

BEFORE THE
UNITED STATES DEPARTMENT OF COMMERCE,
National Telecommunications and Information Administration

In the Matter of

The Benefits, Challenges, and Potential Roles for the
Government in Fostering the Advancement of the
Internet of Things, Notice and Request for Comment

)
)
)
)
)
)
)

Docket No. 160331306-6306-01

RIN 0660-XC024

Megan Doberneck
General Counsel

Blair A. Rosenthal
Assistant General Counsel

Vodafone US Inc.
999 18th Street, South Tower #1750
Denver, Colorado 80202
+1-720-484-0554

BEFORE THE
UNITED STATES DEPARTMENT OF COMMERCE,
National Telecommunications and Information Administration

In the Matter of)	
)	
The Benefits, Challenges, and Potential Roles for the)	Docket No. 160331306-6306-01
Government in Fostering the Advancement of the)	
Internet of Things, Notice and Request for Comment)	RIN 0660-XC024
)	
)	

COMMENTS OF VODAFONE US INC. d/b/a VODAFONE AMERICAS

Vodafone US Inc. d/b/a Vodafone Americas ("Vodafone"), through its undersigned attorneys, submits these comments in response to the NTIA's Notice and Request for Comment in the above-referenced docket ("Request for Comment").

I. INTRODUCTION

Vodafone is a wholly-owned subsidiary of Vodafone Group Plc, which holds affiliates that operate throughout the world, serving more than 400 million customers in 30 countries and reaching 50 more countries through partner networks. Vodafone is actively involved in providing Internet of Things ("IoT") services in the U.S., across the E.U. and in many other countries across the globe, including importantly emerging markets in Africa and Asia. Vodafone is a recognized leader in the IoT, and continues to be recognized by leading analysts as the "number one global operator" in the machine-to-machine ("M2M") space¹ and "ranks as the strongest communication service provider" in Analysys Mason's 2015 M2M scorecard.² Currently, Vodafone has 21.5 million connected devices on its IoT network, a 30% increase in connections from the prior year,³ consuming 84 million Mb of data every month.⁴ Vodafone IoT revenue

¹ See <https://machinaresearch.com/news/m2m-csp-benchmarking-report-2015-the-fast-growing-and-increasingly-competitive-m2m-csp-business-sees-continued-global-leadership-from-vodafone-and-att/>

² See <http://www.vodafone.com/business/m2m/vodafone-tops-analysys-masons-independent-m2m-annual-scorecard-for-record-fourth-time>.

³ See Vodafone Annual Report 2015 at 17 (http://www.vodafone.com/content/annualreport/annualreport15/assets/pdf/full_annual_report_2015.pdf).

⁴ See Presentation of Matt Key at Westminster eForum, "Vodafone Internet of Things: Enabling the IoT" (March 15, 2016) attached as **Annex A**.

growth is equally impressive, with a 24.7% year on year increase.⁵ Importantly, Vodafone includes privacy in the design of its IoT offering, thereby ensuring the security and privacy demanded by the European Union of the data being carried across its IoT network.

Vodafone welcomes the opportunity to participate in this timely proceeding on a topic that is of keen interest to Vodafone and of vital importance to the U.S. and the rest of the world. Indeed, the U.S. Ambassador to the European Union recently stated that, "The scale of the opportunities and challenges related to the Internet of Things literally makes everything else on the U.S.-E.U. agenda seem secondary."⁶ Given our role as a leading provider of IoT services in many countries around the world, we are very happy to share our experiences with the NTIA on this topic.

The scope of the comments sought by the NTIA is wide ranging and covers a number of important topics related to the IoT. In our response, Vodafone outlines its positions on key topics relevant to the questions the NTIA raises, with further detail contained in supporting documents set out in the Annexes. Vodafone believes its comments will provide insightful guidance and commentary as the NTIA contemplates policymaking in this area and, if requested, would be pleased to elaborate on any point discussed.

⁵ Annual Report at 17.

⁶ "The Internet of Things: A Transatlantic Bridge to the Future", remarks at the 7th Annual Internet of Things European Summit by U.S. Ambassador Anthony L. Gardner (May 18, 2016) (<http://useu.usmission.gov/sp-051816.html>).

II. VODAFONE'S COMMENTS ON THE KEY BENEFITS, CHALLENGES, AND POTENTIAL ROLES FOR THE GOVERNMENT IN FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS.

The U.S. government can play a critical role in ensuring the realization of IoT's vast and full socio-economic potential for both U.S. businesses and consumers. This includes collaborating with other governments, industry, and standards bodies to remove (or refrain from putting in place) barriers to the cross-border flow of IoT devices and services and the data flowing from those devices and services and otherwise incenting the use of IoT to promote socio-economic benefits. In general, we believe that the U.S. government should rely on existing law, in conjunction with existing industry self-regulatory initiatives, to regulate the IoT.

A. Recognizing the Vast Potential of IoT, the Government Should Incent, And In Some Cases, Mandate, The Use of IoT In Areas Where Such Use Would Yield a Clear Health, Safety, or Other Socio-Economic Benefit.

In its Request for Comment, the NTIA asks whether it should attach any specific definitions in examining the IoT landscape.⁷ Broadly speaking, Vodafone believes it unwise to rigidly adhere to a definition of IoT given it is such a fast-moving area but that it would nonetheless be helpful for the NTIA to attach descriptions to different elements of IoT, in order to guide its policy making activity.

With this in mind, we suggest definitions of IoT and "Machine-to-Machine" or "M2M" that can be found in our most recent IoT Barometer⁸, which uses the following definitions:

Internet of Things ("IoT"): is the connection of machines, devices, and objects to the Internet, turning those items into "intelligent" or smart assets that communicate with the world around them. IoT is both a technology and service offering.

Machine to Machine ("M2M"): is the remote (typically wireless) data exchange between two or more devices or a central station that allows remote monitoring and control of devices and processes and the sharing of information between those two things. IoT is dependent upon M2M, as M2M is essentially the "plumbing" for IoT.⁹

The IoT Barometer shows how businesses are adopting this emerging technology: which regions and industries are pulling ahead, and how fast the market is growing. We think this ongoing research is helpful in a

⁷ Request for Comment, Question 2.

⁸ Each year, Vodafone publishes research on the evolution of IoT and the benefits it brings to our customers. The Vodafone M2M Barometer 2015 (the "Barometer" or "IoT Barometer") is attached as **Annex B**.

⁹ See **Annex B** (citing Machina Research).

market like IoT, and, in response to Question 11 of the Request for Comment (in which the NTIA asks if IoT should be measured or quantified), we certainly encourage the NTIA to track the growth of the IoT sector.

In Question 3 of the Request for Comment, the NTIA asks if there are current or planned laws, regulations, or policies that foster IoT development and deployment. According to our 2015 IoT Barometer, energy and utilities, automotive and retail lead IoT adoption.¹⁰ The growth in the energy and utilities sector is driven by long-running infrastructure modernization initiatives and ambitious government targets, which shows that government policy has an important role to play in ensuring that the full and substantial benefits of IoT for businesses and consumers in the U.S. are realized.

The benefits of actualizing the potential of IoT is underscored in a recent KPMG report prepared in conjunction with Hogan Lovells and commissioned by Vodafone.¹¹ In the study, KPMG estimated that the gross value add generated by providers of cellular M2M¹² services alone was in the region of €2.5 billion (roughly \$2.75 billion at today's exchange rate) in 2013-14.¹³ KPMG further found that the wider socio-economic benefits from IoT "are likely to be substantially higher."¹⁴

These benefits are only going to increase as the IoT proliferates: KPMG estimates that the number of "things" connected to the Internet will double from 25 billion in 2015 to 50 billion in 2020. Some important and specific examples of socio-economic benefits of the IoT include:

- **Emergency call services** – In the event of a crash, an emergency call services-equipped (eCall) vehicle will automatically trigger an emergency call, which sends information on the accident, including location, to the emergency services. Studies on the benefits of eCall in the E.U. have shown that eCall cuts emergency services response time by 50% in the

¹⁰ See **Annex B**.

¹¹ KPMG in association with Hogan Lovells, *Securing the Benefits of Industry Digitisation: A Report for Vodafone* (November 2015) ("KPMG Report") attached as **Annex C**.

¹² There are multiple manners in which IoT services can be delivered. Currently, the typical, and generally only, manner in which IoT services are provided is via cellular technology. But as discussed in more detail in its comments below, Vodafone believes that the future of IoT will only be truly realized with the development of 5G.

¹³ See KPMG Report at 6, available at **Annex C**.

¹⁴ *Id.*

countryside and 60% in built-up areas.¹⁵ On this subject, the U.S. government should take its cue from the European Union, which mandated eCall for new cars beginning in 2018.¹⁶

- **Smart metering** – It is estimated that smart meters and grids in the E.U. can reduce the E.U.'s emissions by up to 9%, provide average energy savings of 3%, and generate total cost savings of €309 (roughly \$346) per electricity metering point, split amongst consumers, suppliers, and distributors.¹⁷ The California Public Utilities Commission has also recognized the benefits of smart meters.¹⁸
- **Agriculture** – IoT is particularly well suited to agricultural uses, allowing farmers to monitor equipment, precisely manage nutritional levels for crops and livestock, track tractors and other vehicles, monitor fuel consumption and efficiency, and assess the environmental impact of production.¹⁹

B. The Government Should Generally Rely on Existing Law in Regulating the IoT and Otherwise Act Very Cautiously to Regulate this Quickly-Evolving Industry.

In its Request for Comment, the NTIA asks how it should respond to potential consumer protection issues associated with IoT, including issues related to privacy and security.²⁰ Rather than enacting IoT-specific regulation, the government should generally rely on existing law to govern and regulate the IoT. Any concerns posed by IoT are not unique or specific to IoT. Rather, they are consistent with traditional concerns relating to data privacy, security, and other consumer-protection issues that are implicated by other services.

1. The Government Should Generally Refrain From IoT-Specific Regulation At Least Until There's A Demonstrable Need for a Particular Regulation Specific to IoT.²¹

The IoT is a fast moving market—its growth and evolution militate toward a wait-and-see approach. Indeed, Ambassador to the E.U. Anthony Gardner stated that, "We should be cautious about regulating on the basis of speculative concerns, rather than known, demonstrated risks."²² In such a market, the best approach is

¹⁵ <https://ec.europa.eu/digital-single-market/en/ecall-time-saved-lives-saved>

¹⁶ <https://ec.europa.eu/digital-single-market/news/ecall-all-new-cars-april-2018>

¹⁷ <http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>

¹⁸ <http://www.cpuc.ca.gov/General.aspx?id=4853>

¹⁹ GSMA Intelligence, *Agricultural Machine-to-Machine: A Platform for Expansion* (March 2015) (<https://www.gsmainelligence.com/research/?file=9186f77efc0a47fe7f127d79d789c64c&download>)

²⁰ See Request for Comment, Questions 16-18.

²¹ Generally responsive to NTIA's Request for Comment, Question 3b.

²² The Internet of Things: A Transatlantic Bridge to the Future", remarks at the 7th Annual Internet of Things European Summit by U.S. Ambassador Anthony L. Gardner (May 18, 2016) (<http://useu.usmission.gov/sp-051816.html>).

to rely on existing regulation – as opposed to new regulation designed with IoT or even a segment of IoT in mind. In actuality, the FTC has already shown that it can successfully enforce the FTC Act in this area.²³

Because of the nature of IoT, new proposed regulations, such as the "SPY Car Act", provide a telling example of the peril of unintended consequences when the government seeks to regulate IoT on an IoT-specific basis. More particularly, on July 21, 2015, new legislation was proposed directing the National Highway Traffic Safety Administration ("NHTSA") and the Federal Trade Commission to promulgate federal regulations setting minimum cybersecurity and privacy standards for all motor vehicles manufactured for sale in the United States, the so-called Security and Privacy in Your Car Act, abbreviated as the "SPY Car Act".

The SPY Car Act potentially impacts existing automotive safety requirements enforced by regulation and common law and gives regulators nearly unlimited power by requiring "best" security practices and "reasonable" measures to protect against cyber attacks but leaving the NHTSA and FTC with significant – and poorly defined – discretion to define reasonable measures and best practices, leaving both industry and consumers uncertain as to what is required and what may reasonably be expected.²⁴ Further, it disregards significant industry investment to address privacy and security concerns raised in a connected-car context.²⁵ More to the point, the SPY Car Act is unnecessary because existing provisions of the FTC Act have already been relied upon and are effective.

2. In Particular, With Respect to the Issues of Privacy, Security, Liability, and Net Neutrality, Existing Law Should be Applied.²⁶

Industry plays an important role in addressing potential concerns in the IoT arena as demonstrated by the policy recommendations of the European Union's Alliance for Internet of Things Innovation ("AIOTI")

²³ See <https://www.ftc.gov/news-events/blogs/business-blog/2016/02/asus-case-suggests-6-things-watch-internet-things>.

²⁴ For a helpful summary of the proposed legislation and the concerns it raises, see http://www.hoganlovells.es/files/Publication/fcda1298-7ad0-410d-922c-5c26ebad3446/Presentation/PublicationAttachment/fa284343-dba3-432e-a889-6da83a6e0cec/Automotive_News_August_2015.pdf.

²⁵ See Letter to the Federal Trade Commission from Participating Members of the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers dated November 12, 2014 (<http://www.autoalliance.org/auto-issues/automotive-privacy/letter-to-the-ftc>).

²⁶ This section of Vodafone's comments is generally responsive to NTIA's Request for Comment, Questions 16-17.

(chaired by Vodafone). Given the cross-cutting of IoT as it relates to privacy, security, liability and net neutrality, the AIOTI endorses a policy of applying existing law.²⁷ Similarly, the Body of European Regulators for Electronic Communications ("BEREC") recognizes that, in general, no special treatment for, or specific regulation of, IoT is necessary. BEREC also recognizes the use of extra-territorial and supra-national numbering for cellular IoT applications as well as the socio-economic benefits of so-called "permanent roaming" as an appropriate connectivity model. BEREC also found no need to deviate from the basic principles of data protection law in the IoT context, i.e., that there is no need for a special treatment of IoT services and privacy.²⁸ Vodafone agrees that no IoT-specific regulation is necessary absent a known, demonstrable risk.

3. The NTIA Should Adopt an International Policy Against Restrictions on Data Transfer, Use of Supra-National Numbering, or Other Restrictions That Would Prevent the Cross-Border Flow of IoT Devices or Data Associated with Those Devices.

In question 21 of its Request for Comment, the NTIA asks which issues it should focus on as part of its international engagement relevant to IoT. The NTIA also asks in question 24 what factors can impede the growth of the IoT outside the U. S. (e.g., data or service localization requirements or other barriers to trade). Given the global nature of IoT, Vodafone's view is that the NTIA should adopt a policy discouraging other agencies and governments from imposing undue restrictions on data transfers, requiring national numbers, or otherwise imposing restrictions on cross-border IoT activities. Governments should recognize that the IoT is inherently cross-border, both because of the frequent nature of the customer's needs (such as in international-supply-chain applications) and because for a provider to achieve economies of scale, the provider must employ a centralized platform. As such, it is crucial that there are no undue regulatory restrictions to cross-border storage and use of data associated with IoT applications. Vodafone supports efforts to remove (and certainly not implement) any barriers to the cross-border, free-flow of IoT data.

²⁷ See Alliance For Internet Of Things Innovation Alliance For Internet Of Things Innovation, Report of AIOTI Working Group 4 – Policy (October 15, 2015) attached **Annex D**.

²⁸ See http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

Customers also benefit from the economies of scale that allow them to purchase the same IoT solutions in multiple countries or to purchase the same solution when the contemplated use involves the IoT device traveling to more than one country. The free flow of data from country to country and the ability to purchase the same IoT solution for multiple countries also reinforces the need to permit permanent roaming as a global model for connectivity.

With respect to ownership of data, new IoT-specific regulations are unnecessary to determine which parties should have access to, or control of, data associated with IoT applications. Instead—just as in the case of privacy, security, liability, and net neutrality referenced above—we should rely on existing law, including private contractual negotiations, to address any data-ownership issues that arise. Further, the U.S. government should adopt an international policy to discourage other governments from adopting new regulations or applying existing regulations to IoT in a manner that would inhibit the flow of IoT-related data.

In addition to preventing or eliminating barriers to the cross-border flow of IoT-related data, a supportive regulatory approach to the use of numbering resources is required to support continued development of IoT. In Vodafone's case this involves use of ITU supranational numbers that have been specifically allocated to Vodafone for M2M and IoT applications.

The NTIA also asks in question 3 of its Request for Comment for examples of laws, regulations, or policies that unnecessarily inhibit IoT development and deployment. An instance in which a foreign government imposed restrictions on numbering and roaming that has had significant negative effects and has otherwise impeded the growth of IoT outside of the U.S. can be seen in Brazil. There, the Brazilian regulator, Agência Nacional de Telecomunicações ("ANATEL"), has expressed its understanding that international roaming must be necessarily temporary in nature. Brazil's *de facto* prohibition against permanent-roaming SIMs, does, in Vodafone's view, unnecessarily inhibit IoT development and deployment.²⁹ To comply with this interpretation of Brazilian law, Vodafone developed and deployed a "local solution" that provides connectivity

²⁹ Although there is no specific resolution on this matter, ANATEL has made its view of Brazilian law on this issue clear.

using a Brazilian number in partnership with a Brazilian carrier.³⁰ The KPMG Report (**Annex C**) also identified a number of direct impacts to Vodafone created by the prohibition on permanent roaming. These include:

- approximately 2.5 years of lost M2M revenues while the local solution was developed;
- additional costs associated with the development of the bespoke local M2M solution in conjunction with the local partner, including significant capital expenditures;
- significant added complexity and time delays to develop, test, and deploy the solution; and
- higher operating costs on an ongoing basis.

In addition to costs to Vodafone, KPMG identified that the prohibition on permanent roaming also affects enterprise customers in the form of:

- lost revenues associated with their use of M2M connectivity in their products for the Brazilian market over the period of delay in deployment;
- additional costs and complexities associated with being required to use two SIMs in their devices (the Global SIM outside of Brazil and a local SIM in Brazil), including supply chain production costs, monitoring and testing costs; and
- loss of the service benefits associated with use of Vodafone's global M2M platform.³¹

Given the significant costs to customers and providers of IoT, the NTIA should actively discourage any attempts—both inside and outside the U.S.—to impose number restrictions or restrictions on roaming.

Finally, to illustrate where other concerns on cross-border restrictions have been identified in other parts of the world, Vodafone refers the NTIA to Section 4 of the KPMG Report attached at **Annex C**, which contains a number of other case studies.

C. The U.S. Government Should Collaborate with other Governments Along With Industry and Standards Bodies on Policy Affecting IoT.³²

Given the global nature of IoT, it is vital to maintain an effective policy dialogue between governments, industry, and the relevant institutions that are also active in this area (e.g. standards bodies). In particular, collaboration should occur in the areas of interoperability and 5G networks.

Vodafone supports the use of existing licensed bands for the development of Narrowband-IoT technology to support IoT applications. Beyond that, a policy framework that supports the development of 5G will provide a vital opportunity to unlock IoT opportunities. Licensed spectrum is necessary to ensure

³⁰ See **Annex C** (KPMG Report), Brazilian Case Study at 30.

³¹ *Id.*

³² Generally responsive to NTIA's Request for Comment, Question 23.

performance and reliability over the lifetime of IoT devices and avoids disruption to the signal from other technologies attempting to use the same frequencies, which would be prevalent if unlicensed spectrum were used. High reliability, low latency, and freedom from interference are critical for many IoT applications, such as connected automobiles, medical applications, and industrial automation. An appropriate future-proofed network for IoT will require: significantly-reduced latency; ultra-fast download and upload speeds; improved spectral efficiency and reliability; high energy efficiency, and the ability to accommodate an exponential increase in the number of devices that simultaneously connect to the network.

One estimate finds that an additional 25 billion "things" will be connected to the Internet between 2015 and 2020.³³ The surest and best way to minimize IoT disruptions is for governments, standards bodies, and industry to quickly collaborate on a 5G network that will accommodate the exponential growth of IoT.

Beyond facilitating the use of spectrum that will ensure the full potential of IoT, the U.S. Government should collaborate with other governments, industry, and standards bodies to encourage interoperability and harmonization. Standardization and interoperability are essential to facilitate the full socio-economic benefits associated with M2M and IoT data. Industry collaboration with international standardization bodies, partners, and governmental authorities to define industry standards and best practice for data interoperability will be a positive development for the future of IoT. In particular, to achieve interoperability and thereby open the global market, there must be a standard and open means to discover IoT devices, to learn and interpret their data, and to interact with them (e.g., retrieve data or initiate commands). As with any communication network, interoperability between elements of an IoT network is particularly important for a successful deployment of the technology, with standards playing an important role.

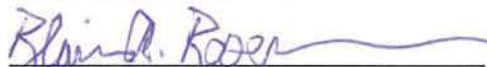
³³ **Annex C** (KPMG Report citing Cisco, taken from <http://www.cisco.com/web/solutions/trends/iot/portfolio.html>).

III. CONCLUSION

The U.S. Government is at a pivotal policy moment where it can incent or inhibit the further development of IoT in order to realize the health, safety and other socio-economic benefits IoT provides. The NTIA should refrain from imposing IoT-specific regulation unless and until there is demonstrable need. Instead, the NTIA should allow existing law and industry standards to support the development of a robust policy framework that simultaneously delivers on IoT benefits while driving appropriate industry behavior. Beyond that, the government should collaborate with other governments, industry, and standards bodies to facilitate the growth of IoT, including by removing barriers to the cross-border flow of IoT devices and data stemming from those devices and promoting a 5G network that can help IoT fulfill its potential.

Respectfully submitted,

VODAFONE US INC.



By: Megan Doberneck

Blair A. Rosenthal

999 18th Street, South Tower #1750

Denver, Colorado 80202

+1-720-484-0554

ANNEX A

Vodafone Internet of Things Enabling the IoT

Matt Key
March 15th 2016





Vodafone Internet of Things

24% revenue
growth YoY

**Global M2M
Platform with
35.5m
Connections**

84 million Mb
of data supplied
each month

**1400 M2M
professionals**

Vodafone Automotive
687 000
telematics subscribers

Rated as the best by
independent
analyst reports



**Machina
Research**

Gartner.

