating a state change of some parameter.
- *It has real-time operations* often, not just near real-time, with very different ranges of time in which exchanges must occur, ranging from a few microseconds to weeks, months, even years.

- *Clusters of strongly typed networks interoperate*, but perhaps not with any network outside the cluster, ever. Thus the structure is one of a network of networks (although the internet could be used to interconnect dedicated IoT networks within the cluster, by appropriate gateways). In addition, the IoT services demanded over the network may become much less fixed to one server or cluster, and so more decentralised – so that operational complexity increases with the complexities of these networks of networks, all with their own modes of working, communications protocols and architectures.
- *Devices are deployed in very high numbers* (millions, even billions) that are often deployed in rugged, difficult conditions, with limited resources, possibly battery-powered, often with tiny storage and little processing power (perhaps none) and frequently with constraints on cost and communications.
- *It needs to serve a wide range of quite different vertical industries*, each with its own proprietary or open identification schemes and formats, levels of security and limits on privacy, types of processing required and communications protocols. Each may have access controls that correspond to its applications, processing and data models.
- *It uses radio-based communications*, in which physical location may be less relevant, especially if mobile, although propagation range is critical. Thus the availability of suitable spectrum is a key factor for widespread IoT deployment. Many M2M networks already exist with comparatively narrow amounts of spectrum in industrial, scientific and medical (ISM) bands, while white space device networks for M2M applications are also planned.[109] In licence-exempt ISM bands, the output power and duty cycle of link budgets may be constrained, perhaps down to 0.01 percent. The latter radio technologies can avoid the use of relatively expensive mobile connectivity, based on a SIM card, for M2M communications.[110] These sharing technologies will also employ 'spectrum-aware' techniques,

[109] For example those from Neul in the UK, whose WSDs are specifically aimed at M2M markets, with their weightless protocol

[110] For example for a smart energy grid, the cost over 20 years of using frequency hopping spread spectrum for management and energy saving in a licence-exempt ISM band against a mobile connection, for meter reading only being made just once per year, is of the order of €2 billion for a national smart grid in a Member State the size of the UK; source: SCF Associates Ltd's submission response to Ofcom public consultation, March 2013, on licence exempt band for short range devices, 870-876 MHz.

such as cognitive radio. Using radio, mobile transceivers may roam and attach to different networks, so they may disappear altogether, only to reappear on a different network later, provoking naming and addressing issues.

- *Identification for object resolution*, for discovery, search and location of network attached objects may employ different naming and addressing forms that are not directly compatible. Yet the IoT resolution mechanisms must work across multiple heterogeneous network domains (multiple identification, object discovery and resolution schemes).
- *There are varied dedicated network architectures*, which are quite different from those of the internet's peer-to-peer structure (with TCP/IP packets, as in its networking layers). For example, an IoT network may have a mesh design of daisy-chain topology, or perhaps centralised master–slave for process control. Typically IoT sensor networks use the BLAST (Bursty, Lightweight packets, ASynchronous command-response, Transitional) networking concept or is inherently mobile –it is not download or upload centric as with a base station arrangement.
- *It has autonomic operations* – self-repairing and self-modifying capabilities for distributed processing, possibly with the formation of new links and relationships as the new form adapts to its internal status and external environment, as its sensors analyse its situation and detect the need for change.
- *It has ad hoc operations* – communications among IoT devices as well as with related services, may occur at any instant, anywhere, via a range of media across multiple types of network.
- *Its security and privacy domain is built in* – and in consequence may be far more difficult to construct and maintain. New and stringent privacy (and security) measures are needed, while transparency and accountability in providing IoT services demands far more effort.

We conclude that there is a clear need for an IoT architecture distinct from the internet architecture. The key question, then, is whether there can there be a single IoT architecture, or reference model, and this is examined below.

B.4.4. Can there be only one IoT architecture, or if not one architecture, one reference model?

Currently a whole series of designs projected to be IoT architectures have been published, most of which have evolved from current industrial systems. Thus while a single IoT reference model might be identified eventually, it is far more likely that several reference

models would co-exist. As emphasised, the architectural question is really of accomplishing an interworking set of different systems.

So the future is likely to be a continuation of multiple models. Whether eventually a common architecture or even a higher level meta (or reference) model will evolve is doubtful. The conclusion from the IoT features examined above is that a single architecture covering all the domains of potential IoT activity is unlikely in practice at this time. Instead what we may have is a series of linked domains.

Thus, at a network level we would have an overall architecture of different standalone systems planned for purpose with strict design rules, which interoperate. **Interoperability** becomes the critical architectural component and in some ways the only one. Here there is a role for the existing internet but it may have to be a reinforced infrastructure for:

- support for mobility of communicating entities, including services, that drop out and return with support for intermittent and non-continuous link radio communications
- lightweight protocols to reduce load on resource-constrained devices
- non-peer-to-peer communications
- support for real time – faster time constants – for lower latency in some systems.

In consequence, the future lies far more with melding and interoperating different architectural models than a single high level design or even a reference model.

B.4.5. Stability and resilience of an architecture – the related attributes

Society will increasingly rely on the IoT, so its architecture must reflect certain classic architectural features, which are aimed at maintaining acceptable levels of service, such as redundancy and failover, to increase its overall resilience. This has policy implications.

However, the IoT is not just single a complex system – it is a collection of autonomous or semi-autonomous complex systems, with many independent agents. Society needs an IoT architecture that is inherently both stable and resilient to any damaging event or degradation, almost in an organic manner. The key tools for this need to be built in at an architectural level, so they become part of the infrastructure. Depending on user requirements each of the following measures should be built into the architecture, not retro-fitted on top afterwards. They may include at a design principle level:

- proven architectural components – re-use of proven models for processing, communications and storage structures, which are unchanging; a standard technique to make the architecture more resilient as well as stable

- static architectural design – the principle of simplicity as an approach to resilience and stability – the fewer the number of active agents, with possibly uncertain behaviours, the better (see Annex B for an example of a solution in this direction).

Moreover, the IoT architecture must counter a range of risks in operation to be more robust than the internet, as its failure may directly concern safety of life, perhaps on a large scale, every day of the year, and so the uptime is far more critical:

- Stability and resilience are especially needed for safety when decisions are made by machines so that the correct decisions are made despite system failures and evolution of the system with new releases (the origin of many instances of 'IT is down today for upgrade'.
- Resilience – failure and interruption of key services – may become a policy issue; any interruption of the smart electricity grid is very expensive (in the UK it would cost over €8 billion for a major outage of a large region for 12 hours[111]).
- Applications which are essentially extensions to the physical infrastructure can need stronger security.

Measures at an implementation level include:

- provision for redundancy, back up, alternative routing, failover, resend
- failure resistant types of structures – eg mesh networking – for alternative routing and non-base station dependence
- inbuilt privacy measures
- security systems to resist attacks, human error and natural disasters with mechanisms built into the architectural concepts, as inherent features, not added afterwards, eg for access control
- adaptation to intermittent connections – detection and recovery from signal outages with no effects on normal functioning following recovery.

Detailed technical excellence must come from appropriate standards, endorsed by a policy that encourages or even mandates the use of best practice. For the IoT, additional pressures on stability and resilience are engendered by two developments for more advanced systems that will have negative (or perhaps positive) impacts at an architectural and at the policy level:

[111] SCF Associates Ltd's response submission to Ofcom public consultation, March 2013, on licence exempt band for short range devices, 870-876 MHz, with smart grid assessment of economic factors.

- An extension of the simple pre-programmed processor or controller – the capacity for decisions to be taken by IoT objects. Here, we enter the policy realms of robotics, where machines can take decisions that affect the safety of life. Thus the architecture itself must be designed, as the foundation of such control techniques, such that any autonomous decisions can be monitored and controlled continually for aberrations and dangerous outcomes (Annex B examines mitigation measures).
- Autonomics – for more advanced IoT systems – the capability for decision-taking can be applied to self-repair also (or can be automatically triggered by certain status signals).