**analysys
mason**





The Future of Things is Connected

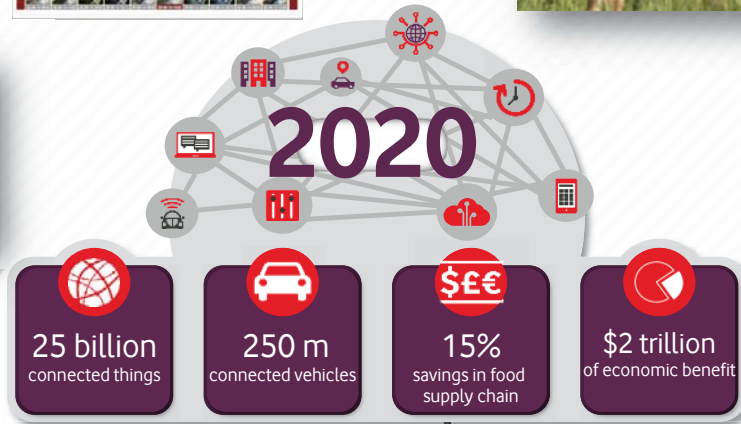
Flood Prevention:
Environment Agency



Connecting Cows
when calving: Mocoal



Machine Tracking:
Kärcher



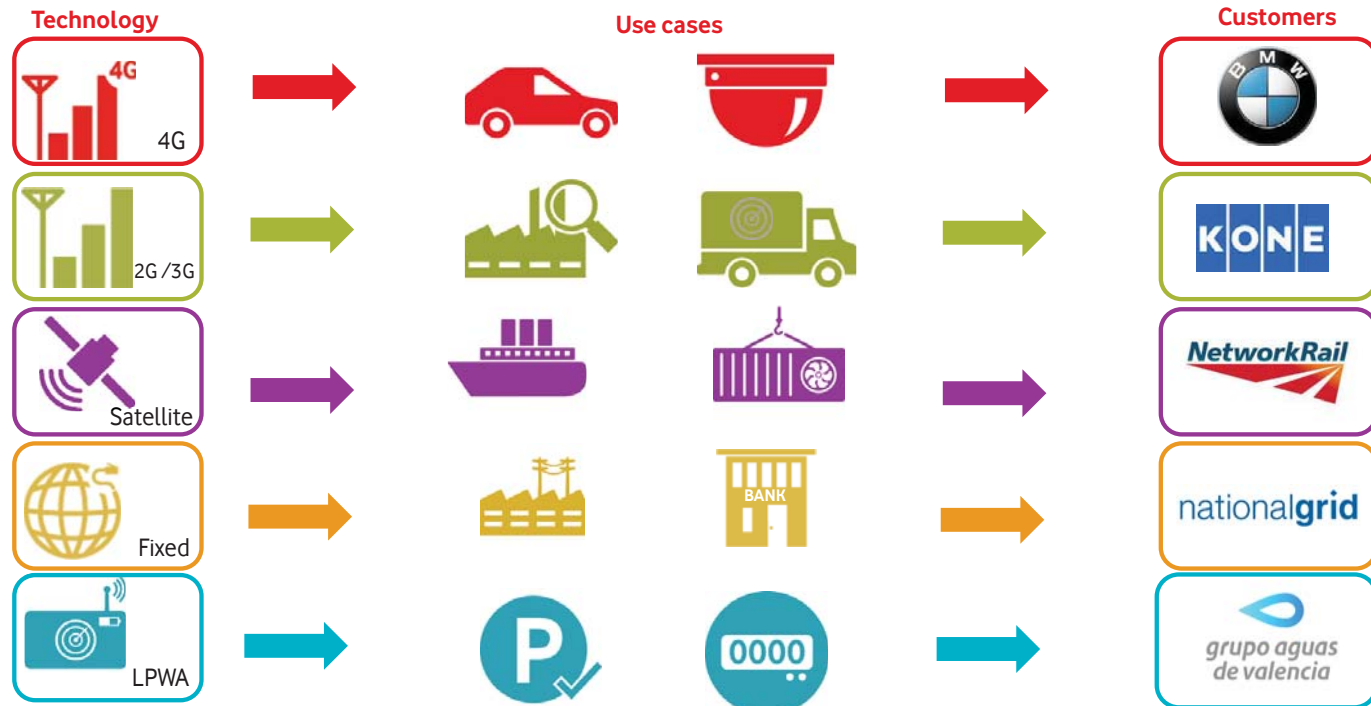
grupo aguas
de valencia

Connecting underground
water meters:
Aguas de Valencia



ANNEX A

Today's cellular technologies only partially address some verticals





What is LPWAN & NB-IoT?

LPWAN

Low-power WAN (LPWAN) is a wireless wide area network technology that is specialized for interconnecting devices with low-bandwidth connectivity, focusing on range and power efficiency.

Narrow-Band IOT (NB-IOT) is a technology being standardized by the 3GPP standards body. This technology is a **narrowband** radio technology specially designed for the **Internet of Things (IoT)**, hence its name.

NB-IoT



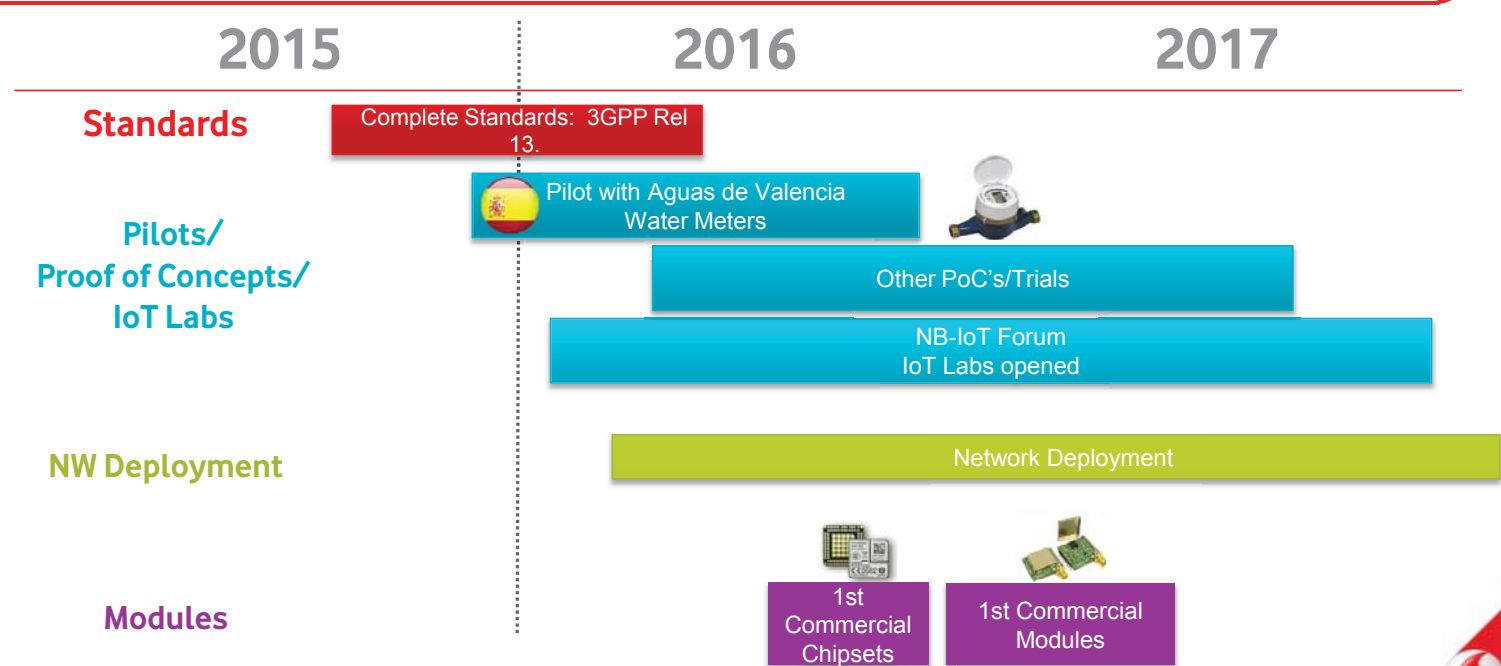
Low Power Wide Area (LPWA) networks aim to address some critical requirements for growth into IoT

Battery Life	>10 years	Many opportunities (e.g. smart meters) demand substantial battery life
Extended Penetration	+20dB link budget over GSM	A number of applications need deep in-building or underground coverage
Scalability	Up to 100k devices per cell	Once we embed M2M modules in 'every' device – we need a system that can handle billions of connected devices
Cost	<\$2 per module*	The lower the cost of the module, the greater the opportunities that are presented
Cost & Time to Deploy	Mix of HW & SW Updates	Allows us to leverage our existing network assets, accelerate rollout, and reduce costs

*Based on combination of analyst assumptions. Expected to decrease as scale increases.



We are executing our first pilots in NB-IoT



Future applications are different



Uplink is a new downlink

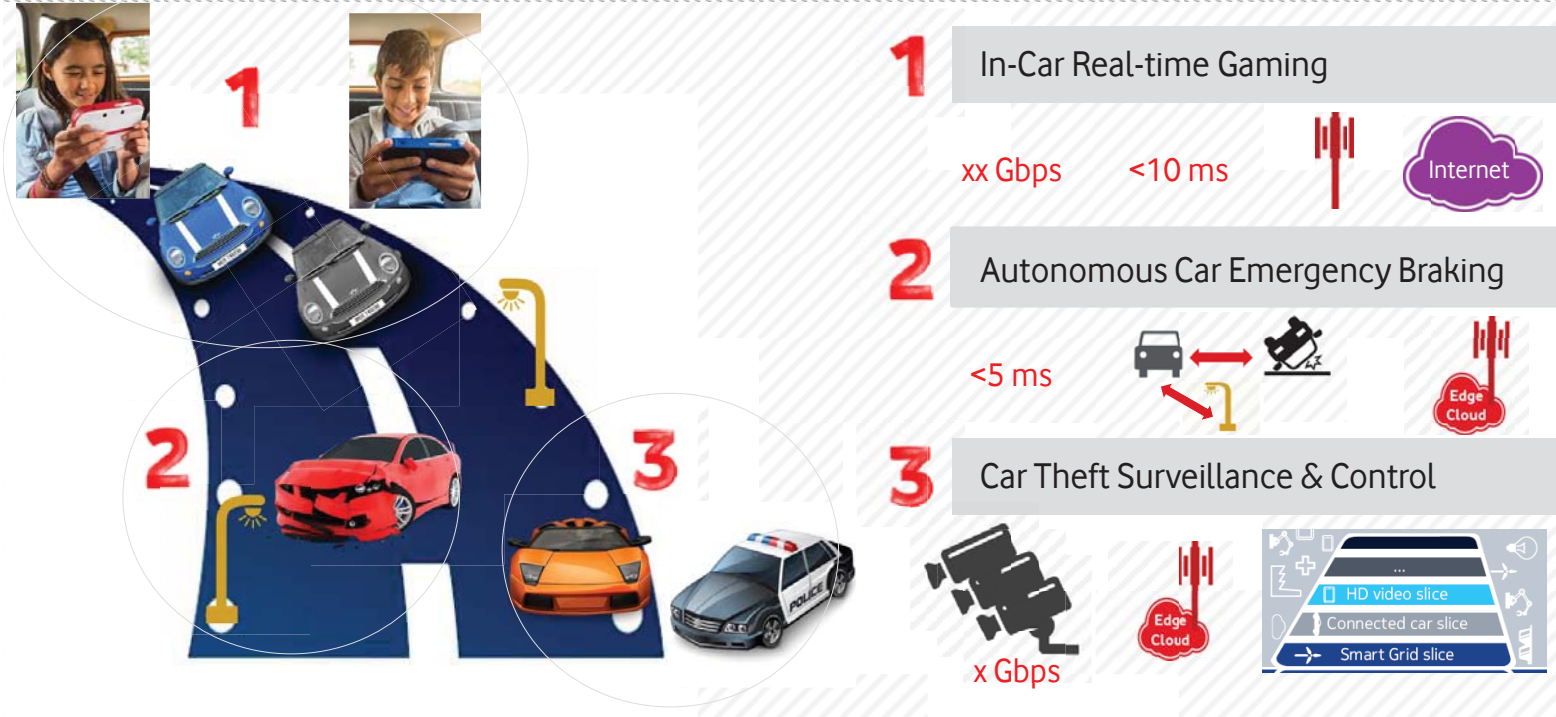
Universal network coverage

More than peer to peer

Smartness is pervasive and long-lived

5G is a mind shift!

5G Brings to Life Future of Automotive



Vodafone's vision for the Gigabit Society

**Widespread connectivity of 1 Gigabit per second by 2030
provided by robust, reliable, future proof technologies**



Competitiveness	Local development	5G	Citizens	Public services
<ul style="list-style-type: none">• Digitalisation of industries• Connected cars• Cloud based services• SMEs	<ul style="list-style-type: none">• Attractiveness of regions• Increase in fibre penetration linked to higher employment• Smart cities	<ul style="list-style-type: none">• Full potential of 5G needs fibre backhaul	<ul style="list-style-type: none">• New ultra high definition video standard 4K, 8K• VR / AR	<ul style="list-style-type: none">• More efficient and cost effective public services• e-health, e-education

Connectivity as an enabler , not a constraint



ANNEX A

Thank you

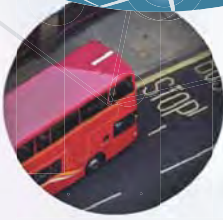
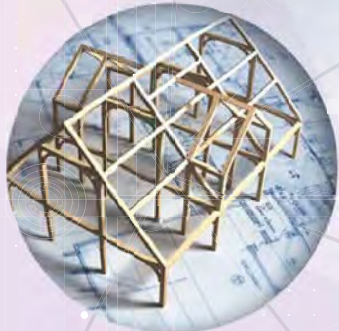


Vodafone M2M Barometer 2015

Detailed insight into how Machine-to-Machine communications and the Internet of Things are driving business transformation around the world

m2m.vodafone.com

Vodafone
Power to you



Foreword:

Taking the pulse of the connected world



Erik Brenneis

Director, Machine-to-Machine,
Vodafone

This is the third edition of Vodafone's annual M2M Barometer. Since we first set out to survey the market, it has changed dramatically. Machine-to-Machine (M2M) communications is no longer a niche technical term; it's a driving force for innovation in our cities, homes, cars and workplaces, and its potential is being recognised by business leaders in every industry.

We created the Barometer to track how businesses were adopting this emerging technology: which regions and industries were pulling ahead, and how fast the market was growing.

But more and more businesses have turned to M2M and the Internet of Things (IoT) to help them achieve their goals, both as part of strategic M2M projects and as an integral part of the products and services they buy. As a result we are seeing more evidence of how M2M is transforming lives and business.

To reflect this growing maturity, the Barometer has evolved. We still report the level of adoption, but instead of just looking at what kinds of business are using M2M, we're investigating which businesses are using it effectively — and which approaches to M2M produce the strongest impact for them.

To answer these questions we have again conducted in-depth interviews around the world with more than 650 business and IT executives. This year we have supported our research with insights from leading M2M analyst company Analysys Mason.

Whether your business has been working with M2M for years or is engaged in pilots for the first time, we hope you find the Barometer valuable. We'd be interested to hear your comments. You can contact me and my team at m2m@vodafone.com.

Yours,

A handwritten signature in black ink, appearing to read 'Erik Brenneis', written in a cursive style.

Erik Brenneis

Director, Machine-to-Machine, Vodafone

Contents

	Executive summary	2
1	Awareness of M2M is high, and growing	5
	M2M goes by many names.....	5
	Our definition of M2M.....	6
	M2M matters.....	6
2	M2M adoption continues to grow	7
	More than a quarter of businesses have adopted M2M.....	7
	There are different kinds of adoption.....	8
	Smaller organisations use M2M too.....	9
	Industry rankings have changed since last year.....	9
	AMEAP leads adoption, Europe shows fastest growth.....	13
3	Companies are evolving how they use M2M	14
	Adopters are increasing the scale of their M2M projects.....	14
	The sophistication of applications is also growing.....	15
	Transformation is as important as optimisation.....	16
	Mission-critical M2M needs the right connectivity.....	17
	M2M pioneers tend to be technology pioneers.....	18
4	M2M delivers value, and does it quickly	19
	Adopters see clear, significant ROI.....	19
	Organisations report significant cost savings.....	19
	Return on investment takes many forms.....	20
5	More sophisticated use of M2M leads to greater benefits	21
	There's a clear link between sophistication and impact.....	21
	Larger organisations are ahead in M2M sophistication.....	22
	M2M sophistication and Business Readiness are linked.....	22
	A clear strategy is essential.....	23
6	Few barriers stand in the way of M2M adoption	24
	Security and privacy are the most common obstacles.....	24
	Organisations are concerned about security breaches.....	25
	IT leaders are more concerned about security.....	25
	Despite the concerns, most say their IT is secure.....	26
	Providers can help businesses to address security.....	26
7	M2M involves the whole business	27
	The business sees M2M as supporting innovation.....	27
	All roles are committed to business transformation.....	28
	The CIO leads, but many other roles are involved.....	28
	Less than half of M2M projects come out of the IT budget.....	29
	External providers play an important role.....	29
	Conclusion	30
	Further reading	31
	About Vodafone / About our contributors	32

Executive summary

Our research proves that not only are organisations continuing to adopt M2M and extend it throughout their business — they're seeing powerful and measurable results. Here are our key findings, by the numbers.

M2M is a top priority for businesses

Compared to last year, more businesses have heard of M2M, more say that it's relevant to them, and more have an M2M project in place.

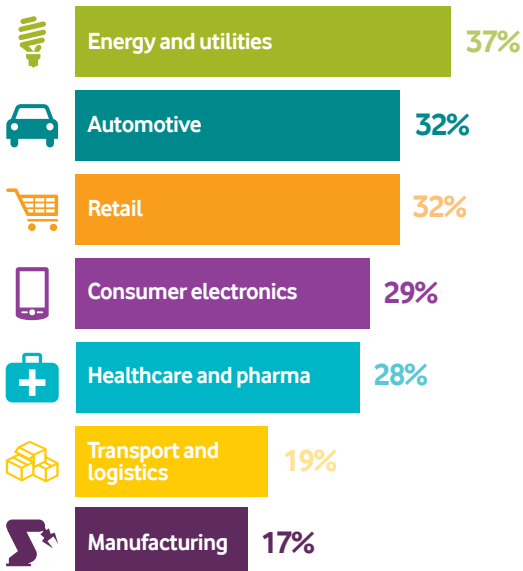
- 76% have heard of M2M, up from 61% in 2014.
- 90% say M2M is relevant to their organisation today, up from 86% in 2014.
- 27% have an M2M project in place, up from 22% in 2014. A further 37% say they have projects ready to go live within the next two years.
- Energy and utilities, automotive and retail lead adoption — as the chart below shows.

The use of M2M is evolving in many ways

Once organisations start using M2M, they evolve and expand how they use it, to support ongoing strategic business transformation.

- 81% of those that were using M2M in 2014 say they have increased their use of it since, and in many different ways — see the chart below.
- Businesses are using it in more advanced ways: 81% of adopters are using analytics on the M2M data they gather, up from 75% in 2014.
- 50% of M2M adopters say they're using it to enable new business and operating models.

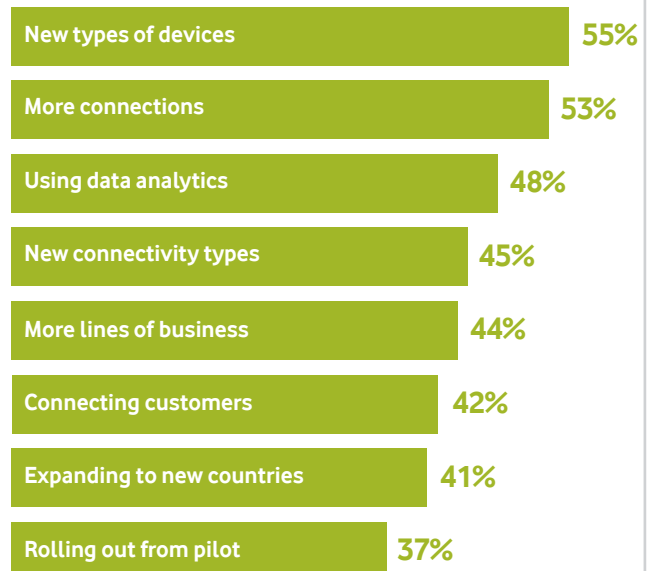
M2M adoption by industry, 2015



Which industries are leading #M2M adoption? Find out in the Vodafone M2M Barometer.



Companies' M2M use is growing in many ways



Adopting #M2M is just the first step. Find out what companies do next in the Vodafone M2M Barometer.



See **Section 2** (page 7) to find out more about how businesses are adopting M2M.



See **Section 3** (page 14) to find out more about how adopters are using M2M within their organisations.



M2M delivers significant ROI, usually within 12 months

A large majority of organisations are reporting strong and transformative returns on their investment (ROI) in M2M initiatives.

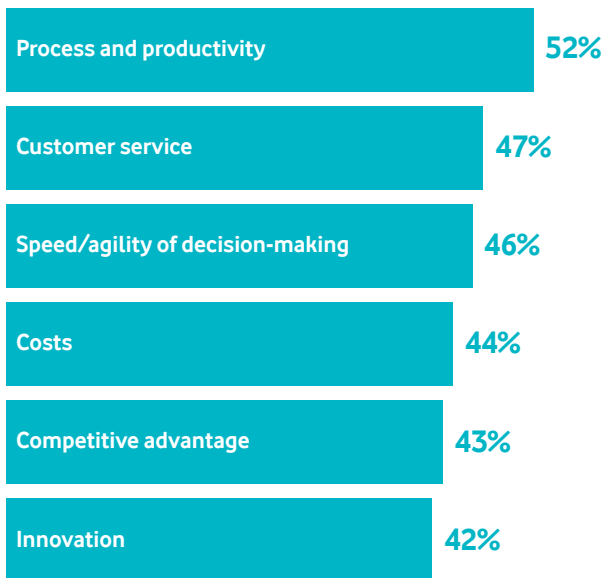
- 83% of adopters agree that they have gained competitive advantage from M2M; 38% agree “strongly”.
- 59% of those using M2M say they’ve seen “significant” ROI, up from 46% last year.
- 54% of M2M adopters reported ROI within 12 months.
- Nearly 10% of M2M adopters have reduced their costs by over 25%. The average cost saving is 18%.
- Companies report a range of benefits from M2M — including those shown in the chart below.

M2M projects involve the whole business

As M2M gains a higher profile and expands across business processes, its ownership and position within the organisation is likely to change.

- 79% agree that M2M is not about buying technology, but about improving business processes.
- The CIO leads projects in 36% of cases; the CEO leads in 16%. 63% report having multiple leaders involved.
- Only 46% of projects get charged to the IT budget. 28% of businesses already use risk/reward sharing models, and 29% charge the cost direct to the consumer — as shown in the chart below.

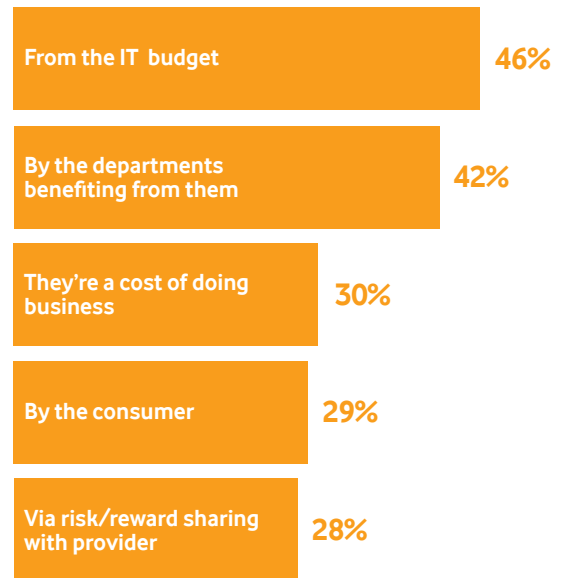
Where have you seen benefits from M2M?



Organisations are seeing a range of benefits from #M2M. Find out more in the Vodafone M2M Barometer.



How are M2M projects funded?



Companies are experimenting with #M2M business models. Find out more in the Vodafone M2M Barometer.



To find out more about the results businesses are seeing from M2M, see **Section 4** (page 19).



To find out more about the role of M2M projects within the organisation, see **Section 7** (page 27).



The M2M Barometer is based on robust global research

We commissioned Circle Research, an independent market research firm, to interview businesses representing multiple sizes, industries and regions.

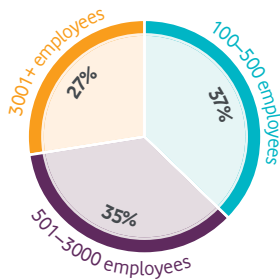


Figure 1a: Respondents by company size

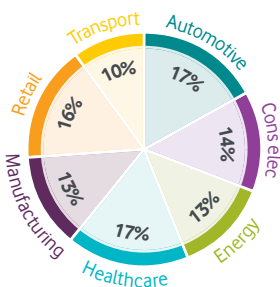


Figure 1b: Respondents by industry

The Barometer has always been a global study of the views of business and IT leaders. As per last year, interviews were spread across seven of the major M2M-using industries. This year we expanded our reach by:

- Increasing the number of countries covered from 14 to 16. The countries represented are the US, Brazil, Germany, Italy, the Netherlands, Spain, the UK, Turkey, Australia, India, Japan, South Korea, China, South Africa, and, new for this year, Canada and New Zealand.
- Adding small to medium enterprises (SMEs). This year respondents come from companies with as few as 100 employees to more than 100,000; and include national, regional and global businesses.
- Increasing the number of interviews by 80%, to a total of 659.

The respondents represented IT, R&D, finance, strategy and planning functions. They ranged from senior management to board-level and were qualified as M2M decision-makers for their organisation.

The online interviews were conducted in March and April 2015, and were supported by in-depth qualitative discussions. We have drawn the quotations included in this report from these in-depth interviews. We have also included commentary from the M2M practice of respected consulting and research company, Analysys Mason.

All interviews	277	234	259
Qualifying interviews	207 (75%)	224 (96%)	228 (88%)



Figure 1c: We surveyed businesses from all around the world

Awareness of M2M is high, and growing

Section

1

Most businesses say they are familiar with the term “M2M”, reflecting the fact that the technology is moving into the mainstream.

M2M goes by many names

M2M has always been known by many labels. Some of these relate to specific applications, with names and prefixes such as “smart” and “connected”, as in smart metering or connected car. Others, such as “Internet of Things” (IoT) apply to a much broader (and often contested) space.

This variety of terminology is not holding back awareness. We asked about the most common terms, and found that most people have heard of both M2M and its alternatives, particularly IoT (see Figure 2). These numbers are significantly higher than we found last year — which, given the publicity around M2M and IoT in the business and consumer press, is understandable.

Businesses that have heard of M2M, 2014/2015

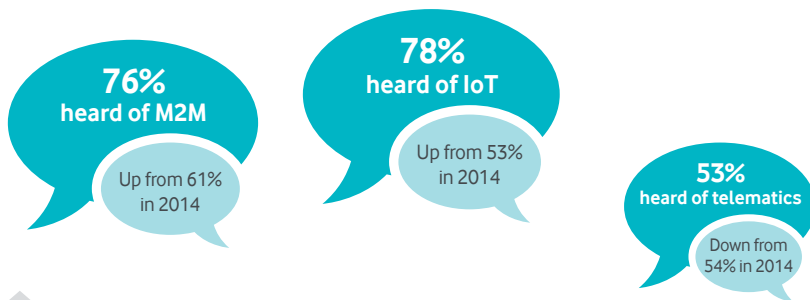


Figure 2: Recognition of IoT has quickly surpassed that of M2M and telematics

“IoT” seems to be becoming the term of choice, and as well as it seeing the greatest growth in awareness across our sample, we found it to be even more dominant in the answers given by smaller organisations and by those who haven’t yet adopted M2M. This perhaps reflects how IoT is being associated in the media with consumer applications, while M2M has a legacy of being linked with industrial and corporate applications.

Industry 4.0: M2M’s industrial resurgence?

While the term “IoT” increasingly shows a pronounced consumer angle, M2M’s heritage is in industrial sectors. Through sensors and communications, manufacturers have automated and streamlined their factory floors and their supply chains for decades.

Now, the industrial aspect of M2M is seeing resurgence. The German government coined the term “Industry 4.0” in 2011. The term refers to a fourth industrial revolution, built on smart factories, which now forms part of the country’s high-tech strategy. Industry 4.0 includes many different technologies, from cloud and big data to collaboration solutions — in fact, the Boston Consulting Group describes “nine pillars” for Industry 4.0.¹ However, M2M forms a key part of it. Since then, others too have reasserted the industrial role of M2M. GE coined the term “the Industrial Internet”, and Accenture talks of the “Industrial Internet of Things” (IIoT).

Our definition of M2M

In our survey, after asking about awareness of the various terms, we defined M2M to ensure that we can fairly compare the answers given during the survey.

Definition:

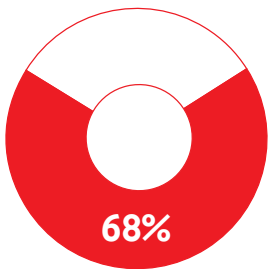
M2M connects machines, devices and objects to the internet, turning them into ‘intelligent’ assets that can communicate. M2M enables the Internet of Things.

It's clear that there is significant overlap between M2M and IoT, and for many purposes it's possible to use the terms interchangeably without real confusion — nobody disputes that both terms are about connecting objects in the world to share data and communicate. But we see a qualitative difference between M2M and IoT.

M2M is primarily about remotely connecting an organisation's assets and machines; IoT is about all types of assets, machines and 'things' becoming connected together, to benefit a broader range of parties.

As M2M evolves into IoT, we see increasing:

- **Connectivity:** Organisations will use a wider range of network types to connect a wider range of “smart” assets and products. Highly customised solutions will be complemented by more standardised and off-the-shelf solutions that function at scale.
- **Data gathering:** More data will be gathered for analysis, and it will be shared beyond functional silos, and beyond the organisation's four walls.
- **Sharing:** Projects will not just deliver value within departments, but span whole ecosystems of companies across multiple industries and multiple regions. Solutions will be delivered direct to consumers, not just corporates — for instance, wearables.



68% of businesses say that M2M adoption has reached a tipping point.

M2M matters

We found that most businesses think they know what M2M is... but do they care about it? The answer is a resounding “yes”.

We asked whether M2M products and services are relevant to their organisation today: 90% agreed, up from 86% in last year's survey.

The analyst view: M2M vs IoT

“M2M and IoT continue to be used interchangeably on both the demand and supply side of the industry. M2M typically refers to the connectivity that enables two or more machines or things to communicate with each other.

The IoT industry is nascent and its boundaries and structures are still evolving – and, as a result, so is its definition. IoT is often closely associated with the consumer market and consumer devices, and IoT certainly takes into account the human interaction with the data generated by devices in a connected environment. However, IoT is just as relevant, if not more so, in the enterprise domain as it is in the consumer environment.”

M2M adoption continues to grow

The Barometer's mission has always been to report the impact that M2M is having on business — and the foundation for that is to measure how many businesses are actually using it.

More than a quarter of businesses have adopted M2M

Here's the headline: 27% of businesses say they have M2M projects in place today, up from 22% last year (see Figure 3). This is a significant year-on-year growth of 23%, which far outpaces both the growth rate of the IT market as a whole (which some reports suggest has declined year-on-year²), and of the global economy.³

A further 37% of organisations say they have their first M2M projects targeted to go live by 2017. While the nature of complex technology projects means this is unlikely to translate directly into adoption figures over the next two years, we still see a very healthy pipeline for growth.

Section

2

“M2M is now being considered as a key component in our wider strategy.”

Retailer, AMEAP

Adoption of M2M, 2013–2015

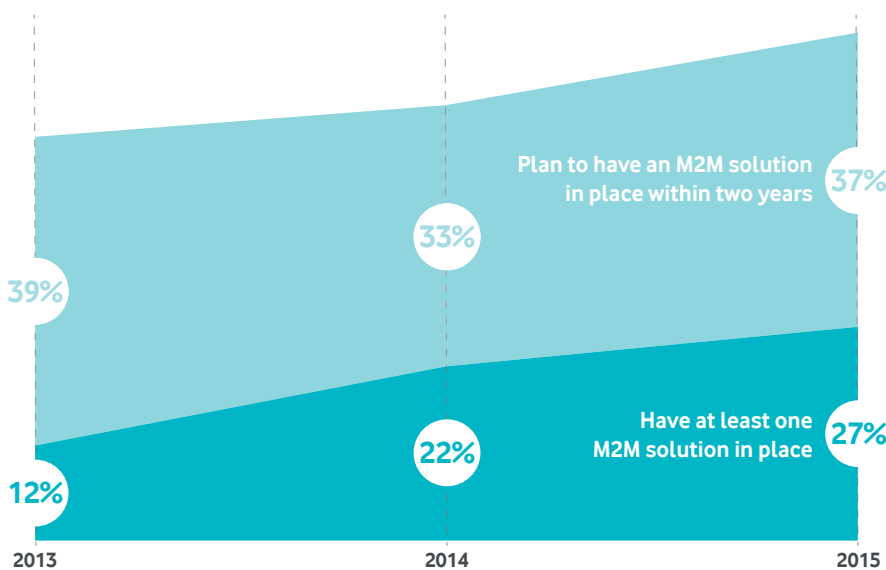


Figure 3: Current M2M adoption is 27%, with 37% more saying they'll adopt within two years

The analyst view: adoption is growing broader

“M2M adoption continues to grow at a significant pace. Awareness of the benefits of M2M has grown across various sectors since its inception over a decade ago, and segments such as smart metering and fleet management have been at the forefront of that growth. We are now entering a new era or phase of adoption in which M2M will be adopted in a broader range of industry verticals. This is partly driven by supply-side factors that have aligned to lower the barriers to entry.”



There are different kinds of adoption

Our headline adoption figure is based on business and IT leaders stating they “have already implemented M2M projects”. Those “M2M projects” — with defined goals, owners and budgets — are the ones we’re really interested in, because they reshape businesses and produce measured outcomes.

But in M2M, there is another kind of adoption that we need to recognise. Businesses may start using M2M outside of formal, strategic business projects: we call this “shadow” adoption.

Just like other “consumerised” technologies, such as mobile devices and cloud, many kinds of M2M are being brought into organisations by individual employees and as part of other activities, without a formal corporate mandate.

Shadow adoption in action

A healthcare organisation is adding new models to its fleet of company cars, as it does every year. The fleet manager doesn’t necessarily engage the IT department or treat the purchase as part of a formal, planned “M2M project” — which is how a new mHealth initiative at a corporate level would be approached. But the vehicles could be M2M-connected, with stolen vehicle recovery and usage-based insurance built in. And these features might actually have factored highly in the fleet manager’s purchase decision.

In both cases, the company is “using” M2M and probably seeing benefits from it, but there is a distinct difference in intent, approach, visibility, and the contribution that M2M makes to achieving defined business goals.

As M2M finds its way into more and more products and services that businesses and their employees buy every day, we’ll find this shadow adoption will continue to grow. Whether it complements or threatens planned initiatives from the CEO or CIO will depend more than anything on the organisation and its cultural attitude to innovation and integrating new technology.

The analyst view: how SMEs are using M2M

“SMEs adopt M2M for the same reasons as their larger competitors — to decrease costs, increase productivity and gain competitive advantage. Startups in some industries may structure their business processes to take advantage of connectivity from inception to gain a competitive advantage over larger, less agile firms. But other SMEs are not as technologically savvy, and may have neither an IT department nor the capability to take on significant ICT projects. Pre-configured off-the-shelf, plug-and-play solutions are opening up the capabilities of M2M to this kind of organisation.”

Smaller organisations use M2M too

It's easy to generalise about organisation size when it comes to technology adoption. Some argue that small organisations are agile, unencumbered by bureaucracy and legacy technology. Others say that because large organisations have more in-house IT expertise and capital, they are better able to innovate. This year we broadened our survey to include organisations as small as 100 employees so that we could investigate this issue.

While we found that larger organisations are more likely to be using M2M, the difference is not dramatic: around 24% of the smaller SMEs in our research (100–249 employees) use M2M, compared to 35% of organisations with over 50,000 employees.

M2M is enabling SMEs to compete with corporates

Technology has always helped break the link between employee headcount and the amount of work that a business can perform.

Now, thanks to cloud, some highly leveraged tech companies might serve millions of customers with a handful of employees. And M2M is having a similar effect: by automating processes using connected devices, businesses can make their employee headcount go much further. For example, car-sharing service DriveNow is an SME, yet it has more than 460,000 customers, making it the largest service of its kind in Germany. Find out more about DriveNow's use of M2M on page 10.

Industry rankings have changed since last year

This year most sectors have reached around 30% adoption — meaning a few of the laggards in last year's survey have caught up with the leaders (see Figure 4).

Adoption of M2M by industry, 2013–2015

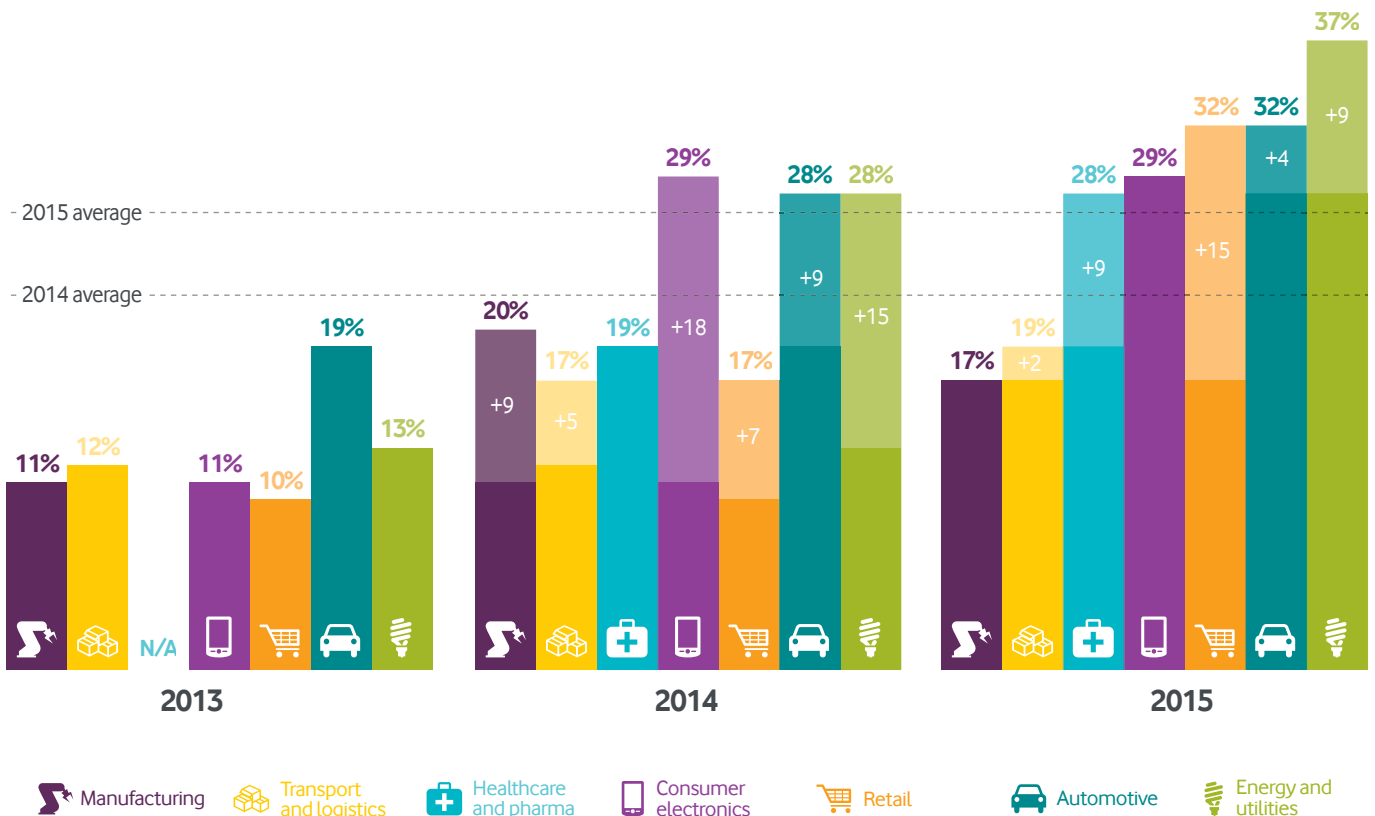
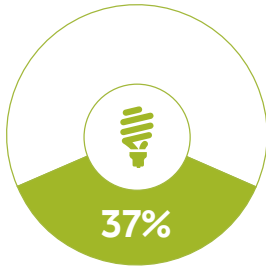


Figure 4: Adoption by industry 2013–2015 shows energy and utilities leading, closely followed by automotive and retail

Energy and utilities



Energy and utilities was already a strong performer last year, and it has pushed ahead to lead the field at 37% adoption. These are highly regulated sectors that operate largely independently of the broader economic climate, and much of their investment — for instance, in applications such as smart metering — is driven by long-running infrastructure modernisation initiatives and ambitious government targets. Analysys Mason forecasts 23% compound annual growth rate (CAGR) in number of global M2M connections through 2020, suggesting that this sector will maintain its momentum.



The analyst view

“Government regulation on smart energy metering in many countries has fuelled strong M2M adoption in this sector. This should continue for the foreseeable future although take-up may slow in countries where penetration of electric smart meters is already high (for example, Italy), and in others where stimulus plans have expired (for example, in the US).”



Automotive

Automotive was an early leader in M2M, and today remains one of the top sectors for adoption, at 32%. All the large consumer OEMs have a “connected car” strategy, and are pushing M2M technology as a way to improve driver services. Other organisations in the automotive sector, such as parts suppliers and the aftermarket, are increasingly looking at how M2M affects them.



The analyst view

“Automotive OEMs are fully aware of the benefits that M2M connectivity affords with regard to reducing their operating costs, such as those for maintenance and warranties; the advantages of operating a service model that sustains more intimate engagement with customers; and the benefits that connectivity provides to their customers to enhance their digital lifestyles. 89% of new cars sold worldwide will have some form of connectivity by 2024.”

Case study: DriveNow runs its business with M2M

DriveNow is Germany's biggest car-sharing organisation. It has over 460,000 customers in eight cities in Germany, Europe and the US. While it's a joint venture between two large businesses — BMW and car rental company Sixt — DriveNow is an SME, and a great example of how smaller companies are using M2M in sophisticated ways.

DriveNow has used M2M in its cars for three years. This enables it to track their locations and provide information services to drivers. Innovation is key, and DriveNow is always looking at how to enhance the customer experience. For example, it's looking at using analytics, and integrating its services with third parties, such as public transport providers, to give customers a joined-up transportation experience.

M2M is core to DriveNow's 24/7 operations, and reliable connectivity is critical. But as it plans more complex services — like streaming audio and video to its cars — high-speed connectivity is becoming more of a factor. It's looking at using 4G in the future.

“When customers rely on you 24/7 you must provide a stable service, and M2M enables us to do that.”

Retail

Retail showed the biggest increase in adoption from 2014 from 17% to 32%. Retailers are enthusiastically adopting solutions like asset tracking to streamline the supply chain, digital signage for interacting with customers, and energy data management for reducing their facilities costs. In research we conducted with European SME retailers in March 2015, 97% said that smart energy solutions would be valuable to their business. A clear majority also said that asset tracking, smart vending machines, smart payment and digital advertising would be valuable.



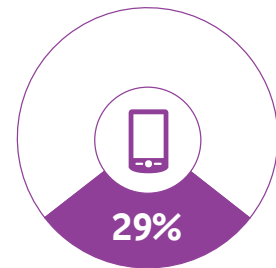
The analyst view

“Retailers are gaining awareness of the potential benefits that connected services can bring to their businesses. Benefits include strengthening the relationship with their customers through personalisation of the shopping experience as well as streamlining retailers’ own internal operations. The data illustrates that adoption in the retail sector has increased significantly from a smaller base than some of the other sectors.”



Consumer electronics

Consumer electronics saw little change in terms of the number of companies adopting M2M this year, as a result of the slowing economy in some regions,⁴ and adoption stands at 29%. But those consumer electronics companies that have started using M2M are committed to expanding it across their product ranges aggressively: Samsung has announced that every single one of the products it sells will be connected within five years.⁵ IoT has also become a prominent theme at industry events such as CES.⁶



The analyst view

“Adoption of M2M in the consumer electronics industry has been slower than anticipated. Replacement cycles are slow and coupled with the issues around fragmented standards, this has undoubtedly led to slowing adoption. Enterprises in the market are waiting to see which standards dominate. In addition, use cases are sometimes poorly defined and consumers are not clear on the benefits.”



Healthcare and pharmaceuticals

Healthcare showed a significant growth from a relatively low base, from 19% to 28%, perhaps revealing that M2M has finally passed through the more measured product development cycles and greater regulatory burden that this sector faces. M2M offers significant potential for cost savings and reduced risk everywhere from front-line patient care to the pharmaceuticals supply chain, so we expect growth to continue. Analysys Mason forecasts 19% CAGR in M2M connections through 2020.

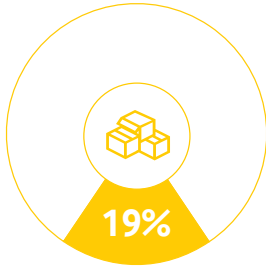


The analyst view

“Long lead time required for medical device safety and performance certification, coupled with data protection regulation, has subdued development of M2M solutions for the healthcare sector in recent years but solutions are now coming to market. Increasing pressure on healthcare systems and rising awareness of the benefits of M2M has renewed interest in the adoption of innovative connected solutions.”



Transportation and logistics



This sector saw only modest growth and reported adoption stands at 19%.

Transport companies often adopt M2M when they replace a vehicle or other asset, and many have chosen to delay their refresh cycles and sweat their assets for longer. This is partly due to declining fuel prices, which have taken the pressure off companies to switch to the latest energy-efficient vehicles. And it's also taken away the urgency to adopt other efficiency-boosting measures, such as M2M fleet-management solutions.

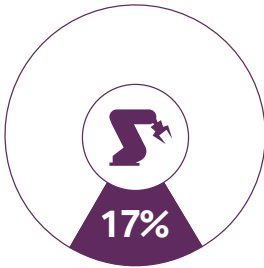
More broadly, transport CEOs report a cautious attitude to economic performance,⁷ and consequent budget constraints, which will have an effect on IT investments.

The analyst view



“Fleet management is probably the most mature M2M market segment. Nevertheless, Analysys Mason forecasts good growth of 10% CAGR over the next decade in this sector. The need to drive down costs and remain competitive is critical in a crowded market. With regard to logistics and asset tracking, M2M facilitates new functionality such as location tracking and monitoring the conditions of transit. It reduces the risk of loss, theft and wastage. This will drive M2M deployments in the next few years.”