Thus the IoT may be likely to evolve into a set of complex adaptive systems, which in some domains (not all) will be agent-based to supply critical services, as well as being self-starting and aware of its internal status and external environment. This will include adaptive self-configuration for optimal performance. The control of agents may be a further area for policy intervention.

The stability of architecture is also a contribution that increases resilience. Stability and resilience together set the levels of availability and operation in a dependably predicable manner. The architecture sets the design, blueprint or outline for the IoT systems that will be built following it. Thus a successful architecture will remain the same, stable and unchanging, while the IoT systems built using it may go through an evolution, perhaps of 20 releases. The hallmark of quality of an architecture is its ability to support applications and systems evolution without in itself changing.

Annex C. Identification

C.1. Encoding of HTTP URIs in RFID tags for the IoT – an example of an identification solution for RFID between EPC and URI

C.1.1. Fundamental identification problems and the IoT

A fundamental problem for the IoT is the convergence of a naming and addressing system for communicating objects that together form the IoT, but such difficulties are not insuperable. The intention of this brief annex is to show one example of how it might be possible to overcome some of the difficulties between the EPCglobal and internet spheres of operations.

While the internet has been based on the DNS system, objects in a commercial world of independent vertical industrial sectors each have their own conventions for identification, as can be impressed on RFID tags or other types of identifier, such as 2D barcodes or other devices that have a network address, such as a meter responder in a smart electricity grid with a meter point administration number. Could RFID tags meet internet URIs in some way? A further IoT-related issue is whether there is a need for unique identifiers. In governance terms, this indicates a need for identifiers that are common and unique.

This in turn indicates a need for coordination at global level. But does that imply the requirement for a single centralised body, or a federation of peer global organisations, for example the ISO, the ICANN, and perhaps GS1, or a set of regional bodies, for example involving CEPT, ETSI and the Federal Trade Commission (FTC) or Institute of Electrical and Electronics Engineers (IEEE)?

Currently, it is possible to encode a globally unique identifier in a low-cost passive RFID tag. It must comply with the GS1 EPCglobal Class 1 Gen 2 or ISO/IEC 180000-6C air interface protocols by using either an existing EPC scheme defined by GS1 in the EPC Tag Data Standard or an identifier qualified by an application family identifier assigned by ISO. Several EPC schemes are defined. The majority of these support encoding of existing GS1 identifiers, although some EPC schemes are not aligned with GS1 identifiers.

As new industry sectors consider adoption of low-cost RFID, they must consider whether they can reasonably use one of the existing EPC schemes or ISO application family identifiers. Some industry sectors have deeply entrenched existing practices for unique identification and already use these in data carriers other than RFID, such as nameplates, bar codes and matrix codes.

C.1.2. Origins of the codes

The GS1 Global Trade Item Number (GTIN) traces its origin to the Uniform Product Code 12 (UPC-12) and EAN-13 codes, which were originally designed for use with linear barcodes, to provide a highly efficient way of assigning globally unique product codes. The GTIN is an all-numeric code constructed from the concatenation of an indicator digit, a GS1 company prefix, an item reference and a check digit which is calculated from the preceding digits. The GS1 company prefix is all-numeric, ranging from 6 to 12 digits.

However, some industry sectors use alphanumeric codes for identifying the organisation that issues the identifier – typically the brand owner or manufacturer. The Commercial and Government Entity (CAGE), NATO Commercial and Government Entity (NCAGE) and Department of Defense Activity Address Code (DoDAAC) are examples used in the aerospace and defence sectors. When the UPC-12 and EAN-13 codes were introduced, the internet was not in widespread use by companies or the public and the World Wide Web and URIs were not established until the late 1980s and early 1990s. At the time, the issuing of a compact globally unique code to refer to a single organisation was considered novel and had a relatively high value proposition.

However, in recent years with the ubiquity of the World Wide Web and low-cost registration and renewal fees for domain names this is no longer the case; for most people or organisations in the developed world, it is very affordable to register a domain name and create an unlimited number of globally unique identifiers – HyperText Markup Language (HTTP) URIs – by concatenating their registered domain name with a locally unique string, the two being separated by a slash character ('/').

Furthermore, the semantic web and linked data initiatives by default use HTTP URIs to provide globally unique names for people, places, organisations and even concepts and relationships, and the fact that an HTTP URI can also function as a URL means that information about that resource can be provided very simply, for example using a web browser directed to that HTTP URI. This can then point to a web page of information about the identified thing – or even to machine-readable linked data about the thing, expressed as Resource Description Framework (RDF) triples representing factual claims about the identified thing and its properties or attributes, as well as relationships with other things.

Today, individuals, companies and industry sectors do not need to go to issuing agencies in order to construct HTTP URIs, but there are still a number of data carriers (linear barcodes and low-cost passive RFID tags) that have limited memory capacity and therefore require efficient storage of identifiers. This can lead to delay of the adoption of RFID. GS1 is both an issuing agency and a standards development organisation facilitating the development of open standards of direct relevance to the IoT. However, difficulties can arise if an industry sector finds that its existing embedded identification scheme cannot be accommodated within an already defined EPC scheme.

Currently neither GS1 EPCglobal nor ISO/IEC have defined a straightforward way to encode a compact HTTP URI identifier into a low-cost passive RFID tag. If such a mechanism were defined (eg in a future version of the GS1 EPC Tag Data Standard), then multiple industry sectors whose deeply entrenched identification systems prove to be unsuitable for straightforward translation into an existing EPC scheme could instead consider using a general-purpose method for encoding an HTTP URI into an RFID tag.

C.1.3. Unique identifiers for an IoT, with an RFID tag

It is important to understand that a unique identifier is stored in binary format in an RFID tag, and that the cheapest tags do so by providing a memory capacity of 96 bits, although tags with up to 480 bits for the EPC identifier are available, albeit at a price premium. Furthermore, a number of URL-shortening services (eg bit.ly, tinyurl.com and snipurl.com) are in common use on the web. These allow anyone to shorten a long URL to a much shorter URL consisting of a domain name such as 'bit.ly', a forward slash ('/') and then a string of mixed-case alphanumeric characters, which serves as a database lookup to the original long URL. On typing the shortened URL into a web browser, a script extracts the string of mixed-case alphanumeric characters and performs a database lookup, then issues an HTTP 301 (permanently moved) redirection header to the original full URL. However, there are concerns about the sustainability of the business models for such URL-shortening services, especially as some have discontinued their operations, so in practice, companies may prefer to register a short domain name themselves and operate their own URL shortening service internally. What now follows is a technical proposal for how this could be achieved.

This encoding procedure translates a short URL (or HTTP URI) of limited length into a binary string, suitable for encoding into an RFID tag with as few as 96 bits, although an additional variable-length EPC scheme up to a maximum of 480 bits can also be defined, to provide even greater capacity. The URL is assumed to be either constructed from a registered domain name (eg 'ex1.net') or to make use of an established well-known URL shortening service (eg 'bit.ly', 'tinyurl.com' etc).

C.1.4. Mapping URIs for encoding a binary string from EPC

In Figure C.1 the mapping shows how such URIs can be encoded and decoded from a binary string reader from the EPC/UII memory bank of an RFID tag, starting at position 20 hex. Both methods use an 8-bit header and a 4-bit filter value. A 4-bit filter value allows for a maximum of 16 possible values. The first eight of these might be aligned with the filter values defined for GS1 identifiers, leaving the next eight values (1000 to 1111) for user-defined filter values. The first method then includes an element, which represents the encoding of the registered second-level domain name. The string before the dot delimiter and top-level domain (TLD) (eg .eu) is treated as a sequence of alphanumeric characters that are converted to uppercase (since alphanumeric domain names are case-insensitive). Each character is then converted to an 8-bit ASCII byte and its most two significant bits are truncated. For each character, a 7-bit sequence is formed by concatenating a '0' bit (in the most significant bit position) followed by the 6-bit sequence from the ASCII byte with its two most significant bits truncated. For decoding from six bits back to eight bits, the following rule applies: 0xxxxx → 010xxxxx (uppercase letters A–Z), 1xxxxx → 001xxxxxx (digits 0–9).