Manufacturing



Manufacturing was an early adopter of connected technology, through factory and warehouse automation — and as we've seen, government initiatives often focus on promoting this sector. In addition to Germany's Industry 4.0, China has launched its “Made in China 2025” strategy.

However, in many countries this sector is suffering from economic conditions which may be constraining investment in technologies of all kinds. Research shows that manufacturing CEOs are more pessimistic about growth than other sectors.⁸ This explains why adoption stands at just 17%.

However, M2M has an extremely clear business case, and manufacturers are aware of its potential. In research with European SME manufacturers we conducted in March 2015, 94% said that smart energy solutions would be valuable to their business; 89% said that being able to use M2M to remotely manage their manufacturing equipment would be valuable to their business. 82% of manufacturing SMEs rated being able to track their moving assets as being valuable to their business. We believe that larger manufacturers hold similar attitudes.

Note:

Our adoption figure for manufacturing is actually lower than last year's, which is due to variations in our survey sample from 2014 to 2015. None of the manufacturing adopters we surveyed this year said they had stopped using M2M or were doing less M2M than the year before.

The analyst view



“The ‘smart factory’ opportunity may take longer to materialise in manufacturing compared to other sectors because of proprietary legacy equipment. Other M2M opportunities lie in the manufacture of connected products, which may require a shift to new service-based, rather than product-based, business models. This type of transformation will develop over the next few years.”

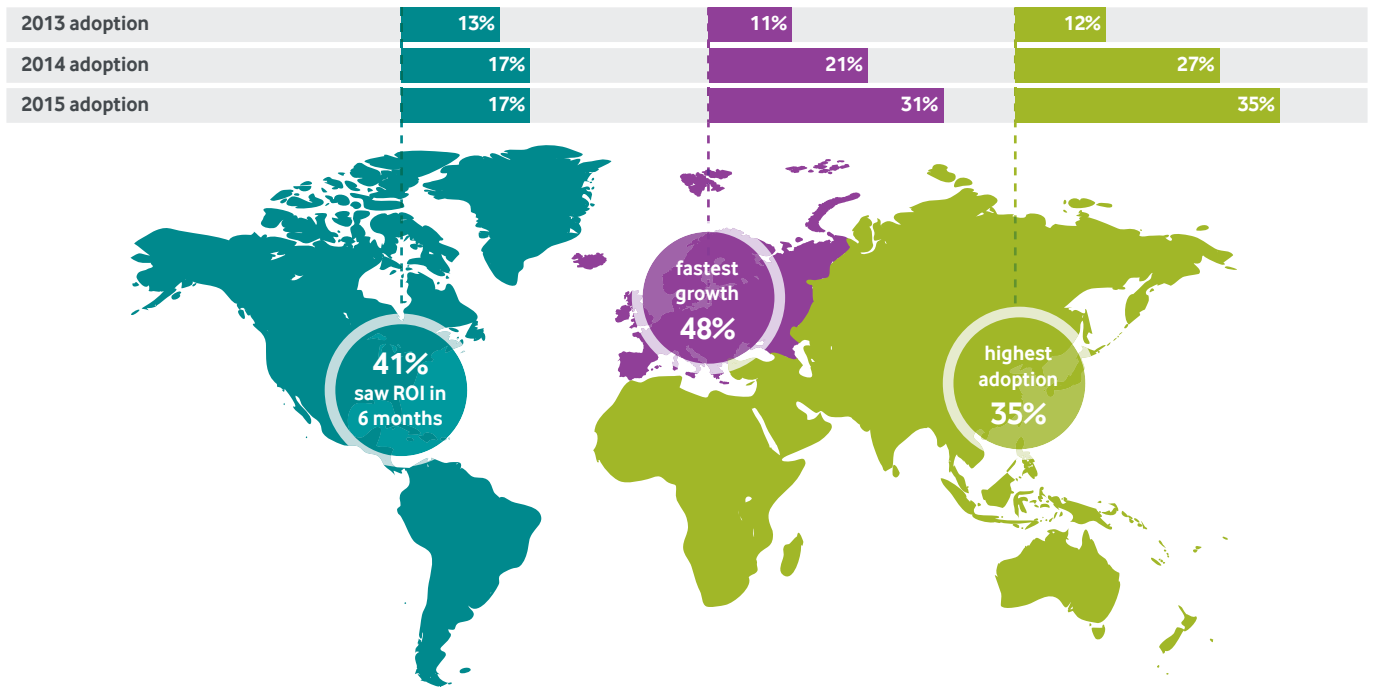


Figure 5: AMEAP has the highest adoption today, but adoption is growing fastest in Europe

AMEAP leads adoption, Europe shows fastest growth

At 35% adoption, Africa, Middle East and Asia/Pacific (AMEAP) is continuing to outperform other regions, led by confident growth in India and China and performance in sectors such as energy and utilities and retail (see Figure 5).

We knew that AMEAP would perform well, given the region's overall confidence, lack of regulatory hurdles, and lack of legacy infrastructure. Many AMEAP governments are also strongly pushing IoT as a matter of national policy, for instance in China and South Korea. Across developing markets in AMEAP, the rollout of foundational IT and communications infrastructure is proceeding extremely quickly.

Europe showed the strongest overall growth, from 21% to 31% adoption year-on-year. The strong German market is partly responsible, with its government push of Industry 4.0 and its advanced automotive sector. Across Europe generally we also saw strong performance from energy and utilities and retail.

The Americas — Brazil, the US and Canada — show little change in adoption, with growth being masked by the addition of Canada to our survey this year. Despite this, the Americas are ahead in adoption of connected consumer devices and smart homes and buildings, reflecting the groundswell of consumer interest in IoT. Also, more businesses in the Americas say they have seen ROI in the shortest time period – 41% within six months. As a result, the Americas represents one of the most sizeable growth opportunities: Analysys Mason forecasts that the number of M2M connections in the region will more than double between 2015 and 2020.

Other technologies show a similar adoption pattern

We asked respondents about their organisation's use of two other trending technologies, big data and cloud. A similar pattern emerged, with AMEAP ahead of Europe and the Americas. For example, 49% of AMEAP businesses that have a strategy for M2M have already adopted big data, compared to 35% in Europe and 29% in the Americas. We discuss this relationship further on page 18.

The analyst view: Americas

“Our research shows that the number of M2M cellular connections in the Americas has grown by about 30% year-on-year since 2011. Companies that have adopted M2M are expanding their installed base of devices and exploring new use cases for the technology. In the US, M2M deployment has been concentrated in the utilities and automotive verticals. However, growth in smart metering has slowed. Government stimulus programmes to fund energy grid upgrades have been exhausted and new funding mechanisms have been slow to materialise. M2M growth is now more concentrated in other sectors, such as retail, healthcare and manufacturing, but it will take time for momentum to build in these areas. Raising awareness and providing the market with demonstrable ROI proof points will be critical.”



Section

3

Companies are evolving how they use M2M

Once organisations start using M2M, they evolve and expand how they use it, to support ongoing business transformation.

Adopters are increasing the scale of their M2M projects

Of those adopters who were using M2M a year ago, 81% say they've increased their use of M2M since. None say they are using it less than they were. But what does "increasing use" mean? Are they just doing more of the same, or are they changing how they use M2M?

For many businesses, the answer is both (see Figure 6). They're increasing the size of their M2M initiative, by adding more M2M connections, expanding into new countries, and connecting new devices.

More than half of those that say they're increasing their use of M2M have added more connections, and four in ten have expanded their solution into more countries.

How adopters are increasing their use of M2M

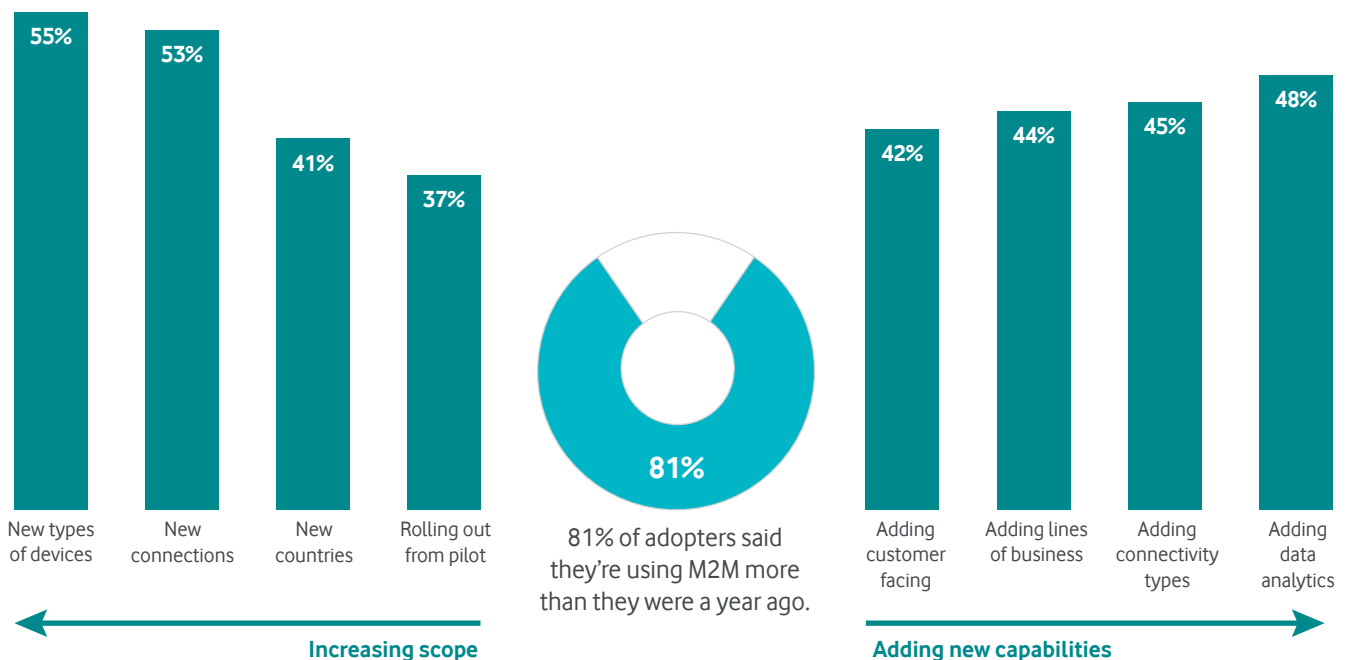


Figure 6: Adopters are expanding their projects in many ways, both expanding reach and increasing sophistication

The sophistication of applications is also growing

Many are also making their solutions more sophisticated, in a number of ways:

By applying analytics to their data

– cited by 48% of M2M users

As we predicted last year, M2M is all about the information. The value comes from gathering insight that supports decisions. 81% of pioneers say they are using analytics on the M2M data they gather, up from 75% last year. Some sectors, such as automotive, are bigger users of data than others.

“We are getting to the stage now where we are wanting more information in a quicker, more readily available fashion, so we are going to collect more data.”

Oil and gas, Europe

By bringing more lines of business into their programme

– cited by 44% of M2M users

M2M may start within a single business process — for instance, optimising a retailer’s restocking schedule — but expand to span and integrate processes. For example, automatically tracking sales across sites can not only help plan restocking visits, but help guide strategy for where to open new stores, give input into which new products should be sourced or developed, and help production make more accurate estimates.

“One of the best ways to unify [the disparate parts of the business] is using M2M.”

Aviation, Europe

By expanding from internal to external strategies

– cited by 42% of M2M users

Instead of just supporting the efficiency of internal operational processes, M2M can touch customers directly. As we reported in the 2014 Barometer, there’s a logical progression for many businesses to start by streamlining operations: using M2M to automate existing internal business processes for greater efficiency. From that point, they can start to innovate, to drive customer experiences, and to push for more revenue through new customer-facing connected products and services. 66% of those already using M2M say their M2M strategy focuses on external stakeholders.

“At this moment, our focus is still internal-oriented i.e. we want to use M2M to enable real-time data exchange to let us better monitor our operational processes — however, we will extend M2M to enhance our customer experience very soon.”

Retailer, AMEAP

Internal vs. external

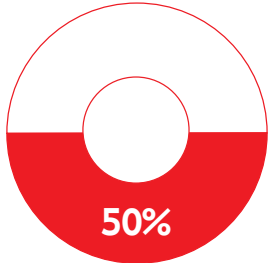
We broadly see M2M projects as falling into two categories:

- **Internal:** target the operational effectiveness, reliability, and efficiency of business processes.
- **External:** target the experience of customers, partners and other stakeholders interacting with the business.

Some M2M solutions are purely internal — for instance, energy data management. Others are inherently external — for instance, mHealth solutions. Many are both: for example, using M2M to track the movement of shipments can help to improve internal supply chain efficiency; it can also be used to give more accurate and flexible delivery estimates to customers.

Transformation is as important as optimisation

Changing what they do is one thing — but what do businesses say is motivating their M2M strategies? We asked businesses what they are using their M2M solutions for, and found a spectrum of responses (see Figure 7). Many still emphasise “doing what we do more efficiently”, choosing options like “automating processes” and “measuring service delivery”.



50% of M2M adopters say they're using it to enable new business/operating models.

Purpose of M2M projects

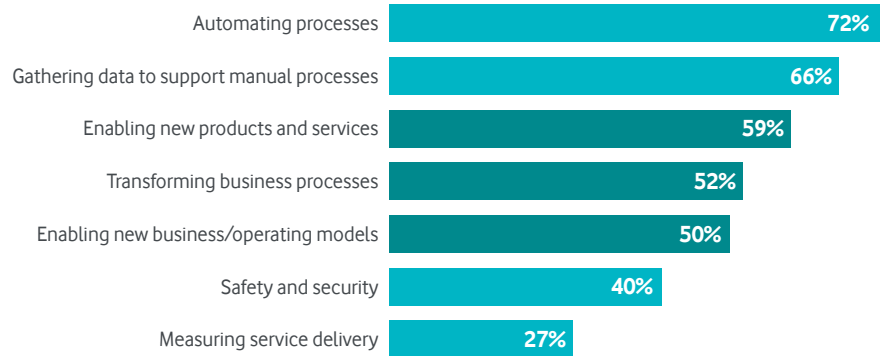


Figure 7: Businesses see their M2M projects as supporting strategic **efficiency** and **innovation** goals

But a significant number of businesses choose options that indicate more strategic, transformative goals for M2M: such as enabling new products, services and business models, and transforming business processes.

“If M2M is not helping you improve business processes, it is probably a lost opportunity, so I would not see it as just a technology purchase.”

Oil and gas, Americas



“M2M is a major strategic focus for us because it's close to the customer.”

Case study: Kärcher makes sophisticated use of M2M

One large German manufacturer, Kärcher, has made M2M a prime part of its integrated IT strategy, recognising the potential impact that the technology can have for its customers.

Kärcher provides cleaning technology for both consumers and businesses. For organisations that might run a fleet of equipment, such as building service contractors, the inclusion of M2M enables managers to check on the status of each device in real time, to see if there are any problems or if they need servicing.

“M2M is a major strategic focus for us at the moment because it's close to the customer, and we expect M2M relevance to increase,” says Prof. Dr. Matthias Mehrtens, Vice President IT of Kärcher.

“Our partner must be innovative, to meet our own thirst for innovation, and that of our customers. We need worldwide coverage and high levels of availability to support our international deployments. We're already looking ahead to technologies like 5G to see how they will affect our business.”

Mission-critical M2M needs the right connectivity

Organisations are using M2M more widely across their operations, and are looking to achieve some strategically important goals from it. In other words, they take M2M seriously. We can support this interpretation by looking at what organisations — both those that have already adopted M2M and those on the path towards it — see as important technical qualities in M2M solutions, and particularly the connectivity between edge devices and central systems (see Figure 8).

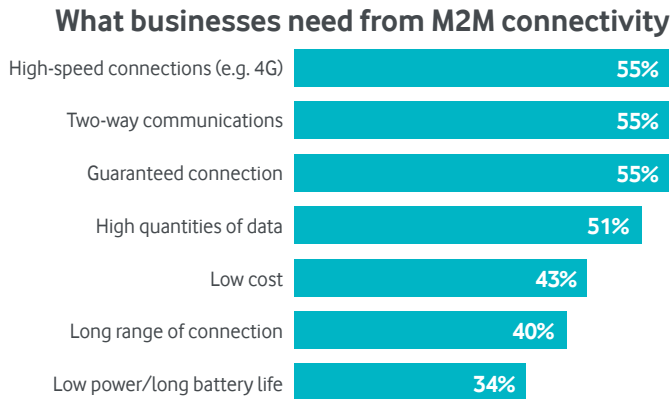


Figure 8: Organisations have a multitude of requirements for M2M connectivity

Businesses from all sectors and regions said that speed, two-way communication and guaranteed connections are important. This suggests that today M2M has moved from simple one-way monitoring applications into more diverse, sophisticated and often high-bandwidth applications, like connected-car infotainment services, digital signage, mHealth monitoring and remote security. Not all businesses are demanding in the same way, and we saw definite clusters of needs. For example:



Energy and utilities companies are most interested in the cost of connectivity — when rolling out millions of smart meters to function for ten years or more, for example, every euro counts.



Transport and logistics firms are interested in low power consumption — when tracking shipping containers that may spend months at sea or on the road, for example, endurance matters.



Consumer electronics are more interested in having long-range connections — when devices might be carried around with consumers or installed in homes anywhere around the region, for example, coverage is important.

Choice is important

Businesses are demanding. They want speed, reliability and cost efficiency — not to mention long range and power efficiency. It's not always possible to deliver all of these qualities at once, so we believe businesses will look to providers to offer a range of solutions, giving them the choice of the right technology for the task at hand.

“4G must be the most promising solution — real-time transmission without any delay must be the end outcome we want to have — a sudden downtime of our facility may cause a big disaster so that real-time data transmission is a very important task we need to achieve.”

Oil and gas, AMEAP

Organisations have the future in mind

While many organisations said that they want high-speed connections and other advanced features, that doesn't mean they're using all those capabilities today. Our research suggests that, particularly with features like 4G cellular, they're trying to future-proof their deployments in anticipation of high-bandwidth use cases emerging in the years to come.

For example, in the automotive space, OEMs are putting 4G SIMs in cars because they know 4G will become the default cellular connection during the life of the typical vehicle. Similarly, utilities companies are choosing 4G for smart meters in case 2G and 3G networks are decommissioned during the many years that meters remain in the field.

M2M pioneers tend to be technology pioneers

“In the next 3–5 years, we would pay a lot of money to explore the use of big data and construct the cloud platform to better acquire as well as store data.”

Oil and gas, AMEAP

The technology landscape today is complex and interrelated. We believe that those organisations that are taking a more holistic view of process transformation will have a broad technology vision and be more likely to have adopted other technologies along with M2M, particularly big data and cloud. We found that is absolutely the case.

Figure 9 visualises how M2M adopters are using M2M in conjunction with big data and cloud. Of those businesses that have already adopted M2M, more than half (52%) are using it alongside cloud and big data today. Only 19% of M2M adopters are using M2M on its own.

Adoption of M2M, big data and cloud technologies

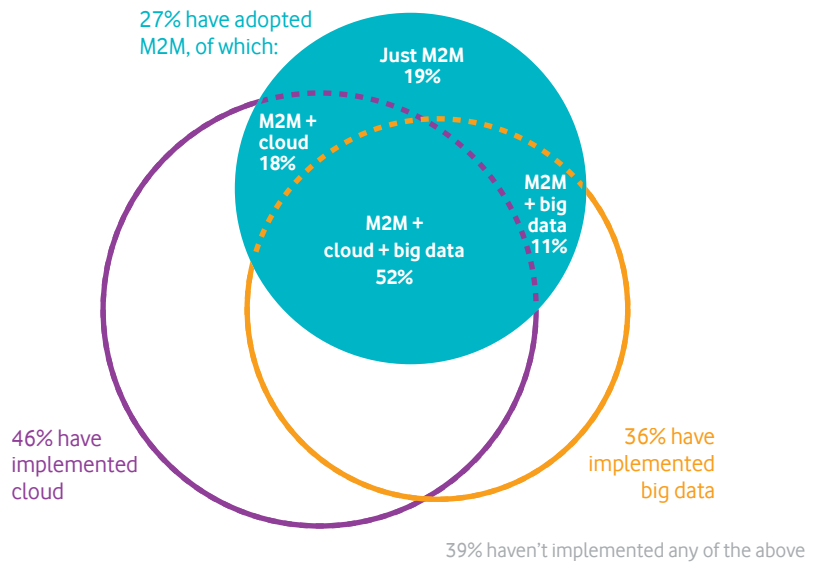


Figure 9: Of those using M2M, over 80% use cloud or big data too

“[M2M is] part of the broader conversation of trends we are seeing evolving.”

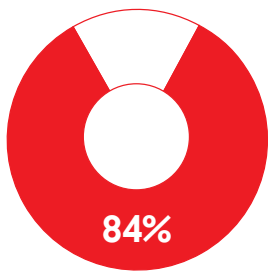
Oil and gas, Americas

It's also worth noting that, even leaving M2M aside, there is a very significant overlap between those that are using big data and those that are using cloud.

Clearly, it's possible to use M2M without big data and cloud — but very few organisations choose to do so. Businesses are recognising that they may get better outcomes by adopting these technologies together. An organisation might gather data from M2M endpoints, store it in a cloud environment, and extract value from it using big data analytics tools.

As well as simply using big data tools, organisations are confident that they can get value from them. 84% of adopters say that they are comfortable they can analyse the data they gather from their M2M solutions. This seems to us a little overconfident, given widely reported market shortages of data scientists.⁹

Businesses might also bring mobile into their overall solution, to share M2M-gathered insight with users. Indeed we found that M2M adopters are ahead in adoption of mobile. Compared to those that have yet to launch their M2M projects, they are more likely to agree with the statement that “mobile is at the heart of our business processes” (82% vs 71%).



84% of adopters are comfortable that they can analyse the data they gather from their M2M solutions.

The analyst view: technologies are interdependent

“There are clearly synergies between M2M, cloud and big data. M2M generates volumes of data that are expected to increase exponentially, and this data is stored in the cloud. Enterprises need access to the data generated from M2M applications in real time to perform the analytics that are instrumental in delivering efficiencies to their business. Interdependency between the technologies is increasing.”



M2M delivers value, and does it quickly

Organisations overall are reporting strong and transformative returns on their investment in M2M.

Adopters see clear, significant ROI

It's no wonder that organisations are increasing their adoption and broadening their sophistication in M2M — they're reporting strong results.

▶ It's transforming their businesses

We asked what impact M2M has had on their business, from "limited impact" (1) to "fundamentally transformed our business" (10). The mean score is nearly 8 out of 10. And 9% of adopters rank the impact a full 10 out of 10.

▶ It's delivering competitive advantage

83% of adopters agree that they have gained competitive advantage from M2M; 38% agree "strongly".

▶ It's producing significant ROI

Year on year, ROI is getting better. This year 59% of those already using M2M said that they've seen "significant" ROI, up from 46% last year.

▶ It's producing ROI fast

We also asked about ROI, both how significant it is and how quickly they've seen it. Generally the ROI period is very short — between 6 months and 2 years. 54% of pioneers reported ROI within 12 months.