Both methods then include an element that consists of two 7-bit sequences where the most significant bit is always a '1' – 1xxxxxx 1xxxxxx. The least significant six bits of each of these two sequences are concatenated to form a 12-bit integer in the range 000000 000000 to 111111 111111. It could then be proposed that the range 000000 000000 to 011111 111111 is reserved for lookup of the TLD, with some examples as shown in Figure C.1.

Figure C.1 Example of process of mapping of an EPC coding for a 96-bit RFID tag to Tiny URL

Field	Description	Length (bits)
For RFID tag	Example of 96-bit RFID tag with http://ex1.net/fJ4k3P as identifier	
EPC | **F**	**ex1 21 bits** | **.net/ 14 bits** | **fJ4k3P 42 bits**	
EPC header	8-bit header value (to be assigned by GS1), which distinguishes this EPC scheme from other EPC schemes	8
Filter value	4-bit filter value	4
Encoding of domain name portion before TLD **(eg ex1 in this case)**	7-bit sequences per character of second-level domain name consisting of literal '0' in most significant bit position, followed by 6 bits resulting from 8-bit binary representation of *upper-cased* ASCII code character, in the range ASCII 48–95, with the first two most significant bits truncated. For decoding of the 6-bit sequences to 8-bit ASCII bytes, 0xxxxx → 010xxxxx (upper-case letters A–Z) and 1xxxxx → 001xxxxx (digits 0–9) If a URL-shortening service is used this entire element is omitted.	21 ('pay load' = 18)
Lookup code for TLD **(eg .net/)**	Two 7-bit sequences, each with a '1' as the most significant bit. The remaining bits in positions a–f and g–l are interpreted as a 12-bit unsigned integer and mapped to either existing defined TLD names (this example) or to established URL-shortening services, eg bit.ly, tinyurl.com/ etc, so for example, for bits: *a b c d e f g h i j k l* : *0 0 0 0 0 0 0 0 0 0 0 0* = *.com/* *0 0 0 0 0 0 0 0 0 0 0 1* = *.org/* *0 0 0 0 0 0 0 0 0 0 1 0* = *.net/* *0 0 0 0 0 0 0 0 0 0 1 1* = *.info/* *0 0 0 0 0 0 0 0 0 1 0 0* = *.eu/* *0 0 0 0 0 0 0 0 0 1 0 1* = *.fr/*	14 ('pay load'= 12)
Encoding of path information (the part of the URI following the TLD and slash)	A sequence of six 7-bit sequences. Each represents a character of the path information following the slash (which is not encoded explicitly). For each ASCII character represented as an 8-bit binary string, truncate the most significant bit in order to obtain the corresponding 7-bit sequence. A 96-bit tag has capacity for a total of 10 characters consisting of the second-level domain name before the .TLD/ and the path information following the slash. In this example, the second-level domain name (ex1) occupies 3 characters and the path information occupies 6 characters (fJ4k3P). For the 96-bit scheme, any remaining bits following the encoding of the path information are set to zero padding bits, to reach a total of 96 bits for the EPC (7 bits here). If a longer EPC scheme or variable-length EPC scheme is also defined, additional capacity is available for the domain name and path information and trailing zero bit padding is applied up to the next 16-bit word boundary of the EPC/UII memory bank.	42

For tiny URL	Example of tiny URL mapping to http://tinyurl.com/fJ4k3P	

EPC header	8-bit header value (to be assigned by GS1), which distinguishes this EPC scheme from other EPC schemes	8
Filter value	4-bit filter value	4
Lookup code for TLD – designates type of tiny URL (eg tinyurl.com/)	Two 7-bit sequences, each with a '1' as the most significant bit. The remaining bits in positions a–f and g–l are interpreted as a 12-bit unsigned integer and mapped to either existing defined TLD names or to established URL-shortening services, eg bit.ly, tinyurl.com/ *a b c d e f g h i j k l : 1 1 1 1 1 1 1 1 1 1 1 1 = bit.ly/* *1 1 1 1 1 1 1 1 1 1 1 0 = tinyurl.com/* *1 1 1 1 1 1 1 1 1 1 0 1 = snipurl.com/ etc*	14 ('pay load' = 12
Encoding of path information (the part of the URI following the TLD and slash)	A sequence of 7-bit sequences. Each represents a character of the path information following the slash (which is not encoded explicitly). For each ASCII character represented as an 8-bit binary string, truncate the most significant bit in order to obtain the corresponding 7-bit sequence. A 96-bit tag has capacity for 10 mixed case alphanumeric characters of path information following the slash. For the 96-bit scheme, any remaining bits following the encoding of the path information are set to zero padding bits, to reach a total of 96 bits for the EPC. If a longer EPC scheme or variable-length EPC scheme is also defined, additional capacity is available for the path information and trailing zero bit padding is applied up to the next 16-bit word boundary of the EPC/UII memory bank.	42

C.1.5. International rules differ but a universal scheme is possible for URI based RFID

Note that some countries (such as the UK) do not allow registration directly under the TLD name of the country (eg .uk) so, instead, the effective TLDs (.co.uk, .org.uk etc) should be supported in Figure C.1. The range permits a total of 2048 TLDs, which is more than sufficient for those in current use, with capacity for growth. Furthermore, it is proposed that the range 111111 111111 to 100000 000000 is reserved for lookup of URL shortening services, such as tinyurl.com and bit.ly.

This range permits a total of 2048 such services, which is more than sufficient for the most popular URL shortening services in current use, with capacity for further growth. Both elements finally include an element, which represents the encoding of the 'path information' part of the URL that follows the TLD and the slash character that follows it. In the case of URL shortening services, it is this path information string that serves as the lookup key to redirect to the original URL that was shortened. Each character is then converted to an 8-bit ASCII byte and its most significant bit (a zero bit '0' for ASCII

characters 0–127) is truncated, so that each character can be encoded as a 7-bit sequence. This path information element permits mixed case alphanumeric characters and any symbol characters within the ASCII character set (ASCII 32–127) that can be encoded in a URL without the use of a percentage escape sequence.

C.2. Defining the problem – challenges for a global universal identification scheme

However, despite the efforts to establish a global EPC, some industry sectors have well-embedded existing practices for their specific domain's identification and already use these in data carriers other than RFID, such as nameplates, barcodes and matrix codes. Thus today many sectors have their own proprietary identification schemes with coding standards that may date back one or two decades.

The current schemes mostly come from the RFID world, but the IoT will cover a vaster range of items, some with identification meta-data models that do not necessarily align with the RFID world. Although in many cases they could be adapted, a universal scheme may need to be more flexible and wider ranging in its meta-data model.

In consequence, a single global identification scheme for all the attachable objects globally is not yet possible today. Moreover, it is highly unlikely that the commercial stakeholders will move to a different object identification system without strong commercial and regulatory pressures. Furthermore the current identifier authorities want to continue to manage their unique identifier schemes and yet leverage the next generation of information exchange.

So how could the transition to the IoT be managed?

Use of the internet is possible to some extent. Today, individuals, companies and industry sectors do not need to go to issuing agencies in order to construct HTTP URIs, but there are still a number of data carriers (linear barcodes and low-cost passive RFID tags) that have limited memory capacity and therefore require more efficient storage of identifiers. Such an approach does not appear simple and practical for a universal IoT identification scheme, although evidently various buffering and proxy solutions may be possible.

While use of HTTP URIs may lead to the further adoption of RFID itself, difficulties will arise when an industry sector finds that its existing (and perhaps deeply entrenched) identification scheme cannot be accommodated within an already defined EPC scheme, or in future IoT developments. In view of these 'legacy' identification schemes, consideration of a wide variety of vertical industry identification schemes to achieve a global object identification schema will be required for a universal identification scheme for electronic codes as examined above.