"In the past, our loss due to inventory mis-allocation, transportation error and counterfeits was around 1% of our overall revenue — a lot of money — currently, the figure is lowered to be close to 0% — this can be translated into around 20% of our operational cost if we also take manpower and time cost into consideration... This cost saving could be seen clearly in the first month of the project launch."

Retailer, AMEAP

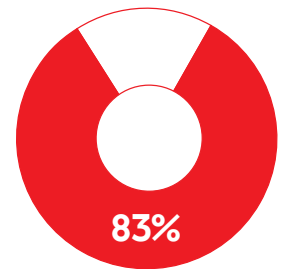
Organisations report significant cost savings

Direct cost savings ranked high on the list of benefits. Along with process and productivity improvements, this fits in to the top goal of "automating processes" (see page 16) and largely aligns with the "internal" M2M projects that we discussed in Section 3 — for example, smart metering reducing a utility company's manual meter reading costs, or a manufacturer using remote monitoring to avoid unnecessary field maintenance visits.

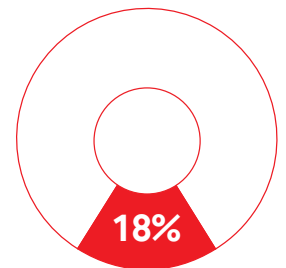
This year we asked about the scale of cost savings businesses are seeing. On average, adopters report an 18% cost reduction — significant enough to explain the fast ROI for M2M projects. Nearly 10% of M2M adopters have reduced their costs by over 25%.

Section

4



83% of adopters agree that they have gained competitive advantage from M2M.



On average, adopters report an 18% cost reduction.

“So far, all the indicators tell us that the M2M performance is up to our expectation. We can really save a significant cost after using M2M.”

Oil and gas, AMEAP

“The investment in M2M has been confirmed as being justified — the customer is happier, it is international and now covers a number of our products and there will be more.”

Manufacturer, Europe

Return on investment takes many forms

ROI for any IT project is conventionally measured in terms of payback on an amount spent, with the payback taking the form of additional revenue generated, costs saved (including in staff time) or spend avoided.

But, with sufficient effort in benchmarking and measurement, many different benefits can contribute to quantifiable ROI: from improved customer loyalty (which can boost customer lifetime value) to greater business agility and faster innovation (which reduces product development cost and can increase market share and, ultimately, revenue).

We asked adopters what benefits they’ve experienced from their M2M initiatives, and we saw a wide range of responses, as Figure 10 shows.

Areas where improvements seen after adopting M2M

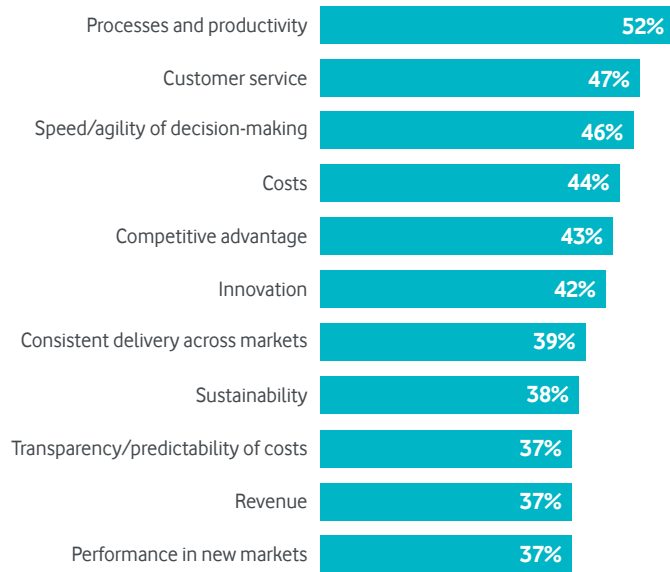


Figure 10: Businesses reported improvements in a wide range of areas

Businesses report a wide range of benefits. Some show an operational focus on streamlining and solidifying market position (for example through improved efficiency, consistency, and predictability). One small European manufacturer emphasised the impact on operational quality: “[We have seen benefits in] efficiency and substantial reduction in errors, which can be quite costly for us.”

Other benefits are about stretching and growing the business (which may be through competitive advantage, innovation, revenue, or new markets). This reflects the diversity in M2M applications and the diversity of organisations’ market positions. For example, one European manufacturer highlighted customer satisfaction: “The investment in M2M has been confirmed as being justified — the customer is happier, it is international and now covers a number of our products and there will be more.”

Prediction

As M2M projects grow larger and more deeply embedded in the business, we’ll see businesses report more significant ROI (>60% saying “significant” ROI by 2017), but longer ROI periods (<50% reporting ROI within 12 months).

The analyst view: cost is just the start

“Many M2M projects start life with an “internal” business focus, the primary objective of which is to reduce costs. Cost savings might be the primary measure of impact, but cost savings are achieved in different ways. Enterprises cite a number of measures that they use to justify investment, many of which feed into the business case: from compliance with safety regulations to improved customer retention and the creation of new revenue streams.”



More sophisticated use of M2M leads to greater benefits

Organisations see consistently stronger results when they make a greater commitment to M2M.

There's a clear link between sophistication and impact

We found a very clear correlation between the degree of sophistication of an organisation's use of M2M (which we discussed in Section 3) and the degree of benefits that they report (which we discussed in Section 4).

After ranking each company on M2M sophistication (using the methodology described across) we split them into four groups, from lowest sophistication to highest. Comparing these groups we found that the companies that are most sophisticated in their use of M2M are much more likely to report that:

- **They are seeing "significant" ROI.** 83% of the organisations in the top group have seen "significant" return, compared to 43% of the least sophisticated businesses.
- **M2M has transformed their business.** 69% of the most sophisticated group say that M2M has "fundamentally transformed" their business, compared to 13% of those in the group with the lowest rankings.
- **They are seeing large-scale cost savings.** 50% of the companies in the most sophisticated group have seen a cost reduction of more than 20% as a result of deploying M2M, compared to just 2% in the bottom group.

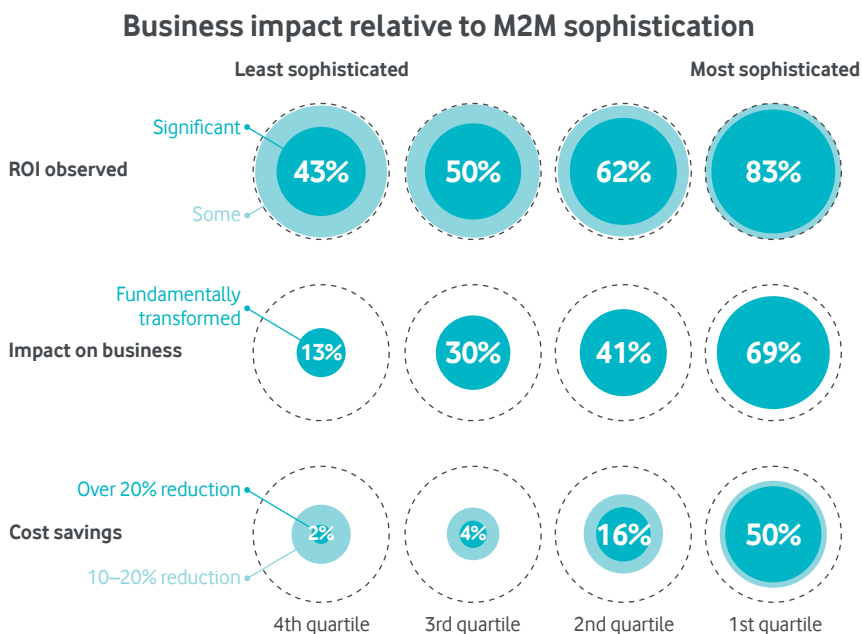


Figure 11: More sophisticated businesses report more significant benefits from M2M

In fact, the only metric by which high scorers perform worse is the time taken to see ROI. This, we believe, is because more sophisticated solutions take longer to deploy, potentially cost more, and produce ROI in ways that are harder to measure — for instance, agility or customer satisfaction instead of direct cost savings.

Section

5

Methodology for measuring sophistication

To measure sophistication we scored businesses on five factors that we think indicate ambition and pervasiveness of M2M use. Companies were awarded points if they:

- **Have increased the size of their M2M projects**, indicating commitment and business integration.
- **Are demanding in their connectivity requirements**, looking for multiple factors such as speed, reliability, and power efficiency, indicating that they have high ambitions for M2M.
- **Use M2M both internally and externally**, indicating that they are committed enough to trust their customer relationships to M2M.
- **Use a greater range of M2M applications**, indicating that they see M2M as being relevant across their operations.
- **Use analytics** to extract value from the data they collect, indicating that M2M is being used to support strategic decisions

We then grouped companies into four quartiles based on this score, from highest sophistication to lowest.

Larger organisations are ahead in M2M sophistication

There are leaders in M2M sophistication in every region, sector and size of business. But larger businesses tend to be more sophisticated. Organisations with more than 10,000 employees account for just 4% of the least sophisticated quartile, but 23% of the most sophisticated quartile (see Figure 12). The most sophisticated organisations are also most likely to have worldwide operations. 88% of top performers operate globally compared to just 26% of the least sophisticated group.

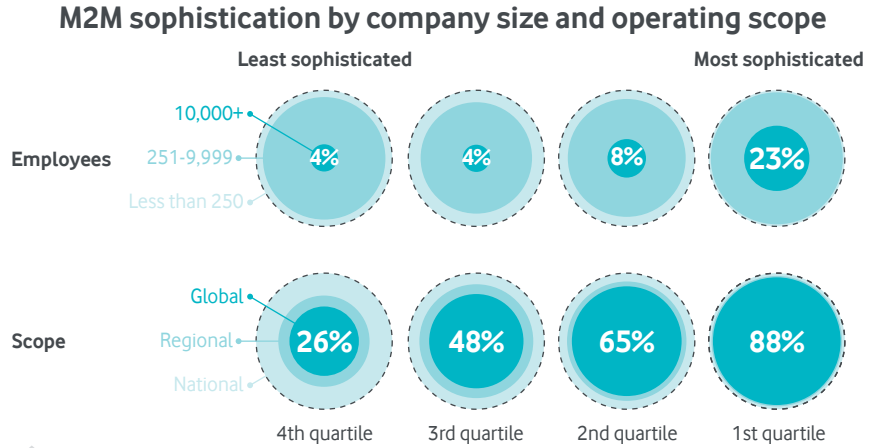


Figure 12: The most sophisticated organisations are likely to be large and global

M2M sophistication and Business Readiness are linked

In other research Vodafone has explored the concept of “business readiness”. We found that companies that have four business readiness characteristics (Figure 13) outperform the market. In an independent 2014 survey, 29% of those in the highest quartile for business readiness strongly agreed with the statement “our business is doing well relative to the competition”, compared to just 12% in the lowest quartile.

Looking at the companies in this year’s Barometer, we found a strong correlation between organisations that score highly on the M2M Sophistication Index and those that score highly on business readiness. For example, 81% of those in the top quartile for M2M sophistication say they have fully integrated IT systems; only 25% of bottom-quartile organisations say the same.

Ready Business characteristics compared to M2M sophistication

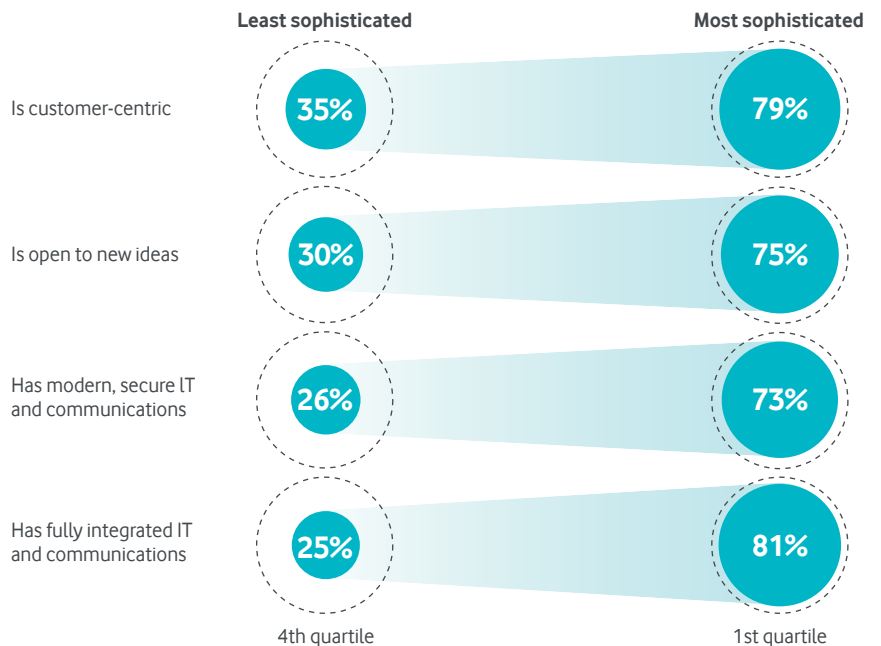


Figure 13: More sophisticated organisations are more likely to be Ready Businesses

To find out more about Ready Business and how it relates to M2M, visit m2m.vodafone.com/readybusiness

A clear strategy is essential

The five sophistication indicators are not a checklist — you can't expect to improve your ROI just by plugging an analytics tool in to your M2M solution. The important word is "indicator".

Our findings suggest that tactical "quick wins" are not the best way to maximise the ROI from an M2M project. You can certainly approach M2M as a technology to take manual labour out of a single operational process, and you'll probably see cost savings. But it's when you join the dots to other processes, mine the data, and imagine new ways of doing things that you will see the best results.

We recommend that you:

▶ **Make a strategic, long-term commitment to M2M**

While you're likely to see fast returns even from initial small projects, changes to processes and behaviours don't necessarily happen overnight. Commit to becoming a "digital business", and make M2M a part of your company's way of thinking.

▶ **Be ambitious, creative, even daring**

It may be simpler and easier to look at off-the-shelf solutions, isolated back-office processes or small-scale rollouts. But the big wins come from taking that broad look at your processes, your markets, your products and your systems, and thinking about how they can not just be automated or refined, but transformed. Think about processes end to end — for example, following a product through from raw materials through to the customer's hands and beyond — not as a series of isolated steps owned by different business units.

▶ **Collaborate and share**

Silos are the enemy of innovation. Data gathered about sales might help marketing and R&D. Data gathered about customer usage might help procurement — or legal, or HR, or finance. Take a broader view, particularly when it comes to analytics.

▶ **Plan for the future**

Think about what happens (both in terms of technology and processes) when your first pilot project gets rolled out. And plan for what happens in five years when the data that you're gathering has grown exponentially and become critical to how your company operates. Once M2M is embedded into business processes, you can't afford to treat it as a short-term experiment.

"Once I have the technology available, this will not automatically mean that I can use it well. Because I feel that's the more difficult part, you know, in a sense of how do we generate profit with it or revenue."

Manufacturing, Europe

The analyst view: making a success of M2M

"As we move into a new era of the digital economy, many enterprises are focusing on how they upgrade their physical assets and processes to embrace that change and remain competitive. M2M is a key enabler in the digital economy.

We believe that it's critical for enterprises to have a roadmap which identifies the main objectives for deploying M2M (reducing costs, increasing operational efficiency, improving process optimisation, digital transformation, and so on) and prioritises the key areas of the business that will benefit from M2M deployment near-term and long-term. The approach will most likely differ depending on the size of the business.

Large corporates may have the resources to deploy a large-scale M2M project which encompasses different areas of the business but may be faced with the complexity of breaking down the silos and streamlining operations across multiple business units.

Smaller companies may not have the budget to deploy a large-scale project but may have more visibility of how M2M will streamline their operations and create efficiencies across different business lines. For all enterprises, a longer-term vision and roadmap on how to achieve their objectives is required."



Section

6

Few barriers stand in the way of M2M adoption

Companies are enthusiastic about adopting M2M and its benefits. But concerns about how best to address security are holding some back.

Security and privacy are the most common obstacles

“I can see that the price and the ease of implementing M2M technology is getting better... it is easier for us to consider doing some projects with it if we wanted to... the complexity and cost has dropped considerably over the last eighteen months.”

Manufacturer, Europe

As M2M has evolved, just like any technology, there have been challenges to overcome: interoperability and standards; cost and complexity; network coverage; battery life; and so on. While adoption continues to grow, and most businesses report extremely strong ROI, we wanted to investigate which of these challenges remain, and what effect they're having on M2M users.

We asked organisations what, if anything, is preventing them from using or increasing their use of M2M. None of the potential barriers that we listed were selected by more than a third of respondents (see Figure 14). This is very encouraging. While there are concerns, notably security and the related subject of privacy, most companies don't see these as a barrier to adoption. These results compare favourably with many of the figures reported for other new technologies, like cloud computing.

Barriers to increasing use of M2M

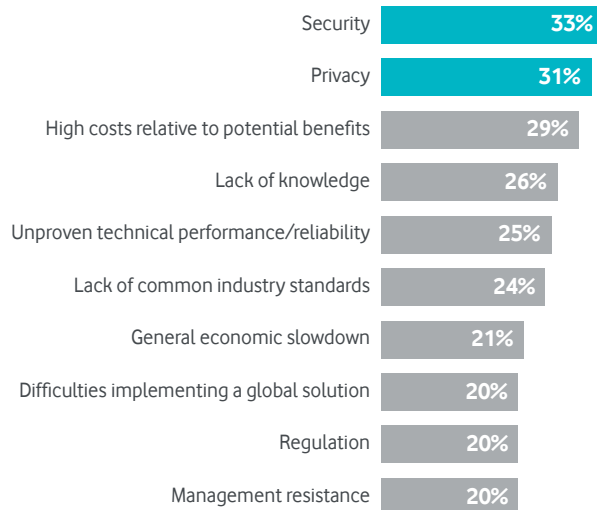
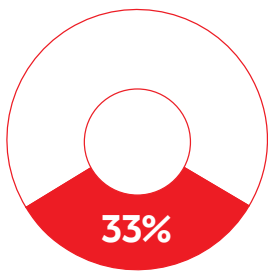


Figure 14: Just a third of businesses say security is a potential barrier to increased use of M2M

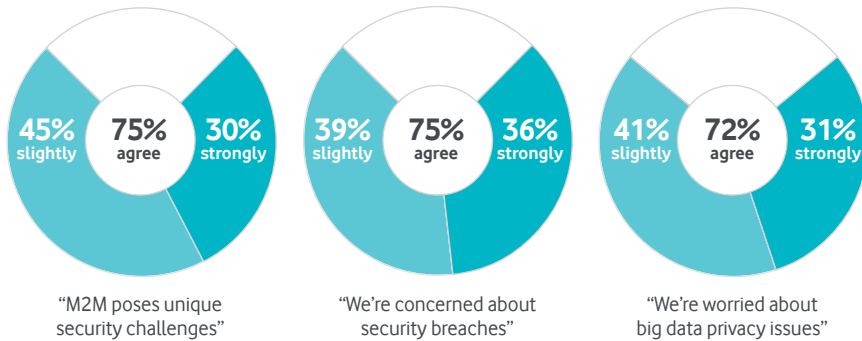


33% of businesses said that security is a barrier to them increasing their use of M2M.

Organisations are concerned about security breaches

M2M providers, analysts and customers talk a lot about security and privacy — we anticipated that they would be important factors. So we asked some additional questions to understand businesses’ concerns in more detail.

Perception of M2M security impact



"We need to reassure customers that we are doing [security], we don't want to hit the headlines."

Manufacturer, Europe

Figure 15: Around three quarters of businesses are concerned about security issues

Understandably, there are some differences by sector. Retail and health ranked highest for security and privacy concerns: 41% of healthcare organisations agreed "strongly" that security breaches are a major concern, compared to 36% across all sectors. 35% of retailers agreed strongly that they are worried about privacy issues, compared to 31% across all sectors.

"There is security of patient data: that goes through Wi-Fi so how secure is that, are devices secure, what happens if they get lost?"

Healthcare, Europe

Businesses in sectors such as healthcare tend to hold a lot of private customer data, depend on maintaining their brand equity, and are subject to relevant regulation, such as PCI DSS for payment card data and HIPAA for healthcare records.

Conversely, sectors like transportation rank lower — just 23% of transportation and logistics companies agree strongly that security breaches are a major concern. This is probably because businesses such as this hold less personal data.

IT leaders are more concerned about security

Both IT and business leaders focus on security and privacy. However, IT leaders show greater concern than those in other roles (see Figure 16). 40% of IT leaders strongly agree that security breaches are a concern, compared to just 31% of those in product management.

Concern about security breaches, by function

"Security breaches are a major concern for us"

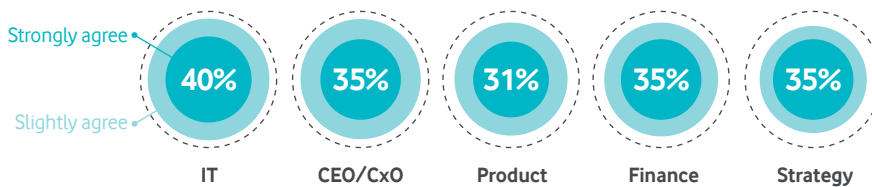


Figure 16: IT leaders most likely to express concern about security issues

Despite the concerns, most say their IT is secure

Over three-quarters of businesses (77%) believe that their IT and communications are secure, while the same proportion are concerned about security breaches. This leads to four groups, which Figure 17 shows:

Four attitudes to security

The rightfully concerned (15%): believe that their businesses are not secure and are concerned about security breaches.

The cautious (62%): feel their IT and communications are secure, but are still concerned about security breaches.

The confident (15%): say that their businesses are secure and aren't concerned about security breaches.

The risk-takers (8%): admit they're insecure, but are unconcerned about security breaches.

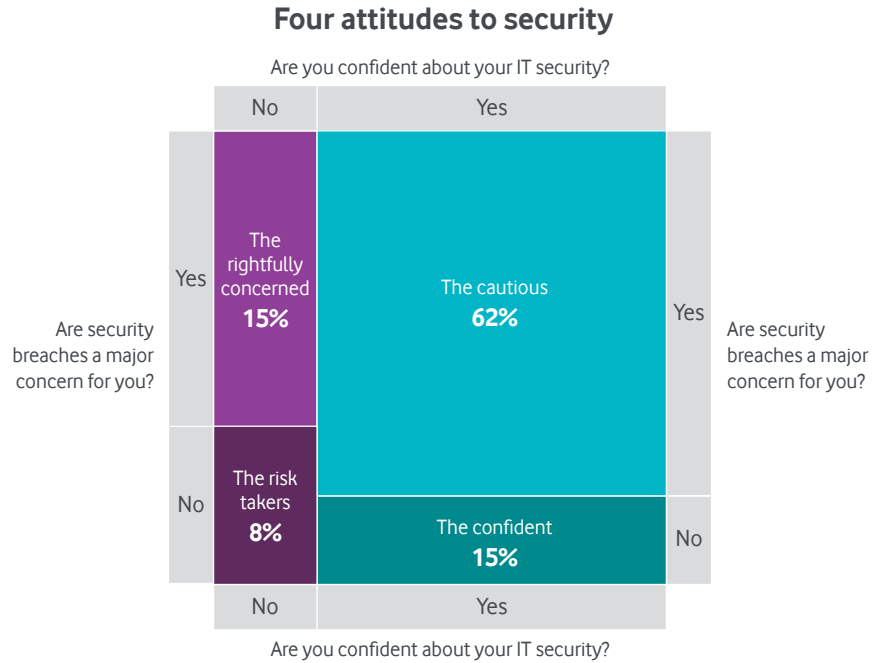


Figure 17: Organisations fit into one of four groups based on their security posture

Providers can help businesses to address security

M2M solutions are composed of several different elements including devices, networks, management platforms, applications and storage. End-to-end providers can provide standards-based and joined-up solutions to effectively protect all these elements together.