An alternative identification scheme approach is that of the MNOs, of using the existing mobile cellular numbering plan as an identification and addressing scheme for M2M communications, based on the SIM card IMSI for identification. Problems here are defined perhaps more by competition and market control issues, although there are also economic and technical issues, related to basic costs of connectivity and the geographical coverage as well as the suitability of the mobile architecture founded on base stations and a core network for IoT sensor networks that must be very low cost and geographically ubiquitous. Moreover, with mobile M2M schemes, there are problems related to deciding on the legal assignment of numbers and who is eligible to receive and hold large blocks of IMSI numbers for object identification. This is currently largely restricted to MNOs in the EU Member State and the assignment is national, as are the assignment policies. Thus today, each Member State NRA carries a responsibility to ensure that adequate numbers and number ranges are provided for 'publicly available electronic communications services' but also there is the problem of whether IoT communications actually fall within this category. Any decisions should facilitate a still developing market, but will have a major effect on any actor including the designation of service for those numbers. So far, eight European countries including Norway have M2M policies, generally limited to providing numbering resources for M2M purposes of between 10 and 100 billion numbering codes, so that the formation of EU-wide M2M networks is still fragmented in 2013 (COMREG, 2013).

C.2.1. There are key technology issues (with governance implications) in identification

In technology terms, there are also several areas of contention to resolve, where development of an IoT identification scheme can impact public policy in Europe, principally:

- *Identifiers as opposed to network addresses*: The IoT may cover a wide range of different address systems with conceptual differences between the identification by name of an object and its network address, or multiple addresses. In theory, the object identity may remain constant whereas addresses may change with physical locality. And although they may serve different purposes, a system could be used where address is the identifier.
- *Resolution and discovery functions*: If there is to be a global (unique) system which is scalable and interoperable, then a critical problem is constructing a suitable mechanism for object discovery and resolution in a mobile environment. If there are multiple identification schemes, this proliferates the difficulties and requires building a form of naming translation with a discovery scheme that enables the object in one namespace to find an object (by finding the information to locate it) in another namespace. In a

network of millions of devices such mechanisms would impose significant performance challenges for any resolution design.

- *Multiple or unique identifiers*: Today there is a drive in some IoT players and standards bodies towards unique identification systems, just as the internet has. However individual industrial sectors today have their own schemes. Development of the identifiers for various classes of IoT objects such as sensors, actuators and RFID tags is now in progress in certain industry sectors as well as in studies inside standardisation bodies (ITU and IETF).

It is not necessarily mandatory that identifiers be unique; objects that communicate only within closed environments can have 'local' names, at least for the purposes of strictly local interaction. Moreover, for efficiency, the topology of the name space should reflect both the need to economise the search efforts, which would be through large global registries, and to reduce probabilities of identification errors. However, unique identifiers have clearer lines of accountability than are seen with some forms of federated identity. It may also be necessary or useful to consider architectures for the formation of combined names for assemblages of objects. The issue here is whether internet protocols, even if security enhanced, can be trusted sufficiently when objects act autonomously and so the efficiencies of self-organisation may be sustained (Alam, Chowdhury and Noll, 2011; Heer et al., 2008).

Therefore, today it still seems unclear whether developments towards a globally unique scheme or several distinct identification spaces, with varying degrees of interoperability, will succeed.

Note that the alternatives of multiple or unique identification schemes have different public policy implications, with the unique identifier requiring major governance efforts in negotiations and long-term management when in operation by a suitable body. Table C.1 lists the impacts for governance of the two types of scheme.

Table C.1 Impacts for governance of multiple and unique identification schemes

Option	Impacts for governance
Globally unique scheme of identification	Requires global cooperation, which must be made pragmatic, to reach initial agreement, and for long-term operation Critical resource – single point of failure for IoT infrastructure, requiring governance rules that assure protection
Multiple addressing spaces and identification schemes	Multiple vertical sectors possible – with market control over competition – requires governance monitoring and intervention Interoperability between schemes is crucial – and is a point of failure; needs governance rules to assure open interworking with naming, addressing and discovery, and protection

Annex D. Critical infrastructure security

D.1. Threats in the IoT

As mentioned in Section 8.4, the full extents of vulnerabilities are as yet unknown in an IoT-enabled world. Table D.1 lists a series of potential threat actors.

Table D.1 Actors that might be threats in an IoT-enabled world

Actor	Motivation	Vector
Criminals	Economic gain	Breach confidentiality of sensor networks or e-meters in order to gain logical access to services illegitimately or defraud customers
Criminals	Desire to cause physiological or physical harm	Affect the confidentiality or integrity of information in IoT infrastructure in order to cause psychological distress, damage to property or human suffering
Terrorists or activists	Ideological	Tamper with or sabotage IoT infrastructure to cause disruption to society and spread panic or fear
Nation-states intelligence organisations	Economic or military advantage	Breach the confidentiality of IoT infrastructure in order to exploit information within, such as with criminal intelligence using IoT
Nation states	Economic or military advantage	Breach the confidentiality, availability and integrity of IoT infrastructure in order to achieve diplomatic, informational, military or economic gain
Economic actors	Economic gain	Fail to respect data protection obligations (eg sharing of data with third parties without consent); see below
Economic actors	Economic gain	Deliberate or accidental fraudulent activity designed to extract economic value from others

To this list of threats must also be added some risks[112] commonly understood from a safety perspective:

- human error (eg misconfiguration of infrastructure with different implications or accidental severing of undersea cable infrastructure)
- natural phenomena, 'acts of God' (eg floods, earthquakes, tsunami)
- systemic risks (emergent risks arising from the sheer complexity of the domain).

[112] We differentiate between threats (where there is a strategic adversary) and risks (which are driven by probability).

There has been evidence of such risks affecting internet infrastructure in recent times as the following examples illustrate.

In 2008, YouTube suffered an outage because of the misconfiguration of routers by Pakistani service providers (Van Beijnum, 2008). An internet service provider was asked to reroute traffic to the website for those within Pakistan but accidentally misconfigured the router, resulting in the site being invisible for around two-thirds of the rest of the world's internet users. The incident occurred because of the publishing of routes that the Pakistani ISP had set up to direct visitors to YouTube to an internet 'black-hole'. The routes were erroneously published to another peer in Hong Kong. As a result of the trust relationship between the Pakistani ISP and the provider based in Hong Kong, these were automatically released to the rest of the world, causing the outage.

In the same year, two undersea cables, SEA-ME-WE4 and FLAG-FEA, were accidentally severed in Alexandria. The SEA-ME-WE4 cable serves Europe, the Middle East and South Asia (Omer et al., 2009). According to the International Submarine Cable Protection Committee, 95 percent of transoceanic traffic goes via submarine cables (Van Beijnum, 2008). Two of these cables were located in the Gulf of Oman off Iran and resulted in serious interruption to internet traffic in the Arabian Peninsula as well as affecting traffic to and from India. This cable was also disrupted in 2010, which affected internet connectivity in India resulting in slow internet access for three to four days as repair attempts were performed. The 2008 cut resulted in India losing 50–60 percent of its bandwidth (Tech Exclusive, 2010).

The Hengchun earthquake in 2006 is another instance of how CIIs might be damaged, this time by 'acts of God'. Cable repairs involved eight ships and took 49 days, and internet traffic to and from China, Hong Kong, Vietnam, Singapore and Japan was impaired with banking, airline bookings e-mail and other services stopped or delayed. Delays were apparent some two months after the earthquake struck (Green et al., 2009).

D.2. Meta-analysis of security issues from the literature

In the remainder of this annex, we aim to summarise and present various important security, privacy and data protection issues concerning the IoT, by reviewing of some of the available technical, scholarly and policy peer-reviewed literature,. We analyse the available concerns and reformulate them from an independent perspective, noting where they are substantially different from those related to the constituent technological underpinnings (eg cloud computing) and where they are innovative.