Organisations should plan the security of their M2M project from the start and ensure that a senior business leader assumes ownership of security for IT and M2M. M2M security is like any other technology: with adequate planning and the right set of controls, organisations can manage risk and protect their data and infrastructure.

The analyst view: approaches to M2M security

“Security is a very real concern for the Internet of Things. Any ‘thing’ with an IP address is potentially vulnerable to a malicious attack. However, the risk of security breaches should not normally outweigh the benefits of deploying M2M and increased awareness of the potential scale of the problem means that there is a heightened focus to address that risk.

Controlling millions of dispersed devices will require more automated security techniques than those required for a typical IT initiative. Security will need to become more pervasive in the network to meet the needs of a perimeterless security environment. Fortunately, there has been a rise of security orchestration solutions to counter network security threats in IT and core telecoms networks. There are a number of suppliers providing solutions to address this requirement.

Enterprises will need to ensure that the roadmap of their security provider meets the requirements of an M2M/IoT environment. They may also want to consider expanding their security skills base to include expertise in managed threat detection.”



M2M involves the whole business

As M2M gains a higher profile and expands across business processes, its ownership and position within the organisation is likely to change.

The business sees M2M as supporting innovation

As we saw in our discussion about security, different roles within the business have a different perspective. Similarly, different roles have their own views on M2M generally, and how it fits into the wider corporate agenda.

We asked businesses to classify their M2M projects (see Figure 18). IT leaders are most likely to see M2M deployment as an “IT project”, suggesting they view it as their responsibility — they are therefore interested in how M2M can be practically deployed across their organisation. CEOs, senior leaders and strategy roles are most likely to see M2M in the context of innovation initiatives — ways to change what the business does and how it works in order to drive improved operational outcomes.

Classification of M2M projects, by function

Rank	CIO	CEO	Product	Finance	Strategy
1st	IT 56%	Innovation 33%	IT 36%	IT 29%	Innovation 42%
2nd	Innovation 17%	IT 32%	Innovation 29%	Business development 23%	IT 23%
3rd	Business development 12%	Business development 26%	Business development 18%	Innovation 16%	Business development 23%

Figure 18: M2M projects are seen in different lights by different roles, but most see it as an IT project

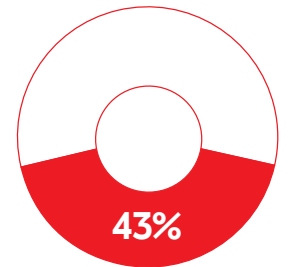
Many respondents also described M2M projects in the light of business development — using M2M to drive revenue growth, without necessarily changing the way the business runs or its fundamental proposition to its customers. This might mean:

- Adding connectivity to existing products to stimulate sales or to enable secondary revenue opportunities, such as using M2M to deliver advertising direct to products.
- Gathering data (for instance, about customer behaviour or environmental measurements) that the business can sell on the open market.
- Using M2M-driven market insights to target sales and marketing efforts to improve conversion rates and customer lifetime value.

Respondents from the Americas were more likely to describe M2M projects in this way — and this region also reported the fastest average ROI.

Section

7



43% of businesses see M2M projects as being “IT projects”. 21% say they are “innovation projects”.

Prediction

By 2016, more than a third of businesses will describe their M2M projects as being “innovation projects”, as M2M moves outside the IT department and plays a larger role in determining customer experience and competitive advantage.

All roles are committed to business transformation

Just because different roles see M2M projects in different lights doesn't mean that IT teams and the rest of the business are working to different objectives. When asked whether they agree that M2M is about improving businesses processes, not just about buying technology, IT leaders are actually more likely to agree strongly (see Figure 19). They are interested in the tangible ROI realised and see it as a strategic business decision.

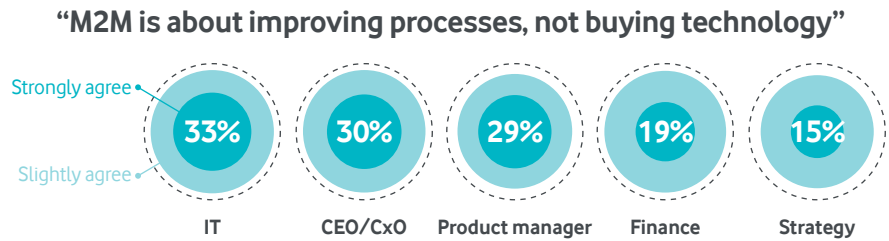


Figure 19: IT leaders embrace the business potential of M2M

The CIO leads, but many other roles are involved

Multiple stakeholders are often involved in decisions regarding M2M projects. The CIO leads most often, in 36% of cases, followed by the CEO, strategy director, operations and finance. The CEO leads the M2M strategy in 16% of businesses.

Regardless of who leads, senior decision-makers from multiple departments may be involved (see Figure 20) — this is natural and desirable when M2M touches so many parts of the business. Nearly two-thirds of businesses (63%) reported having multiple leaders involved; 10% had more than five in their decision-making group.

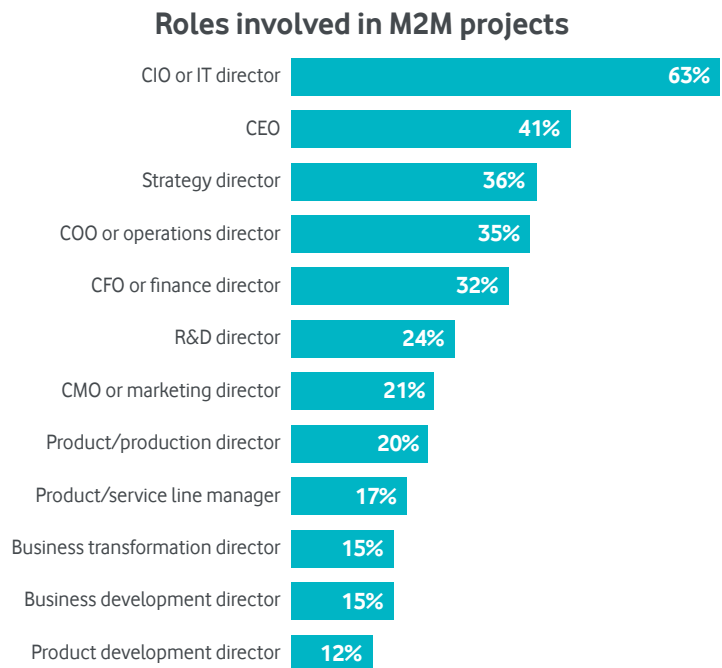


Figure 20: Many senior staff can lead or be represented in M2M projects

Less than half of M2M projects come out of the IT budget

M2M is not seen as a conventional IT project, and that is reflected in the way it's funded. Less than half of businesses say that M2M projects are funded through the IT budget. We noticed a broad spread of financing models around M2M, including more experimental models such as cross-charging, risk and reward sharing, and building it into the price of services to the end customer (see Figure 21).

The prevalence of these kinds of funding innovations support the view that M2M is seen as transformational. Risk and reward sharing, in particular, is not yet common in most areas of IT, yet here 28% of businesses say they use it. We expect this type of model to become increasingly common as organisations put more emphasis on the measurable business value that M2M initiatives are targeted to deliver.

How M2M projects are funded

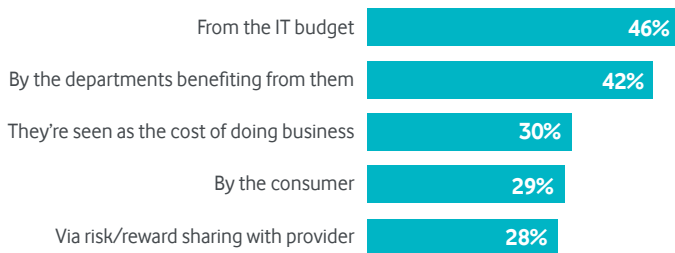


Figure 21: Adopters have tried a range of business models (multiple options allowed)

External providers play an important role

From network providers to device manufacturers, service providers and system integrators, many outside parties will play a role in M2M projects.

Businesses told us that they would be willing to outsource many parts of the solution, from hardware to software and connectivity. 78% say they would use an external provider to integrate the different components of an M2M solution. Those that have an M2M solution spanning both internal and external strategies are more likely to outsource the system integration of their solution.

When it comes to choosing a provider, organisations look for global reach and for end-to-end capabilities. 46% of businesses said it was “very important” to work with a provider that offered all the components involved in an M2M solution. Again, those that have an M2M solution spanning both internal and external strategies stand out, putting much more emphasis on working with an end-to-end supplier to make the project happen (see Figure 22).

The importance of working with an end-to-end provider

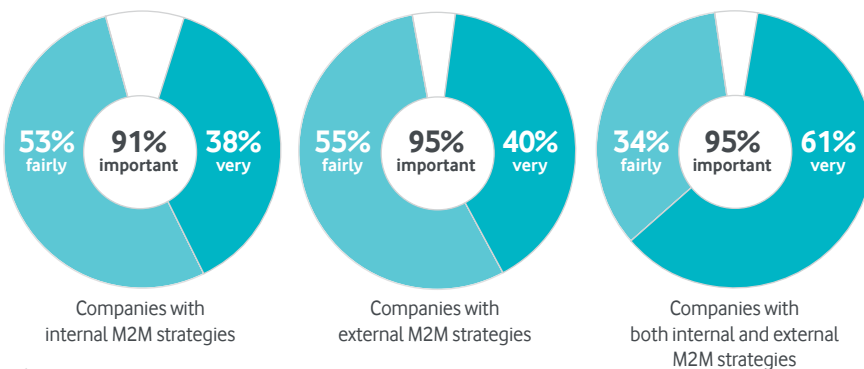


Figure 22: Suppliers are seen to play a more critical role when solutions touch customers

Prediction

Fewer organisations will count the costs of M2M projects as part of the IT budget as they become more deeply embedded in the business. We predict cross-charging will become the most popular way to account for M2M costs.

Conclusion

This year, the question is not whether to adopt M2M, but how best you can use it to drive your business.

As adoption continues to increase year-on-year, we've turned our focus to those businesses that have already committed to M2M, finding out more about their experiences, and what their next steps were.

M2M is proving its worth

Adopters of M2M are consistently positive about the results they've seen. These include a range of benefits, clear ROI, measurable cost savings and — ultimately — a significant level of organisational transformation. Perhaps most tellingly, those that use M2M are satisfied enough to extend their use of it over time.

Sophistication determines outcomes

Organisations are not just using M2M more, they're building their business around it. The more advanced users are bridging organisational functions and extending beyond the company's four walls to affect customers. They're analysing the big data it can generate, too, and using cloud and mobile solutions alongside. These sophisticated organisations see better results across the board.

As M2M spreads, roles will matter more

M2M is still led by IT, but in many cases it's a company-wide initiative. The different motives, concerns and budgets of leaders of many business functions must all be taken into account. End-to-end providers of M2M solutions can help provide support for the IT function, not just with technical issues like system integration and security, but by participating in risk/reward sharing and other aspects of the M2M business model. There's plenty of room for innovation.



Recap of our predictions

As M2M projects grow larger and more deeply embedded in the business, we'll see businesses report more significant ROI (>60% saying "significant" ROI by 2017), but longer ROI periods (<50% reporting ROI within 12 months).

By 2016, more than a third of businesses will describe their M2M projects as being "innovation projects", as M2M moves outside the IT department and plays a larger role in determining customer experience and competitive advantage.

Fewer organisations will count the costs of M2M projects as part of the IT budget as they become more deeply embedded in the business. We predict cross-charging will become the most popular way to account for M2M costs.

Further reading

To find out more about the changing world of M2M, and the opportunities within your industry, visit the following areas of our resource centre.

Case studies

Read about the experiences of more than 50 organisations with M2M, representing businesses from the UK to India, from start-ups to the largest multinationals.

m2m.vodafone.com/casestudies



White papers

Learn about the most important issues and applications in M2M with our growing range of white papers. They cover specific M2M markets, such as security or electric vehicles, and in-depth country-level reports for more varied topics such as mHealth and smart metering.

m2m.vodafone.com/whitepapers



Industries

Discover the broad range of solutions and services we provide for your sector. Our industries area includes videos, case studies, news and more.

m2m.vodafone.com/industries



The M2M Adoption Barometer 2014

2015 is the third year of the M2M Barometer. To find out how things have changed, take a look at last year's report.

m2m.vodafone.com/barometer2014



Start your journey

To find out more about Vodafone's M2M solutions, please contact your Vodafone account manager, email m2m@vodafone.com, follow us on Twitter [@Vodafone_M2M](https://twitter.com/Vodafone_M2M), or visit m2m.vodafone.com

About Vodafone

To find out more about the changing world of M2M and IoT, and the opportunities within your industry, visit the following areas of our resource centre.

About Vodafone Machine-to-Machine (M2M)

Vodafone Machine-to-Machine (M2M) connects previously isolated machines or devices to the internet, delivering new functionality and enhanced services without the need for human intervention. Supported by more than 1,300 dedicated employees, Vodafone's global M2M platform makes it easy for global businesses to centrally manage M2M deployments across multiple territories, with greater control and at a lower cost than previously possible. We have been highly rated by prominent industry analysts including Analysys Mason, Current Analysis and Machina Research. We were also positioned as a Leader in the Gartner Magic Quadrant for Managed Machine-to-Machine Services.

For more information, visit: m2m.vodafone.com

About Vodafone

Vodafone is one of the world's largest telecommunications companies and provides a range of services including voice, messaging, data and fixed communications. Vodafone has mobile operations in 26 countries, partners with mobile networks in 55 more, and fixed broadband operations in 17 markets. As of 31 March 2015, Vodafone had 446 million mobile customers and 12 million fixed broadband customers.

For more information, visit: vodafone.com

References

1. BCG Perspectives, "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries", 2015
2. Gartner, "Gartner Says Worldwide IT Spending to Decline 1.3 Percent in 2015", 2015
3. IMF, "Uneven Growth: Short- and Long-Term Factors", 2015
4. PwC, "Consumer electronics", 2015
5. CNET, "Samsung co-CEO: In 5 years, all our products will be Internet connected", 2015
6. The New York Times, "At the International CES, the Internet of Things Hits Home", 2015
7. PwC, "Transportation and logistics", 2015
8. PwC, "Industrial manufacturing", 2015
9. Bloomberg, "Help Wanted: Black Belts in Data", 2015

About our contributors



Circle was founded in 2006 as an alternative to traditional consumer-focused research agencies. Our mission is to uncover hidden truths about our customers' target market. Through primary research we'll provide insights, which enable organisations to:

- Segment the market and tap into the customer buying journey.
- Invest in the right marketing channels and messages.
- Build a resonant and differentiated brand.
- Create great thought leadership content.
- Create happier, more loyal customers.
- Create successful new products or services.

Based in London, we work globally with ambitious B2B firms, including half of the Top 10 B2B Superbrands.

Learn more at circle-research.com, or follow us on Twitter [@circle_research](https://twitter.com/circle_research)



Our expertise in the three key areas of telecoms, media and technology underpins everything we do and helps us change our clients' businesses for the better.

Analysys Mason's approach is based on a simple but powerful idea: applied intelligence.

By harnessing our collective knowledge, we can solve real-world problems and deliver tangible benefits for our customers.

We're also passionate about what we do. We'll rise to a challenge and enjoy doing so. In fact, when it comes to problem solving, there's a real sense of 'the more challenging the problem, the better'.

It's this unique combination of applied intelligence, a passion for problem solving and consistently looking closer and seeing further that makes us who we are.

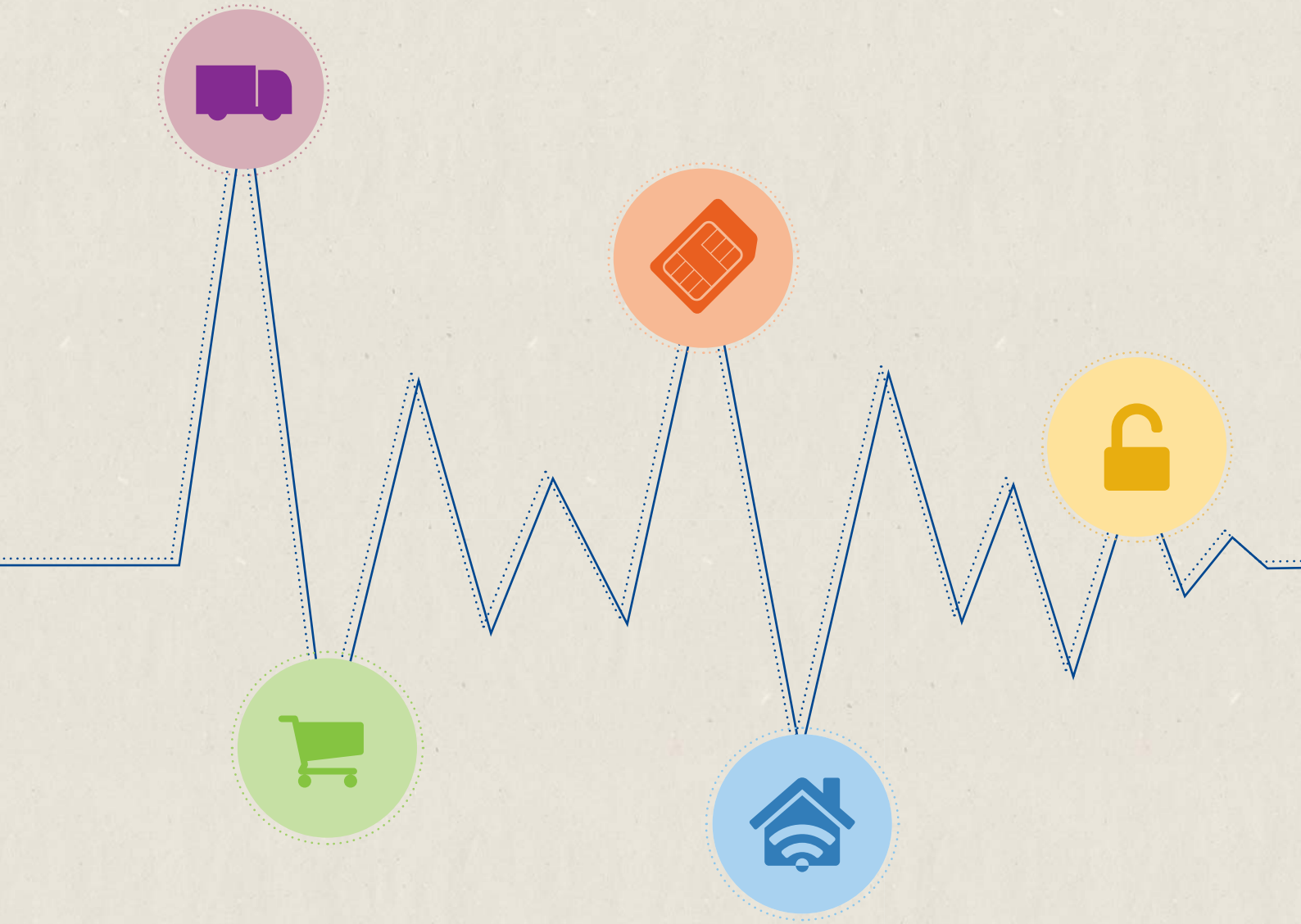
Michele Mackenzie is an analyst for Analysys Mason's IoT and M2M Solutions research programme. She has 15 years of experience as an analyst. Prior to joining Analysys Mason she produced reports for Machina Research and for other clients on areas such as mobile broadband and digital media. Michele worked for Ovum for 12 years where she focused on consumer mobile applications.

Find out more at analysismason.com

m2m.vodafone.com

Vodafone Group 2015. This document is issued by Vodafone in confidence and is not to be reproduced in whole or in part without the express, prior written permission of Vodafone. Vodafone and the Vodafone logos are trademarks of the Vodafone Group. Other product and company names mentioned herein may be the trademark of their respective owners. The information contained in this publication is correct at the time of going to print. Any reliance on the information shall be at the recipient's risk. No member of the Vodafone Group shall have any liability in respect of the use made of the information. The information may be subject to change. Services may be modified, supplemented or withdrawn by Vodafone without prior notice. All services are subject to terms and conditions, copies of which may be provided on request.





Securing the benefits of industry digitisation

A REPORT FOR VODAFONE – NOVEMBER 2015

Contents

	Important Notice	1
	Vodafone Foreword	3
1	Executive summary	5
2	About the study	7
3	The opportunity	9
4	Regulatory threats to industry digitisation	21
5	Policy recommendations	38
	Appendices	
	Key notes and assumptions	39
	Endnotes	40

Important Notice

This report has been prepared by KPMG LLP ("KPMG") for Vodafone Group plc ("Vodafone"), in accordance with the confidential terms of an agreed work order.¹ Although KPMG's work was performed exclusively for Vodafone, KPMG has agreed to publication of this report in order to enable Vodafone to demonstrate that this report has been commissioned and issued and to facilitate wider awareness of the matters discussed.

In preparing this report we have not taken into account the interests, needs or circumstances of anyone apart from Vodafone, even though we may have been aware that others with an interest in the matters discussed might read this report. We have prepared this report for the benefit of Vodafone alone.

This report is not suitable to be used or relied on by any other party wishing to acquire rights against KPMG for any purpose or in any context. Any party other than Vodafone that chooses to rely on this report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG does not assume any responsibility and will not accept any liability in respect of this report to any party other than Vodafone.

The information in this report is based upon publicly available information and information provided to KPMG by Vodafone and other third parties. It reflects prevailing conditions and views which are subject to change. In preparing this report, KPMG has relied upon and assumed, without independent verification, the accuracy and completeness of the information upon which the report is based, including that available from public sources and that provided by Vodafone and third parties.

In its contribution to the preparation of this report, Hogan Lovells has acted solely as legal adviser to Vodafone. This report may not be relied upon as legal advice by any person, and neither Vodafone, KPMG nor Hogan Lovells accept any responsibility or liability (whether arising in tort, (including negligence), contract, or otherwise) to any other person in relation to this report or its contents or any reliance which any other person may place upon it. References or statements relating to any law, regulatory guidance or policy are made as of 24 July 2015.



Vodafone Foreword

Having the right tools for the job is always going to result in a better outcome. Policymakers around the world have long been focused on ensuring regulation protects and encourages consumers participating in the digital revolution. The needs of enterprises as they move towards the digitisation of industry have been less defined. This is why Vodafone has commissioned KPMG to review the regulatory and policy tools currently underpinning the future of successful enterprise development and investment across the globe.