An extensive amount has been written about security and privacy issues of the IoT. Indeed, a careful look at the results of the IoT Expert Group, consultation and other documents (European Commission, 2013) suggests that indeed security and privacy constitute the overwhelming concern. For example, the introduction to a report by the EU's own cyber

security agency, the ENISA, suggests that only by identifying and addressing the challenges and risks in a proactive way can the benefits of the IoT/RFID vision be realised (ENISA, 2010).

Nonetheless, despite this interest and the apparent formulation of these topics as a key concern for many stakeholders, it is not immediately obvious what is explicitly revolutionary about the security or privacy aspects of these topics. Indeed many do not seem substantially different from what is present in other domains but rather, as we have seen with cloud computing (Robinson et al., 2010) (itself a component of IoT), are legacy concerns made more acute and pressing by the particular characteristics or features of the IoT. Two examples, from privacy and security, may suffice.

As the IoT has a relatively ambiguous definition, it becomes difficult to pin down some of the security and privacy challenges associated with its development, all the more because the IoT will be dealing with considerable amounts of potentially sensitive data. In addition, interoperability issues that may arise as a result of the numerous possible approaches to ensuring privacy and security in 'IoT-enabled' devices must be taken into account. In general, whatever security or privacy solutions are proposed will need to be easily scalable as well as implementable on 'things' with resource constraints.

D.2.1. Overarching aspects of security challenges

With the prospect of the merging of physical objects and virtual spaces in the IoT, security and privacy are increasingly being seen as paramount to the overall success of the envisioned IoT, particularly from the point of view of social acceptance. On the one hand, the IoT should aim to accomplish a variety of societal and economic objectives, but, as the Vice President of the European Commission, Neelie Kroes, put it, this advancement should not be achieved at the cost of 'security, privacy and the respect of ethical values' (Europa, 2012).

In 2008, the IoT was identified in a study undertaken for the US National Intelligence Council (NIC) (NIC, n.d.) as one of six potentially disruptive civil technologies that could emerge over the next few years and have a significant impact on US interests (from a geopolitical, economic, military or social cohesion point of view) (NIC, 2008a). Significantly, the study concluded that 'to the extent that everyday objects become information-security risks, the IoT could distribute those risks far more widely than the Internet has to date'. Indeed, in NIC's report *Global Trends 2025* (NIC, 2008b), security and privacy concerns are reiterated as being key barriers to the universal implementation of the IoT. Thus, for the IoT to be a success, it is absolutely critical that it ensures citizens a trustworthy, unobtrusive, safe and secure environment within which to operate.

As yet the impacts of implementing the IoT are not known but might be foreseen to include issues such as:

- loss of confidence in IoT objects
- loss of trust in IoT infrastructure
- first order economic effects (fraud committed against consumers or firms)
- second order economic effects (inefficiencies caused by firms using IoT infrastructure having to price in worse security)
- loss of life or damage to property (eg compromise of IoT infrastructure in smart transport networks; urban infrastructure).

Polk and Turner (2011) discuss some of the security challenges that may be associated with the IoT. The four main areas of concern include applicability of currently available cryptographic techniques, credentialing or registering of devices, identity (user or device) management and privacy issues. Specifically, the current cryptographic algorithms being used in internet security protocols (Advanced Encryption Standard Block Cipher, Elliptic Curve Cryptography and so on) might need to be adapted to address these new challenges, a suggestion echoed by Roman, Najera and Lopez (2011). This is primarily because of the limited processor speed and memory that is expected in devices associated with the IoT. We recommend that the IoT protocol suites should include a configurable security solution that can be turned off when not necessary. As an extremely large number of devices are expected in the IoT, we suggest combining automatic and manual techniques for credentialing (eg the use of 'pairing protocols' such as those employed in Bluetooth security) for initial deployment. The large number of devices and limited user interfaces will also pose problems in identity management. In addition, we propose the use of automated key management techniques since manual configuration of devices ('pre-shared keys') currently used in many internet protocols may be difficult to implement. Another important consideration will be to provide usable security that a device is able to utilise with minimal difficulty. Finally, potentially significant privacy issues that might compromise the IoT may lead to the consideration of adopting older technologies once used in military and intelligence communities to prevent leakage of information.

Edwards (2012) talks about how collections of tiny, smart sensors (what is referred to as 'smart dust') are being used in different everyday scenarios to gather information about people's whereabouts. He uses the example of the SmartSantander project in Spain, where a series of parking sensors embedded in the tarmac will sense whether a parking space is occupied by a car or not. Other examples include GPS-assisted sat-nav systems in cars, which help in traffic automation, or small-scale networks used in smart homes. The interconnection of these multiple sensors will lead to one or more larger information-sharing networks, as is envisaged in the IoT. It is important to know how the public will react to this so-called invasion of privacy where smart dust is effectively transforming into 'surveillance dust', which is being used to track people in real time. In 2012, the European Commission started considering ways of updating the existing Data Protection Act to deal

with the IoT. A survey was conducted to determine how much of their privacy people were willing to give up to 'support' the aims behind the IoT, such as energy efficiency and building automation.

D.2.2. Examples of security analysis of IoT enabling technologies

In this section we present some examples of the security analysis of some of the contributing technological foundations of the IoT.

Mayordomo et al. (2011) propose RFID, wireless sensor networks and real-time location systems as the three key enabling technologies for the IoT. With particular reference to the security and privacy aspects of RFID, we outline the following four simple steps to handle risks:

- analyse the application environment
- identify and assess potential threats
- identify and assess potential countermeasures
- implement the 'top' countermeasures (recommended actions).

A further analysis of the application environment after the fourth step can determine whether or not the selected countermeasures have sufficiently reduced the threats. To ensure integrity of data, the technological countermeasures listed are permanent write-locking of memory, the addition of cryptographic functions to passive RFID, and the addition of physical unclonable functions to a tag. Furthermore, privacy may be assured by encrypting the over-the-air communication and adding the ability to operate in silent mode.

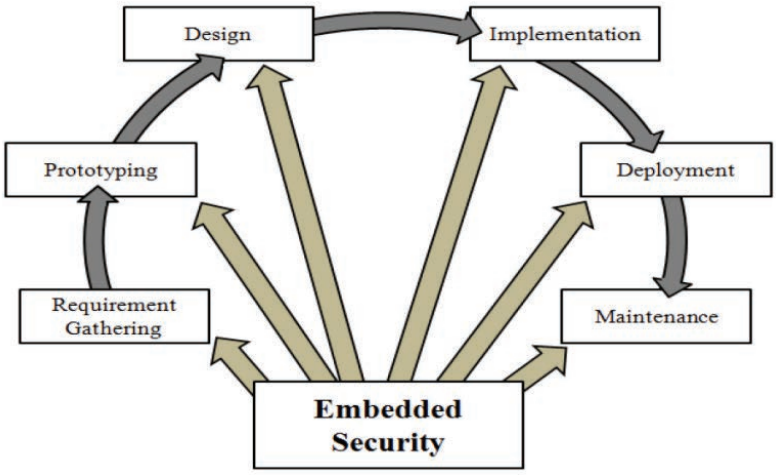
Babar et al. (2011) carry out a detailed survey of embedded security in the context of the IoT. After summarising various possible types of attacks on IoT devices (physical, side-channel, environmental, crypto-analysis, software and network attacks), we identify eight primary security concerns for the IoT:

- user identification
- tamper resistance
- secure execution environment
- secure content
- secure network access
- secure data communication
- identity management
- secure storage.

Limited computational power, battery capacity and storage are identified as obstacles for embedding security features in IoT-enabled devices. A software–hardware design methodology is proposed to aid the design of more secure devices. The various steps

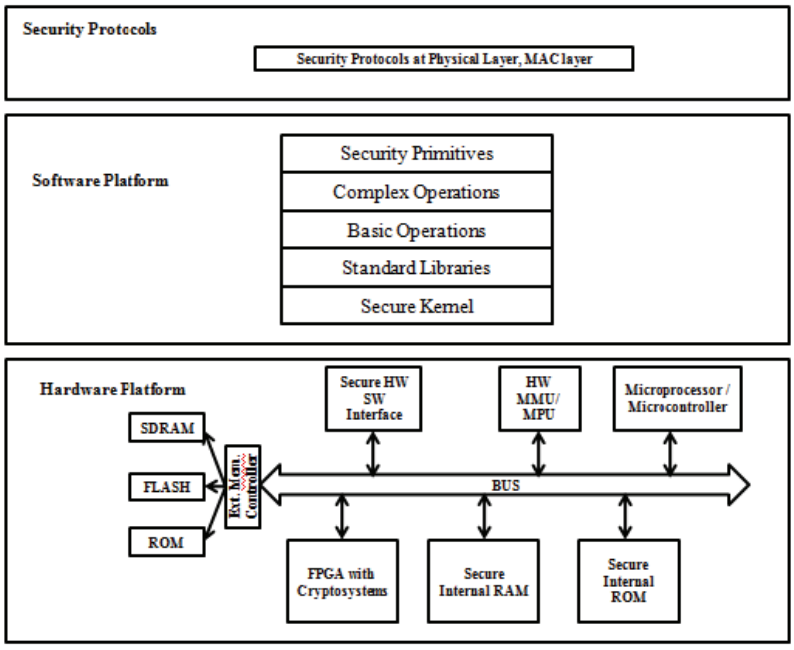
involved in the embedded security design 'life cycle' are illustrated in Figure D.1, while Figure D.2 presents the proposed embedded security framework and architecture. As shown, the architecture has hardware and software platforms along with supporting security protocols at the physical and medium access control (MAC) layers.

Figure D.1 Steps involved in the embedded security design life cycle



Source: Babar et al. (2011)

Figure D.2 Embedded security architecture for IoT devices proposed by Babar et al. (2011)



Caceres and Friday (2012) review some of the research in the field of ubiquitous computing (ubicomp) over the last 20 years. They discuss opportunities available to improve the existing ubicomp infrastructure and highlight some of the future challenges associated with ubiquitous computing. The IoT is presented as a significant opportunity

for developing the large scale infrastructure needed by future ubicomp systems. Setting up such large scale infrastructure would require both industrial involvement and investment. The 'repayment' of these investments is where privacy concerns arise for ubicomp systems. One way of repaying them is by revenues generated through advertising (popular online social networking services use this method). Services using this method of repayment are generally free for users, but the downside is that the service provider is often given rights to use the data supplied by the users, raising important privacy concerns. A slightly different technique, where the user pays for the service, has better privacy options. In this case, the service providers do not have any rights to the information provided by the users, but for this technique to work, ubicomp systems and their applications must provide sufficient value to their customers.

As we have seen, seemingly 'safe' devices such as white goods are also vulnerable to malware and hackers as more and more of these devices begin to get connected through the IoT. Amid the backdrop of increasing numbers of home appliances going online, Arabo and El-Mousa (2012) present a novel security framework for smart devices in a home environment, specifically proposing a dynamic and portable modular device security framework (for the Connected Home 3.0) that addresses several security threats and vulnerabilities associated with smart devices. The framework offers a novel approach to include data security functions for 'things' by isolating personal content (which is, in turn, done by producing a virtual lock on 'things'). Each individual device within the network has the capability of securing itself instead of relying on 'upstream' or 'downstream' security measures for protection.

Haselsteiner and Breitfuß (2006) present an overview of the strengths and weaknesses of NFC technology using a systematic approach to clear up misconceptions about NFC technology (ISO18092) for communications within 10cm. They list threats and describe solutions to protect against them in the context of currently available hardware, applications and possible future developments. They find the main threats are:

- *eavesdropping*: an attacker listens into a supposedly secure channel between two parties
- *data corruption*: the attacker corrupts data so that the data does not make sense for the recipient
- *data modification*: the attacker modifies (not corrupts) data so that the recipient receives data that looks legitimate but are different from those originally intended by the sender
- *data insertion*: an attacker inserts messages into a data exchange

- *man in the middle attack*: an attacker tricks two parties into a three party exchange. The attacker sends and receives data so that the two parties do not suspect that there is a third party in the conversation.

The RFID distance bounding protocol designed by Kim et al. (2008) is considered the most secure distance bounding protocol for RFID. They design a protocol that withstands different types of relay attack (including fraud, where there is a degree of collusion between the tag and the reader, and finally where there is an intruder or illegitimate reader or tag).

In a paper given to RFIDSec in 2009, Courtois (2009) discusses attacks against MiFAREClassic, a crypto-algorithm used in many smartcards. This paper illustrates how economics can affect security – MiFARE Classic Crypto 1 (originally implemented by Phillips) is used by 70 percent of the world's building access cards yet is proven to be insecure. He identifies that secrecy in product development and the specifications for the chip, while being an advantage from a business perspective (as it creates barriers to entry for competitors and has some benefit against hackers), may be counterproductive. This is the case when there is space or undocumented features on the smart card that are not revealed by the specification but can nonetheless be exploited by an adversary.

Hussain and Abdulsalam (2011) propose a model of cloud-based Security as a Service (SECaaS), which deals with existing services of cloud computing. They propose a security architecture model that is user centric, where cloud users have more control over their security. This has the expected benefits of providing more security to cloud-service users and providers.

The technical security risks related to cloud computing have also been the subject of much discussion (see, for example, Jensen et al., 2009; Ristenpart et al., 2009; Chen, Paxson and Katz, 2010) and have been summarised elsewhere (Robinson et al., 2010).

Yan, Rong and Zhao (2009) use public cryptography along with federated identity management to address the case where each cloud contains multiple clouds. The approach achieves single sign-on, allowing a user to authenticate at one cloud provider, yet be able to access her accounts at other cloud providers as well. Single sign-on simplifies the authentication of users.

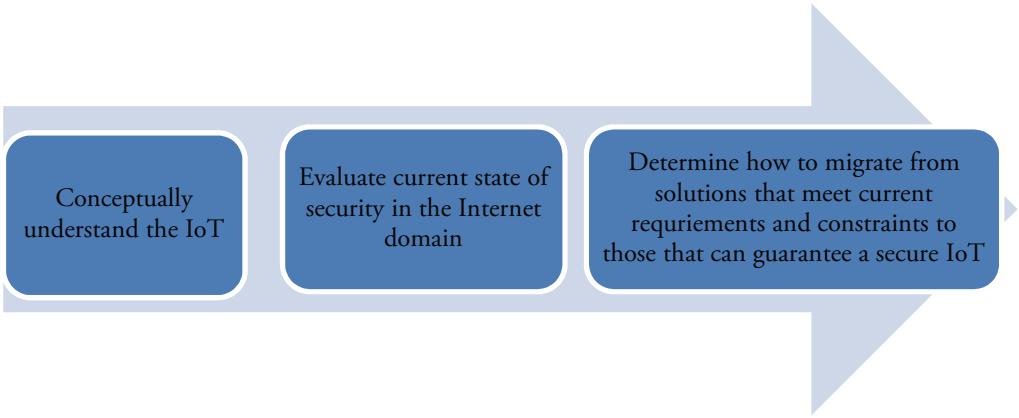
Creese et al. (2009) present a capability maturity model for cloud-computing providers, which permits the assessment of the security and protection offered by cloud-service providers for personal data when stored in the cloud. They suggest that service providers may use design patterns to mitigate security and privacy risks, as well as monitoring to provide a degree of assurance that controls are implemented.

D.2.3. Indicative technical solutions

In this section by way of illustrative examples we present some approaches that researchers have developed to formulate solutions to some of the previously mentioned security challenges.

At a generic level, Roman, Najera and Lopez (2011) outline some key steps in effectively implementing security measures in the IoT, which are presented in Figure D.3.

Figure D.3 Key steps involved in executing IoT security measures successfully



Source: Roman, Najera and Lopez (2011)

Zhou and Chao (2011) propose a novel media-aware security framework for supporting multimedia applications in the IoT. In order to achieve this, we first present a traffic classification and analysis for the diverse multimedia applications running over IoT (these can be divided into three main categories: communication, computation and service). Based on this classification, they propose a media-aware traffic security architecture in the IoT context, which consists of four major components: key management, batch rekeying, authentication and watermarking. In summary, this architecture makes diverse multimedia services available to users anywhere and anytime.