In Vodafone's view, policy and regulation must be developed with the specific needs of the enterprise sector in mind, rather than as a by-product of regulation designed for consumer needs. By way of example, industry will require fit-for-purpose, harmonised access to 5G spectrum to help deliver innovations in telemedicine. Open internet rules must be applied flexibly enough to ensure a real-time, differentiated approach for applications like autonomous vehicles. Fit-for-purpose access to fixed networks is required in order to meet the burgeoning data needs of enterprise customers. It is also vital to ensure that regulation – intentionally or otherwise – does not unduly restrict the transfer of industrial data and services across borders.

It is clear there are a plethora of areas that the KPMG report could have concentrated on but, with the guidance of some of our existing 1,700 multinational customers, we have focused on three key areas:

- issues surrounding transfer of data post-Snowden;
- challenges to cross-border provision of Machine-to-Machine and the Internet of Things; and
- the impact of restrictions on a quality differentiated internet.

These are areas of immediate relevance to multinational businesses that are seeking to fully harness the opportunities of digitisation in the global economy.

This report would not have been possible without the contribution of those business leaders who gave so freely of their time and insights. We believe that their input has led to a report that raises some compelling findings and underpins the need for policymakers across the globe to work together to create policies enabling industry to innovate and transform through digitisation.

Jan Geldmacher

Chief Executive Officer,
Vodafone Global Enterprise

Executive summary

Digitisation is becoming an increasingly important part of the production process for many goods and services; transforming the value chain in many industry sectors. Digitisation is leading to improvements in production processes and, in some cases, is replacing the physical flow of goods.

“There are projected to be over 50 billion “things” connected to the internet by 2020, up from 25 billion in 2015.”

Regulatory and policy frameworks that will impact on the digitisation of industry are currently being developed at both national and regional levels. These cover a wide range of important policy matters including cyber-security, privacy and data protection. Due to the rapid pace of technological change, it is proving a challenge to establish frameworks that appropriately balance the needs of all stakeholders. Policy frameworks also need to be applied in a coherent manner, recognising that in some cases a different approach is needed for ICT services for enterprises compared to services for consumers. Achieving policy coherence across borders is particularly difficult. This study is an effort to help address these challenges, so that the full potential of ICT services might be realised for businesses and consumers alike.

Vodafone commissioned KPMG to assess the economic impact on business ICT services of emerging rules in a number of areas, including net neutrality, licensing and authorisation, numbering, and data localisation. Policy and regulation in each of these areas will shape the future growth of global ICT services used by businesses including Machine to Machine (M2M) or Cloud and Hosting technologies, as well as digital services that rely on a differentiated quality of service. To inform our study we interviewed teams within Vodafone as well as a select number of its Global Enterprise customers. We also conducted wider research and analysis.

The use of ICT services by businesses is already large and is rapidly growing:

- There was an installed base of 5.3 billion M2M devices globally as of 2014.²
- There are projected to be over 50 billion “things” connected to the internet by 2020, up from 25 billion in 2015.³
- sSpending on cloud services and infrastructure could reach \$235 billion by 2017, compared to \$174 billion in 2014.⁴

This adoption is expected to deliver significant and wide ranging socio-economic benefits:

- Our analysis, based on Vodafone data, suggests that the Gross Value Added (GVA) generated by providers of cellular M2M⁵ services alone was in the region of €2.5 billion in 2013/14.
- The wider socio-economic benefits from ICT services are likely to be substantially higher, including for example reduced congestion and fewer traffic accidents thanks to the evolution of connected cars⁶, carbon savings from smart energy markets⁷ and improved health outcomes through remote patient monitoring and advice. As an example, Vodafone has estimated that the total carbon savings from its smart metering, smart logistics and fleet management, call conferencing and Cloud and Hosting services was 3.5 million tonnes of CO₂-equivalent (CO₂e) for active connections in 2014/15, 50% more than in 2012/13.⁸
- Cloud and hosting services can deliver cost savings as well as improving efficiency, scalability and improve productivity.^{9,10}

A supportive regulatory policy regime (on both the demand and supply side) can play an important role in securing these socio-economic benefits. For example, it is estimated that the creation of a connected EU digital single market will drive an additional €250 billion in growth across Europe.¹¹

“Policy makers and regulators have an important role to play in both the demand and supply side of the market to create a supportive environment that allows the digitisation of industry to flourish.”

However, we also found evidence of the economic detriment that regulation of ICT services could cause. In particular:

- Net Neutrality regulations that cover business ICT services may restrict the ability of businesses to offer a range of ICT products that rely on a differentiated quality of service. For example, the use of video-conferencing for remote telemedicine consultations has the potential to reduce healthcare costs and improve patient outcomes. However, the viability of the service will be in large part dependent on the ability of service providers to guarantee network access at a certain level of quality. Similar needs for prioritised network access will apply to ICT applications for emergency services, connected cars, and smart energy meters.
 - By 2020, 50% of M2M devices are projected to require some form of quality of service differentiation.¹²
 - The value of the global video conferencing market (which may require a higher quality of service) is expected to reach \$6.4 billion a year by 2020.¹³
- Our study has found that inconsistencies in the way similar services are regulated in different countries are already having commercial impacts on service providers and their customers. These impacts will grow in importance as the market for such services expands. For example, prohibitions on non-transitory roaming for M2M SIM cards in Brazil are leading to increased costs and delaying the launch of M2M services.
- Regulations that unduly restrict the cross-border transfer of personal and machine-generated data (for example in parts of the Asia-Pacific and Middle East regions), are likely to increase the costs of providing global ICT solutions. This can reduce the range of services available, increase costs and complexity for businesses working to provide the services and, in the extreme, threaten the commercial viability of some services.

Policy makers and regulators have an important role to play in both the demand and supply side of the market to create a supportive environment that allows the digitisation of industry to flourish. Our study suggests that the consequences of not doing this could be significant. There is an urgent need for all stakeholders – including industry, governments and regulators – to work together to create a consistent regulatory environment that is ‘fit for purpose’ for the global ICT enterprise market. We have suggested a number of policy actions that can be taken to this end.

About the study

A combination of technological innovation and improvements in network quality and reach is rapidly changing the nature of the global information and communications technology (ICT) market. These trends, in turn, are driving the rapid increase in the global connectivity of consumers and businesses. Digitisation is also becoming an important part of the production process for many goods and services. Across industry sectors, services provided to end customers are being enhanced by ICT solutions. Connected cars, telehealth solutions, and smart energy grids are just some of the examples we have seen.

A supportive public policy and regulatory regime is critical to the realisation of the social and economic benefits that can come with this process. Such a regime should stimulate the digitisation of industry on the demand side, while facilitating the provision of ICT products and services on the supply side. A growing number of multinational enterprises are expressing concern that the emerging global patchwork of regulation in this area is falling short of such ambitions.

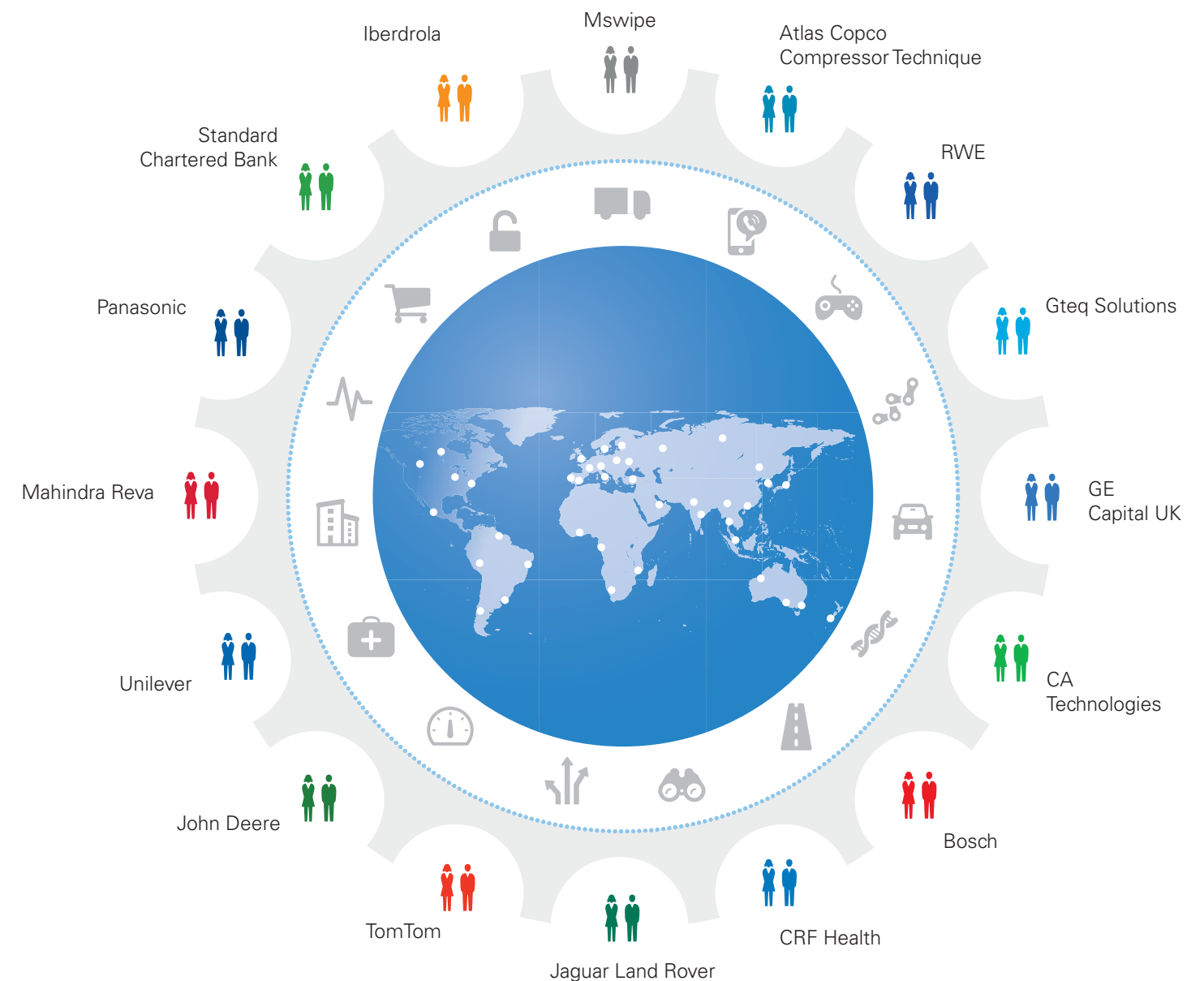
Given this, Vodafone commissioned KPMG LLP to undertake a study to assess the potential economic impact of a number of current and proposed regulations affecting ICT services, including M2M and Cloud and Hosting services. We have also considered how the concerns of business, governments, and consumers can be addressed through policies that enable the digitisation of global enterprises.

Our study comprised:

- Interviews with Vodafone enterprise customers. These customers were selected by Vodafone to reflect a range of ICT services, geographies, and sectors.
- Interviews with Vodafone internal teams.
- Desktop research and analysis of publicly available information, academic and industry studies and forecasts.
- Economic analysis, drawing on Vodafone and publicly available data and forecasts.

Hogan Lovells participated in the preparation of this report by undertaking an internationally co-ordinated quality assurance review of its references to laws, regulations and policies. This review spanned some twenty jurisdictions around the world, and Hogan Lovells is particularly grateful for the expertise provided by colleagues and external counsel in Germany, Egypt, Saudi Arabia, Brazil, Korea, India, Turkey and South Korea.

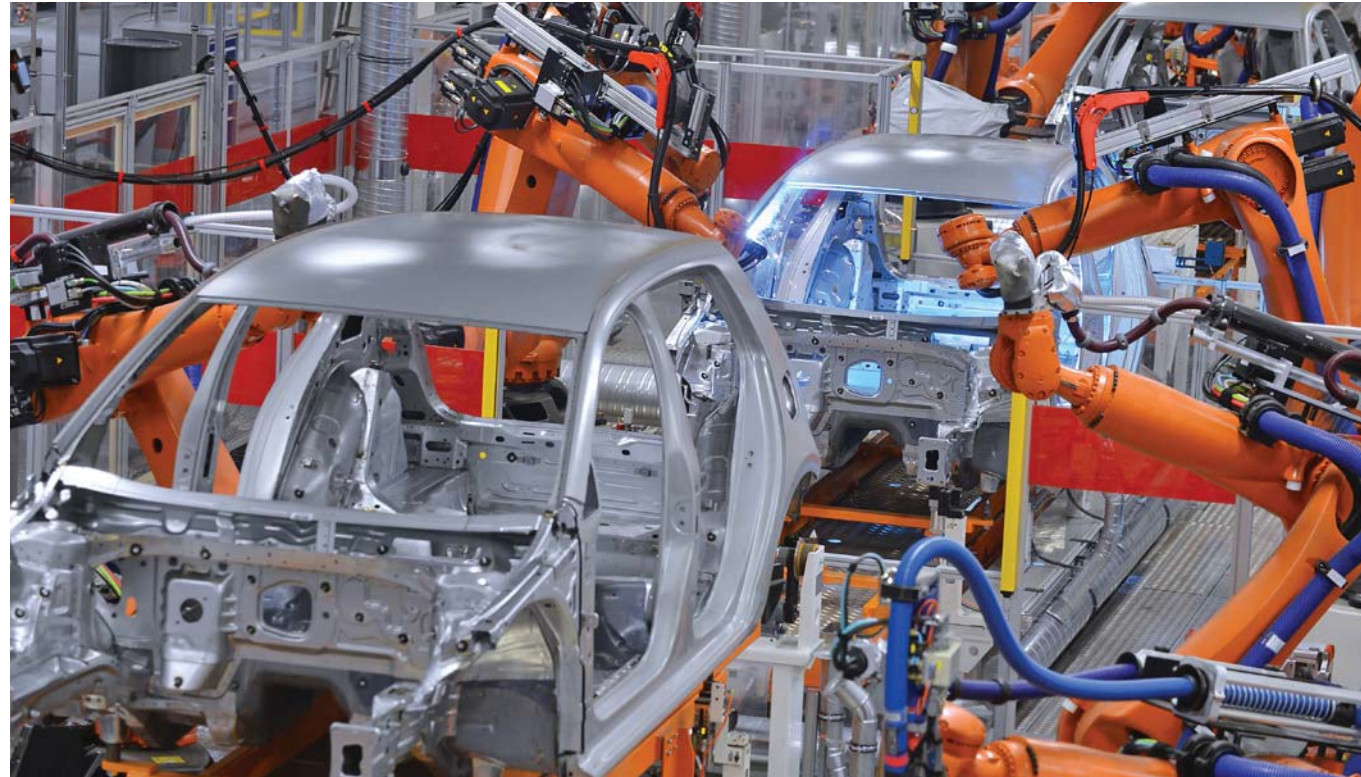
Interviews conducted with Vodafone enterprise customers selected by Vodafone to reflect a range of ICT services, geographies and sectors.



The opportunity



Trends in the use of ICT services and machine generated data by enterprises



Growth in ICT has been a significant contributing factor to the growth of the globalised economy.¹⁴ Multi-National Corporations across all industry sectors, are increasingly reliant on ICT for managing their business processes, systems and operations. Digitisation allows businesses to improve the efficiency of operations, expand market reach and reduce risk.

Consumers have also benefited from more competitive prices, reduced travel times, greater real-time information and an ever-expanding range of value-added services. For society, digitisation is having a range of impacts including greater energy efficiency, smarter transport use, fewer car accidents and injuries and improved health outcomes.

The mechanisms for digitisation are also changing. Forecasts suggest that the rate of growth in data traffic will exceed substantially the growth in mobile connections in coming years.¹⁵ Telecommunications providers are diversifying their revenue streams towards new data and value-added services to capitalise on this. This has led to a significant increase in network infrastructure investment, to new services and to the IT platforms to deliver these. According to recent research by Boston Consulting Group, between 2009 and 2013 the mobile industry globally invested US\$1.8 trillion in mobile communications infrastructure.¹⁶

A range of ICT products and services is being adopted by enterprises as part of their digital strategies. ICT services are being used to deliver new and improved services to customers. For example, video-conferencing for telemedicine, the leveraging of data generated by M2M devices and sensors or Cloud and Hosting services.

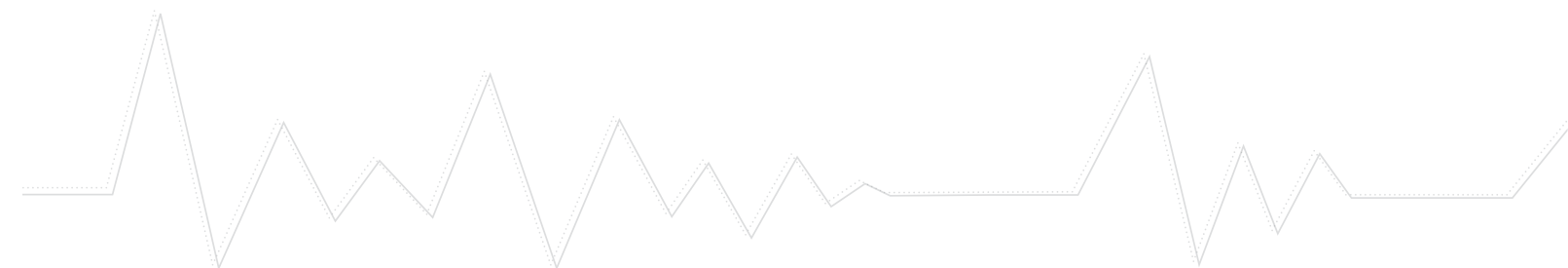
The industrial internet is a 'catch-all' phrase intended to capture the emerging market for industrial machines that connect the physical and digital worlds.

The industrial internet enables firms to use software, sensors, M2M learning and other technologies to gather and analyse data from physical objects or from datasets to manage operations and in some cases to offer new, value-added services.¹⁷

Global enterprises are investing heavily in digitisation in order to drive efficiencies in the production and delivery of new and existing products and services across a range of sectors. At the same time, on the demand side, consumers and businesses are becoming more digitally connected, through the use of smartphones and other connected devices.

The ability to add sensors and data collection mechanisms to industrial equipment is driving exponential growth in the demand for machine-generated data.¹⁸ Growing capabilities in the area of data analytics will continue to improve information on the status of industrial equipment. This will have wide-ranging impacts. For example, more granular, real-time information will help predict and prevent machine breakdowns. This, in turn, will enable businesses to more quickly respond to customer demands for upgraded products and services.

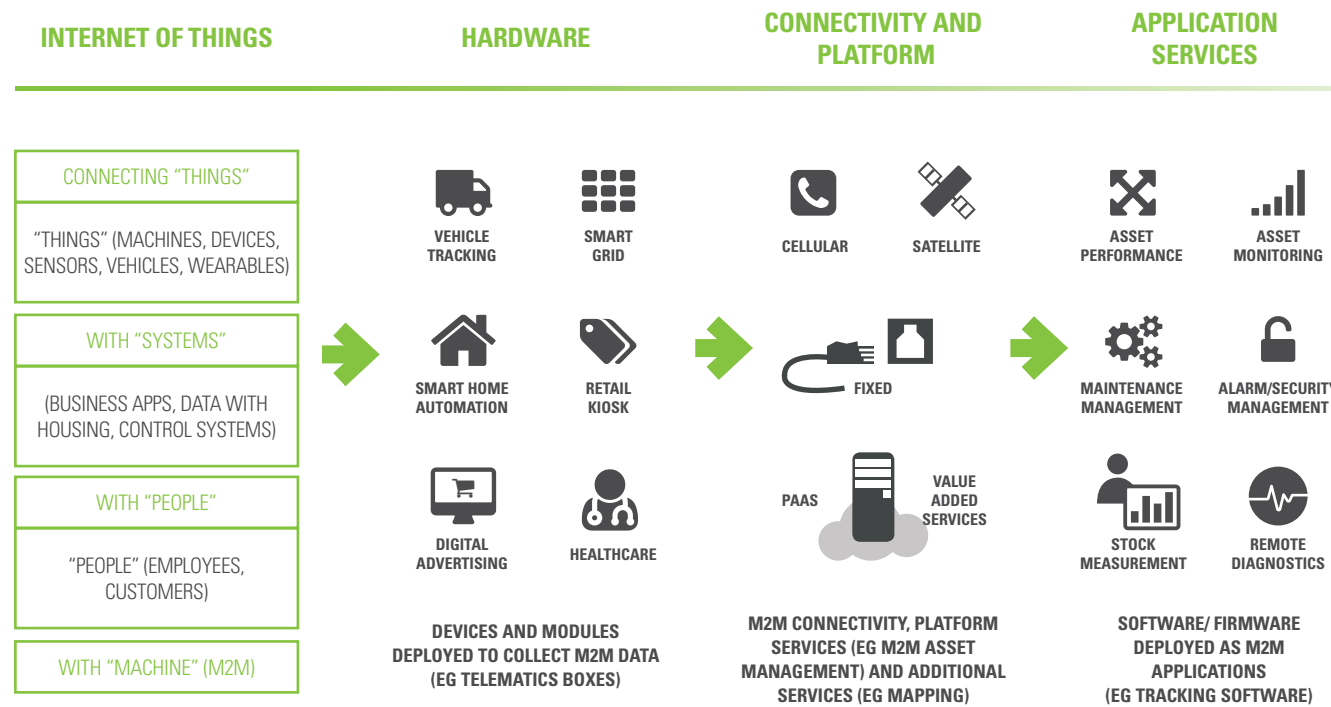
As these trends continue, it is likely that businesses will want products and services that are differentiated in terms of both price and quality. Much like consumers are used to paying different prices for different classes of rail or air travel, there are likely to be a wide variety of digital services where service providers will require a guaranteed or prioritised quality of service and customers will be prepared to accept a higher price for such a service. In other cases, it will be critical that communication networks are able to prioritise some ICT services over others, such as the police, fire, and emergency medical services.



Trends in the M2M market

The M2M market is best considered as a subset of a wider Internet of Things (IoT).¹⁹

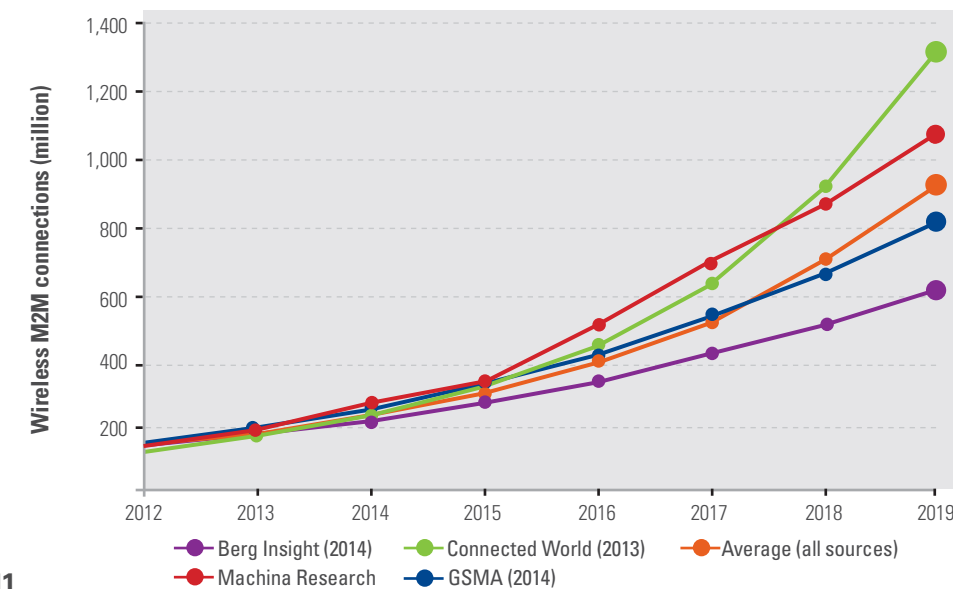
Figure 1: Overview of M2M and in the context of the Internet of Things



Source: KPMG

Machina Research estimates that there were 5.3 billion connected M2M devices at the end 2014, of which 72% were short-range connections (e.g. wi-fi).²⁰ Estimates of the number of cellular M2M connections in 2015 range from 255 million²¹ to 320 million.²² As the market has evolved, the number of firms involved in the M2M ecosystem has expanded, as has the range of application services available.