Liu, Xiao and Chen (2012) propose a feasible authentication and access control technique for the IoT. The authentication technique uses a simple and efficient secure key establishment (based on an elliptic curve cryptosystem); for access control, we suggest a role-based access control authorisation method using the IoT object's role and application in the associated IoT network. Based on the analysis conducted, we conclude that the authors' proposed protocols and algorithms can feasibly prevent attacks in various in IoT scenarios (such as eavesdropping attacks, the man-in-the-middle attacks, key control attacks and replay attacks).

Cadzow (2012) suggests that, particularly in the context of sensor and distributed systems, in order to improve the privacy and security of the system, it is necessary to form a 'trusted and bounded relationship' between the sensors (the data subjects), the data processors and the data controllers. From the regulatory framework point of view, privacy impact

assessments are increasingly being seen as tools to better understand prospective data protection and privacy risks. Furthermore, consent relationships can be agreed using ETSI's Test Purpose Language (TPLan) and then exported as assertions using Security Assertion Markup Language.

Oualha and Olivereau (2011) present a survey of current approaches to ensuring privacy protection in wireless sensor networks in industrial domains, highlighting the necessity for developing novel privacy preserving mechanisms. As has been pointed out previously, the primary challenge is to create identity anonymisation techniques, cryptographic operations and so on that can be efficiently supported by resource-constrained sensors. We briefly discuss a European project called TWISNet (http://www.twisnet.eu/) whose main objective is the development of a secure, reliable and efficient architecture for the integration of wireless sensor networks in large-scale industrial environments.

While presenting an analysis of some of the legal-regulatory data protection and privacy aspects of the IoT and the European Commission's work in this area, Gumzej (2012) highlights the significance of incorporating data protection principles into the data processing systems, citing that this is a 'sound reason for further research in this area, and for conceiving ways to ensure innovative Internet of Things for people while acknowledging consumer concerns that have until today had considerable impact at the EU level'.

Doukas et al. (2012) present a security framework for a prototype IoT compliant cloud-based system that aggregates health sensor data and helps to resolve security issues by means of digital certificates and public key encryption. Lehtonen, Staake and Michahelles (2006) present an overview of RFID product authentication techniques, investigating how RFID can be used in product authentication in a supply chain context. They analyse different categories of RFID product authentication approaches in the context of anti-counterfeiting. Juels and Weis (2009) produced a reference paper which defines strong privacy for RFID. Mitrokotsa, Rieback and Tanenbaum (2008) developed a classification of RFID attacks by presenting a structural methodology for the potential risks that RFID networks face.

Annex E. IoT architecture: players, roles and focus

Table E.1 provides a high-level overview of the current architecture initiatives – the players, their roles and specific focus. It is not exhaustive, but aims to give the main highlights

Table E.1 Key public sector players, their role and IoT focus for architecture

Public sector player	Role	IoT focus
European Commission	Promotional RDI Regulatory Statutory legislation (privacy etc)	Rapid advance of IoT for stimulating EU economy – relationship with all players
National Member State governments	RDI Regulatory	Advance of IoT (at varying pace) for stimulating own economy – strong relationships with national players such as the MNOs
OECD	Provide input to policy for its 34 member nations	Applications that affect member governments – e-health, water, smart infrastructures, trade and RFID, sensor networks, smart manufacturing, energy and transport grids, with analysis of drivers for government policy on such areas as privacy, security and energy policy and competition challenges
NRAs	Set national regulatory agendas for communications in concert with international bodies (ITU, CEPT, RSPG etc)	Manage national spectrum allocation Maintain level playing field for all IoT players, via competition policy (eg COMREG, 2013)
Standards organisations		
ISO	Standards body	Coordinates activities of its technical standards bodies, notably ITU and

Public sector player	Role	IoT focus
		International Electrotechnical Commission (IEC), for all aspects of IoT, including identification and supply chain, RFID, spectrum, etc; offers open standards for interoperability and for RFID (ISO 18000) such as the 18000-7 ('DASH7') wireless sensor network standards for the 433.92MHz licence exempt ISM band
ETSI	EU standards in telecommunications	Open M2M model of architecture with special working group
CEN	Electronics technology standards in Europe	RFID standards
ITU Telecommunication Sector (ITU-T)	Regulation and standards	Agreements on open architectural models and standards
ITU Radiocommunication Sector (ITU-R)	International spectrum regulation	Regulation through global negotiations, largely in WRCs with their preparation
European Communications Office (ECO)	European spectrum regulation	Relevant to spectrum debate in the EU for RFID and System Reference Documents (SRDs) and longer range licence exempt bands
CEPT	Spectrum regulation	SRD bands (ISM) and usage constraints
IEC	Standards body for electrical and electronics equipment – with committee ISO/IEC/JTC-1 for standards for ICTs, with national bodies as members	Electrical and electronic consumer goods industries through a special working group on IoT gaps in standards and market requirements for IoT
International Committee for Information Technology Standards (INCITS)	ICT standards	Study group to coordinate ISO bodies (particularly Joint Technical Committee-1)
IETF	Internet engineering and standards body	Relevant standards in RFCs for networking and inter-process communications and design discussion documents (eg see Lee, 2011)

Public sector player	Role	IoT focus
World Wide Web Consortium (W3C)	Web engineering and development for compatibility through open standards	Architecture for web-based platform – also the 'web of things'
Research institutes		
Fraunhofer IML	R&D	IoT research for industry
Cambridge, MIT, Auto ID Centre	Research into RFID and identification schemes	Identification and EPC for RFID, in line with ISO/GS1
EPRI (US)	Industry focus research	Smart grid research for the electricity industry
Industry consortia	Role	IoT focus
DASH7 Alliance, 50 members, 23 countries	Promotion of 18000-7 standard products though interoperability	Interoperability testing and certification for DASH7 devices, tags and sensor networks; also ZigBee IEEE 802.15.4 at 2.4GHz (915 and 868MHz in some countries)
European projects		
IoT-Architecture	Create European IoT architecture	Generic architecture with reference model
CASAGRAS 1 & 2	Create IoT architecture	RFID focused
Major private sector players – large MNCS		
GE (US)	Industrial conglomerate	Has own concept of the 'industrial internet' for highly focused advanced manufacturing
Google (US)	Web services	Android-based software
Intel	Supplier of semi-conductors for IoT devices	Processor with storage (no RF)
ARM Holdings (EU)	Supplier of central processing unit designs on a royalty basis – low power designs for IoT devices	Chiplets with RF stage incorporated
Xerox PARC	Industrial R&D	Designs for chiplets with thin film organics as substrate for lower cost and size
Texas Instruments	Supplier of semi-conductors for IoT devices and networks	DASH7 network, sensors and RFID tag supply
STMicro	Supplier of semi-conductors for IoT devices and networks	DASH7 network, sensors and RFID tag supply
CISCO Systems	Supplier, networking	Promotes own product range for Internet of Everything (IoE) with own

Public sector player	Role	IoT focus
		forecasting team
VeriSign and Symantec	Cyber-security products and services, especially for digital certificates and signing	Software and services to operate a secure IoT
SMEs		
Neul (EU)	Supplies WSD networks and devices for M2M market	Architecture based on specific protocol – 'weightless' for WSDs for M2M
SIGFOX	Supplies networks and devices for the M2M market	Own cellular technology, based on narrow band technology for low bit-rate signals
Other		
Department of Defense (US)	Defence and financing of defence projects	Has financed the largest sensor network globally using DASH7and open tag, open source software OS; NATO to comply
Federal Communications Commission (FCC)	Spectrum regulation	Regulates US spectrum – regulatory stance can form an example for other regions, eg Part15 rules for 902-928 MHz for SRDs Does not interact outside US except as national opinion via ITU debates, via Dept Commerce
Presidential Counsel of Advisors on Science and Technology (PCAST) (US)	Publishes forward looking reports on what is effectively US industrial policy for high technology and innovation areas to pursue – specifically designing a digital future	Release of federally held spectrum for licence exempt uses – SRDs etc Medical patient data systems Advanced transport solutions

Annex F. Identification: players, roles and interactions

Table F.1 lists the major players in the identification world, their roles and foci with their interactions; a detailed analysis for the RFID side of identification can be found in the GRIFS project report.[113] It is not exhaustive but aims to give the main highlights.

Table F.1 Key public sector players, their role, IoT focus for identification and relationships with other bodies

Public sector player	Role	IoT focus	Relationships with other bodies
European Commission	Promotional RDI Regulatory	Rapid advance of IoT through common identification for stimulating EU economy – relationship with all players	Orchestration of interworking at national Member State, EU and global level
National Member State governments	Regulatory	Rapid advance of IoT for stimulating own economy relationship with national players	Rulemaking for own market and spectrum area
OECD	Provide input to policy for its 34 member nations	Applications that affect member governments on RFID and EPC and infrastructure subjects	Works with other international bodies, eg ISO, ITU, IEC
NRAs	Set national regulatory agendas for communications	Maintain level playing field for all IoT players, eg management of competition by MNOs through numbering, IMSI and SIM card	Work with national and EU bodies for regulation on telecoms and competition
Issuing authorities			
GS1	Issues product identification codes commercially	Electronic product numbering codes for vertical sectors	Works especially with sector consortia, also with ISO and some other standards

[113] The GRIFS project was aimed at closer cooperation between the various RFID standards organisations and players. Its final report (GRIFS, 2010) provides a highly detailed inventory of RFID-related standards bodies, the technical standards and degrees of collaboration.

Public sector player	Role	IoT focus	Relationships with other bodies
			bodies such as OASIS
Dun & Bradstreet	Issues product identification codes commercially	Electronic product numbering codes for vertical sectors	Works with ISO
ISO	Open identification codes including for issuing authorities	Electronic product numbering codes for vertical sectors	Works with all other issuers, commercial and public sector
Vertical sector groups			
Health Industry Barcode Council	Issues codes with support services for health sector	Electronic product numbering codes for vertical sector	Works with some other issuers and standards bodies such as ISO
SITA, air transport	Provides identification infrastructure	Electronic product numbering codes for vertical sector	Works with issuers and standards bodies
Air Transport association (Airlines for America)	Issuing codes with support services for sector	Electronic product numbering codes for vertical sector	Works with other issuers and standards bodies such as ISO
Organisation for Data Exchange by Tele Transmission in Europe (ODETTE)	Support services for automotive sector – cars and components – issuing codes with support	Electronic data exchange and product numbering codes for vertical sector – RFID identification schemes	Works with other issuers and standards bodies such as ISO
EDIFICE	European group for suppliers of electronic components, consumer and computer products	Electronic data exchange and product numbering codes for vertical high tech sector for B2B supply and distribution chains	Works with other issuers and standards bodies such as ISO
		Electronic product numbering codes for vertical sector	Works with other issuers and standards bodies such as ISO
Standards organisations			
ISO	Standards body	Coordinates activities of its technical standards bodies, notably ITU and IEC for all aspects of identification and supply chain, with RFID, spectrum, etc; offers open standards for interoperability and for RFID (ISO 18000) such as the18000-7 ('DASH7') wireless sensor network standards for the 433.92MHz licence exempt ISM band	Provides basis for specialised identification standards in each vertical sector Provides basis for GS1 identification codes

Public sector player	Role	IoT focus	Relationships with other bodies
GS1	Standards body and issuing authority maintaining a list of data identifiers as code numbers, used by its member organisations, for RFID systems for automatic identification and data capture (AIDC)	Identification standards for specific vertical sectors using ISO standards for supply chain, in retail, food processing, health care etc, especially the EPC global code for RFID; also in automotive (ODETTE from the Electronic Data Interchange or EDI); similarly EDIFICE, from EDI, in electronics industry; has contracted VeriSign to operate an ONS system for EPCglobal for IoT applications	Works with end users of identification schemes, and global standards bodies, such as ISO
ETSI	EU standards in telecommunications	RFID technology, identification and product coding, working groups	Cooperates with other technical bodies at EU and global level (CEN, CEPT, IEC, ITU, etc)
ITU-T	Regulation and standards	Agreements on open architectural models and standards	Cooperates with other technical bodies at EU and global level (CEN, CEPT, ETSI, IEC, etc)
ITU-R	Spectrum regulation	Regulation through global negotiations, largely in WRCs	Global forum for spectrum debate for RFID etc
ECO	Spectrum regulation	Radio standards – including RFID	Close cooperation with official EU standards bodies and EC via formal process
CEN	Electronics technology standards in Europe	RFID standards	Strong cooperation with official EU standards bodies and EC via formal process
CEPT	Spectrum regulation	RFID standards	Strong cooperation with official EU standards bodies and EC via formal process and with private industry
OASIS	Standards for security and encryption	RFID and related standards for industry members	Strong cooperation with most players
IEC	Standards body for electrical and electronics equipment, especially ISO/IEC JTC1 SC31 (WG4)	Electrical and electronic consumer goods industries through a special working group on IoT gaps in standards, and on market	Develops standards in association with GS1, CEN, CENELEC, EPCglobal, ETSI,

Public sector player	Role	IoT focus	Relationships with other bodies
	with 8 other IEC committees, including 14443	requirements for IoT	IEEE, IATA, ITU-R, AIMglobal
IEEE	Standards body in electronics, software and networking	RFID, reader and related standards, also for networking, including SRDs	Strong cooperation with most players, public and private sector
INCITS	ICT standards	Study group to coordinate ISO bodies (particularly the Joint Technical Committee-1)	Works with all ISO bodies on specific areas such as identification
Research institutes			
Cambridge, and MIT, Auto-ID centres and other international labs	Research into RFID and identification schemes	Identification and EPC for RFID, in line with ISO/GS1	Work with GS1 and ISO
Industry consortia			
Schema.org, a group of search engine operators – Google, Bing, Yahoo and Yandex (Russia)	Create meta-data for machine-readable identifiers for semantic parsing	Common set of schemas for structured data mark-up (usually for web pages)	Little direct collaboration but could provide meta-data for search and discovery for mapping with other identification schemes
DASH7 Alliance, 50 members, 23 countries	Promotion of 18000-7 standard products though interoperability	Interoperability testing and certification for DASH7 devices, tags and sensor networks; also ZigBee IEEE 802.15.4 at 2.4GHz (915 and 868MHz in some countries)	Use identification issuer codes (GS1, ISO)
Major private sector players – large MNCs			
Texas instruments	Hardware supplier and technical support	Transponders, readers, RFID tags	Works with other hardware suppliers and standards bodies
SAP	Software supplier for AIDC supply chain management	Use of RFID in supply chain	Works with hardware suppliers and standards bodies
VeriSign and Symantec	Identification services provider	Offer services for identification	Contracted by GS1 to operate ONS servers
CISCO Systems	Networking supplier	RFID middleware and	Works with components and

Public sector player	Role	IoT focus	Relationships with other bodies
		networking	software suppliers and standards bodies
Oracle	Database and management software supplier	Database and supply chain software with RFID identification processing	Works with components and software suppliers and standards bodies
Siemens	Supplies software, hardware and systems integration	Identification software and RFID components and supply chain software	Works with components and software suppliers and standards bodies
SMEs			
AIDC Solutions (UK)	Suppliers of RFID tags and readers with software and systems integration services (effectively minor players which tend to be followers of industry norms and market trends)	RFID systems and systems integration in specific sectors – eg warehouse stock control management	Use existing standards – hope for common agreements
Other			
National patient identification schemes – eg NHS (UK)	Manage patient data records	Use of RFID-based and other identification schemes	Works with GS1 for issuing and ISO for standards
FCC	Spectrum regulation	RFID spectrum	Works with telecoms industry bodies such as ITU