Figure 2: Cellular M2M connections globally, 2012-2019



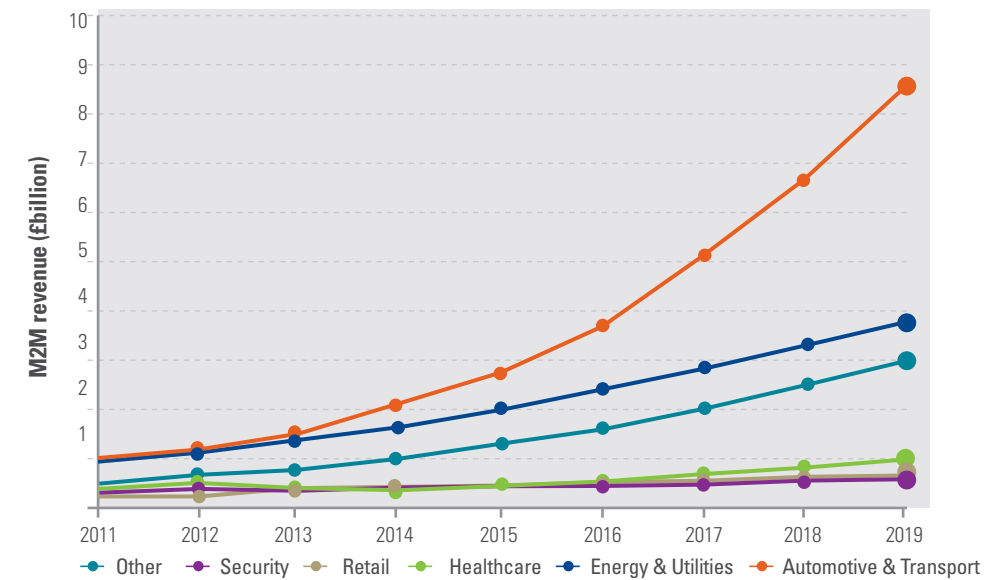
Significant growth is forecast in the number of cellular connections:

- approximately 310 million connections in 2015
- almost 950 million connections by 2019
- average annual growth rate (CAGR) of 32% over the next 4 years

Source: Berg Insight, Connected World, GSMA, Machina Research, KPMG analysis

Different industry sectors are adopting M2M technology at different rates. This trend is shown in Figure 3 below.

Figure 3: Global cellular M2M revenue by industry, 2011 – 2019 (forecasts start in 2014)



In this dynamic, growing international market, technology developments are being increasingly tailored towards the specific needs of different industry sectors. Total cellular M2M revenues are expected to increase at an average rate of 26% per annum, with automotive and healthcare leading the way (see Figure 3).

Source: 2011-12 vertical share as per Berg Insight 2012; 2013-19 vertical share as per Berg Insight 2014

HEALTHCARE

M2M connectivity is being used in healthcare predominantly to monitor diseases and symptoms.

It has been forecast that M2M communications will help treat 7 million patients globally by 2018, up from less than 350,000 in 2012.²³

ENERGY AND UTILITIES

M2M is being deployed in smart metering and grids. Smart meters are being rolled out internationally including in the US and much of the EU. The EU aims to replace 80% of electricity meters with smart meters by 2020 wherever it is cost effective to do so.²⁴

AUTOMOTIVE AND TRANSPORT

M2M has a variety of applications in the automotive sector including:

- remote monitoring and diagnostics;
- accident prevention; and
- placing an emergency call in the case of an accident.

It is expected that every new car will be connected in a variety of ways (a combination of embedded SIM, tethering and smartphone integration) by 2025.²⁵

Trends in the Cloud and Hosting services market

In essence, cloud computing is the delivery of computing services over the internet. Cloud and hosting solutions allow individuals or businesses to use software and hardware, in most cases managed by third parties, at remote locations.²⁶

“Global enterprise spending on cloud services and infrastructure could be as much as \$235 billion by 2017.”

The increasing adoption of IT in enterprises, and the growing volumes of data stored and shared, have brought with them often significant, and growing, overheads in the implementation of in-house computing systems. Time and finance invested in managing IT has increased exponentially alongside reliance on IT systems. Digitisation and data analytics have, in turn, become more important

to businesses. As businesses look for new ways to scale back on overhead and infrastructure costs, they are turning increasingly to leveraging the benefits of the cloud. Reflecting this, cloud-related investment has increased dramatically in recent years. A recent IHS report²⁷ suggests global enterprise spending on cloud services and infrastructure could be as much as \$235 billion by 2017.

The potential socio-economic benefits

The adoption of ICT services by industry is having a transformational impact. As adoption increases, the economic benefits that can be realised through their use are likely to grow further still. Economic benefits are wide-ranging and flow to a range of parties. Economic value added is created by the service providers, as well as generated by the users of the services. Positive economic benefits may be passed on to their customers and wider positive spillover effects accrue to society and the economy more generally.

For Cloud and Hosting services, we can expect to see:

- Improved efficiency and availability as clouds are based on grid computing. This means that the resources of many computers in a network can be applied to a single problem. It also means that the applications can rely on a high availability of IT architecture to minimise downtime.
- The ability to scale computing capacity on demand.
- Rapid deployment due to the use of standard, re-usable, and shared software and hardware. Both public and private clouds can provide self-service access to a shared pool of computing resources.²⁹

Further economic benefits cited in relation to cloud services include reduced IT capex, reduced IT staff headcount, improved business scalability, faster time to market for new goods and services,³⁰ more effective mobile working, higher productivity, and an improved ability to enter new business sectors and geographies.³¹

Percentage of CIOs that consider cloud computing as a 'crucial technology for customer engagement'



IN 2014, AN IBM STUDY²⁸ FOUND THAT 64% OF CHIEF INFORMATION OFFICERS (CIOS) INTERVIEWED MENTIONED IT AS A 'CRUCIAL TECHNOLOGY FOR CUSTOMER ENGAGEMENT', COMPARED TO 30% IN 2009



OF 479 ENTERPRISES INTERVIEWED WHO WERE ALREADY USING CLOUD FOR THEIR BUSINESS³²

81%
REPORTED LOWER IT COSTS



MAJORITY
10-20%
IT COST REDUCTION



12%
30% +
IT COST REDUCTION

CASE STUDY

ATLAS COPCO COMPRESSOR TECHNIQUE

Atlas Copco is a global provider of industrial productivity solutions that uses Vodafone global M2M communication services to monitor the performance and health of its compressed air products on customer sites around the world.

Atlas Copco offers its customers a suite of services which make use of M2M technology, including for maintenance, availability and energy use monitoring. These services can help improve machine efficiency, as well as lessening the risk of machine breakdown, and thus reducing costly production downtime for its customers. Using M2M to monitor machine energy usage can also allow its customers to manage and reduce their energy use, generating costs savings and carbon footprint reductions.

Sector specific examples of the economic benefits of digitisation

For M2M services, we have conducted analysis to estimate the economic value currently generated by M2M service providers. They contribute to the economy through generating economic growth via the value added to the inputs purchased from suppliers – Gross Value Added (GVA).³³

“**€2.5 billion:**
Estimated Gross Value Added (GVA) of the global cellular M2M market in 2014.”

We estimate that the total GVA of the global cellular M2M market was €2.5 billion in the year ended 31 March 2014 – comprising a direct contribution of €1.4 billion and an indirect contribution of €1.1 billion.³⁴

This figure is likely to grow significantly, consistent with the forecast explosive growth of M2M over the coming years.

M2M solutions are often not only used to deliver business benefits internally, but are increasingly being implemented in products and services sold to end customers to add value. Innovation in M2M has the potential to open up completely new market segments and enhance existing ones. For example, data analytics tools can be used to drive product performance through using M2M for remote diagnostics and device performance monitoring. This can help achieve efficiencies in M2M use and delivery.

The 2015 Vodafone M2M Barometer found that over 81% of M2M adopters are using M2M more than they were a year ago.³⁵ Over 40% of all respondents are using M2M to expand into new countries (including nearly half of respondents in the automotive industry).

This is consistent with findings in the equivalent 2014 report which found there has been a significant increase in the number of executives saying that M2M is helping them deliver more consistent services across multiple geographies.³⁶

CASE STUDY

RWE

RWE manufactures charging stations for electric cars. With more than 4000 charging points provided by RWE,³⁷ it has the most extensive network of charging stations in Europe. M2M communications in RWE's electric car charging stations allow for the transfer of data between the car and charging station. This helps to optimise the charging process which has the effect of a more efficient use of electricity.

M2M connectivity allows RWE and customers to remotely monitor the charging station; this allows RWE to change the configuration of the station when needed and also informs customers of their closest available station. The use of M2M also enables efficiency improvements and provides the grid operator with information which enables it to optimise the energy flow, depending on the car charge status and for how long the car will be plugged in to the charging station.

For RWE, the use of a global SIM enables a standardised manufacturing process, irrespective of where the station is to be shipped, which results in significant efficiency savings and quicker delivery of its stations to customers.

In order to highlight the significant size of the economic opportunity that digitisation brings, we have examined trends in digitisation across a number of key sectors.



AUTOMOBILE

KEY SECTOR DEVELOPMENTS AND TRENDS IN DIGITISATION

The global automotive industry was worth an estimated \$800 billion a year in 2014. The global connected car market is expected to grow an average 18% per year and be worth €40 billion by 2018.³⁸

Suppliers are making substantial investments in ICT technologies to increase connectivity and autonomy.

The level of connectivity and autonomy is expected to increase over the next 10 years, with capabilities ranging from interactive media, technologies to assist with managing traffic jams and intersections to eventually semi or fully autonomous driving cars. These rely on both sensor and mobile connectivity based solutions, depending on the specific technology deployments.

In the UK, the number of connected cars is expected to increase significantly from 50% penetration today:

- By 2025, it is forecast that virtually all cars will be connected
- Based on current trends, a 25% penetration of fully autonomous driving vehicles is expected by 2030³⁹

ESTIMATES OF THE ECONOMIC BENEFITS

KPMG⁴⁰ estimates significant economic impacts of connected and autonomous vehicles in the UK by 2030, unlocked by connectivity and increasingly autonomous vehicles:

- **£51 billion** value added annually in the UK by 2030 (at 2014 prices)
- **+1%** impact on UK GDP
- **345,000** total jobs created in UK automotive manufacturing and adjacent industries

Cisco⁴¹ estimates:

- annual costs of personal mobility to businesses and society of **€2.4 trillion in the US alone**⁴²...
- but, these costs could be **reduced by an estimated 40%** due to reduced crashes and pollution, and improved parking, road congestion and traffic services

Cost to society of road accidents is approximately €130 billion per year in Europe with 90% of these accidents involving human error. The European Commission considers these errors can be avoided with connected cars and communications between vehicles and infrastructure and ultimately with automated driving.⁴³

ESTIMATES FOR THE US, EUROPE AND JAPAN⁴⁴, SUGGEST THAT VEHICLE CONNECTIVITY WOULD LEAD TO:

7% less



TIME STUCK IN TRAFFIC (THEREBY INCREASING PRODUCTIVITY)

8% fewer

CRASHES

10% lower

TRAFFIC/ROAD/TOLL OPERATION COSTS

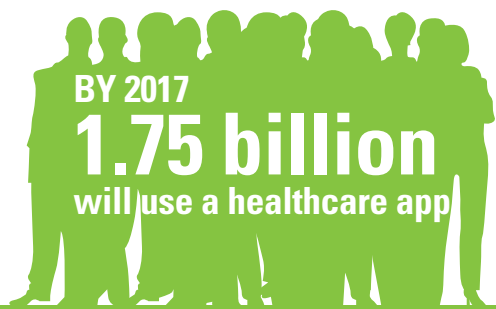
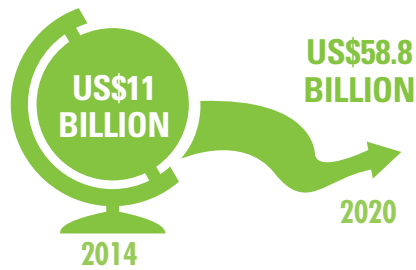
3% reduction

IN CARBON DIOXIDE EMISSIONS



M-HEALTH SOLUTIONS ARE SUPPORTING INDIVIDUALS

GLOBAL VALUE



KEY SECTOR DEVELOPMENTS AND TRENDS IN DIGITISATION

Rapidly growing and ageing populations and an increase in chronic illness are placing pressure on healthcare systems in many countries. The widespread adoption of ICT is expected to:

- increase prevention through more people actively monitoring their own health;
- allow remote treatment of those who fall ill; and
- reduce re-admissions as technology helps them and their care givers look after themselves.

M-health, telehealth and telemedicine solutions are transforming the relationship between doctor and patient.

Faster internet connections and improved technologies coupled with the wider use of electronic medical records are facilitating the digitisation of the health market on the supply side:

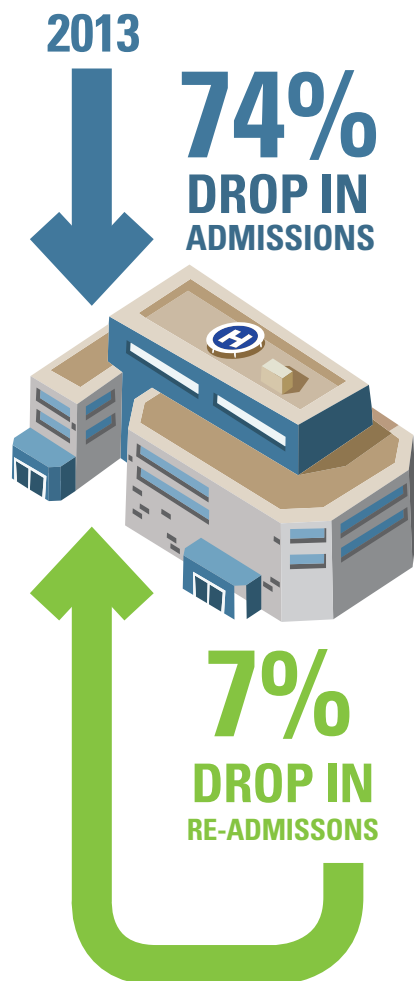
- IHS predicts that the US telehealth market will grow to \$1.9 billion in 2018 from \$240 million in 2013, an annual growth rate of 56%⁴⁵; and
- In 2013, an estimated 52% of US hospitals utilised telehealth solutions, with a further 10% beginning the process of implementing them.⁴⁶

Global M2M healthcare revenues are expected to be \$4.5 billion by 2018. M2M solutions are being deployed in healthcare in a wide range of uses to facilitate remote patient monitoring appointment reminders and medication compliance checks.



M-HEALTH SOLUTIONS ARE IMPROVING PATIENT OUTCOMES

A study in the US carried out by Vidant Health, which started a program of remote health monitoring in February 2012 found:



ESTIMATES OF THE ECONOMIC BENEFITS

Remote patient monitoring is projected to result in global cost savings of up to \$36 billion by 2018.⁴⁷

Telehealth initiatives across Canada are estimated to have saved:

- CAD \$70 million in personal travel costs; and
- CAD \$55 million for the Canadian health system.⁴⁸

In the UK, in 2011 the Lancashire and Cumbria Care Trust launched a large-scale telestroke service across the region allowing consultants to assess patients for thrombolysis treatment by video-link. This has led to significant benefits including:⁴⁹

- faster patient diagnostic services which help reduce the chance of disability and death;
- 24 hours a day provision of a thrombolysis service; and
- estimated cost savings for the North Cumbria University Hospitals NHS trust of £3.9 million a year for the next five years.

M2M connectivity is increasingly used by hospitals to remotely monitor patients' conditions, such as blood sugar levels and heart rates. In the US, Vidant Health, which started a program of remote health monitoring in February 2012, has seen significant benefits for the 600 to 700 patients enrolled in the scheme. The benefits include:⁵⁰

- a 74% decline in hospital admission for these patients in 2013 and a further 54% decline in the first eight months of 2014; and
- a 7% drop in readmissions within 30 days for those with congestive heart failure.

The role of government policy in stimulating industry digitisation

FINANCIAL SERVICES



USE OF ICT IN THE FINANCIAL SECTOR

BY 2019
1.75
BILLION USERS

BY 2019
32%
GLOBAL ADULT POPULATION
USING MOBILE BANKING

KEY SECTOR DEVELOPMENTS AND TRENDS IN DIGITISATION

One area in which banks are increasingly investing is the use of videoconferencing at ATMs and on mobile devices. Video banking can allow banks to “expand the reach and convenience of customer engagement in a relatively low-cost fashion.”⁵¹ A number of banks are using video conferencing facilities in branches and on mobile in an effort to achieve these benefits.

- In the US, Bank of America has partnered with Cisco to offer video conferencing in 500 of its branches.⁵²
- Citibank started to rollout ATMs enabled with video conferencing capabilities across Asia in 2013.⁵³
- In the UK, Barclays rolled out its ‘video banking’ service in 2014 which allows customers to have a face to face conversation with an advisor over mobile, tablet or computer.⁵⁴

ESTIMATES OF THE ECONOMIC BENEFITS

There are a number of benefits associated with the banks’ move towards videoconferencing instead of face-to-face appointments at banks. These include:

- better customer service at a lower cost; and
- lower security costs and less paperwork associated with ATMs compared to traditional bank branches.

THE EC HAS ESTIMATED THAT eCALL COULD

CUT EMERGENCY RESPONSE TIMES



40%
IN URBAN AREAS

50%
IN RURAL AREAS

Effective government policy is likely to play an important role in fostering the digitisation of industry. Acknowledging this, policymakers and regulators are working to develop frameworks to drive growth and stimulate industry digitisation to achieve wider policy objectives.

Some examples of the role of government policy in stimulating digitisation are set out below:

- The creation of a connected EU digital single market is one of the ten priorities set out by European Commission President Jean-Claude Juncker. It is estimated that a single market will drive an additional €250 billion in growth.⁵⁵ Key focus areas include (1) promoting the digitisation of industry, (2) the development of global standards and interoperability, (3) making the most of the data economy and cloud computing and (4) leveraging ‘big data’ through new initiatives to promote the ‘free flow of data’ and a European Cloud.
- In India, Prime Minister Narendra Modi has initiated the ‘Digital India’ programme to transform India into a digitally empowered society and knowledge economy.⁵⁶
- Policies are in place to drive energy smart meter rollout in a number of countries including across Latin America, the Middle East and Africa, the US, China and Japan.⁵⁷ Smart metering aims to improve the communication channel between consumers and utilities to better match the supply and demand of energy use. Consumers can manage their energy use by accessing real-time information about their usage and be billed based on their actual energy consumption rather than on an estimation. For their part, utility companies can manage the supply of energy to meet the dips and peaks in energy demand. The EU aims to replace 80%⁵⁸ of electricity meters with smart meters by 2020, resulting in 200 million smart meters for electricity being installed across the EU by that time. It is estimated that smart meters and grids can:
 - reduce the EU’s emissions by up to 9%;
 - provide average energy savings of 3%; and
 - generate total cost savings of €309 per electricity metering point, split amongst consumers, suppliers and distributors.
- In April 2015, the European Parliament voted in favour of regulation requiring all new cars to be fitted with eCall by April 2018.⁵⁹ eCall is an application that relies on M2M connectivity to automatically contact the nearest emergency centre in the event of an accident.

These examples show a range of positive developments across the globe where the aim is to stimulate the demand side of the market to promote greater digitisation of industry. As set out earlier in this report, there are clear socio-economic benefits associated with the use of ICT services by businesses. The more policy makers and regulators can stimulate, rather than constrain, the digitisation of industry, the greater the potential to realise these benefits.



Regulatory threats to industry digitisation

Many national and regional policy makers and regulators are currently developing and/or modifying their regulatory frameworks to cater for the growing use of ICT services by enterprises. However, getting the correct regulatory settings is challenging given the fast moving nature of the market. Technological advancements are rapidly changing the nature of existing services and creating new commercial opportunities for services that previously did not exist.

The stakes are high: decisions made by regulators now can have significant impacts on the range, price and quality of ICT products and services available now and in the future. Regulations can also have a major influence on the level of industry investment as well as the ability of businesses to deliver the raft of socio-economic benefits promised by industry digitisation.

'Net Neutrality' regulations

THE REGULATORY ISSUE

Over the last few years, policy makers have faced calls to introduce 'net neutrality' rules that seek to force Internet Service Providers (ISPs) to treat all data on the internet equally. As a result, net neutrality rules are being proposed, or have been introduced, in a number of countries including in the US, EU, Netherlands, India and Chile.⁶⁰

“There are likely to be important differences between the needs of consumers and businesses in terms of internet access and use.”

“There is a risk that applying net neutrality regulations that fail to take into account the specific needs of businesses will threaten the viability of a wide range of new and innovative ICT services.”

However, the details of these rules differ widely, depending, in part, on the nature of competition in each country. For example:

- In the UK, the approach has been to promote internet access based on a 'best-efforts' public internet. This is intended to ensure that network operators carry all traffic on more or less equal terms whilst also allowing them to offer managed services, where certain traffic can be prioritised. Broadband providers agreed a voluntary traffic management transparency code in 2011.⁶¹
- In the Netherlands, net neutrality regulations go further by effectively prohibiting specialised or prioritised services by ISPs on the public internet.
- In the US, where there is less competition at the wholesale level, the net neutrality debate has been focused on ensuring that retail ISPs are not able to favour one type of data over another on their network. The latest rules only apply to retail internet services for consumers with wholesale and business services exempt from the regulation.⁶²
- In the EU, agreement has been reached on the details of a new draft law on net neutrality, which, among other things, allows internet operators to offer specialised services in certain circumstances.⁶³

There are likely to be important differences between needs of consumers and businesses in terms of internet access and use. Regulations aimed at addressing consumer protection matters (such as a ISPs' policies on blocking and throttling of content) may have less relevance for business customers. In addition, enterprises may wish to offer a range of ICT services to their customers that rely on differential quality of service. For example, videoconferencing for a telemedicine consultation over the public internet may require the network provider to prioritise this service over others (such as gaming) in order to deliver the service demanded by the customer. There is a risk that applying net neutrality regulations that fail to take into account the specific needs of businesses will threaten the viability of a wide range of new and innovative ICT services.

The ability of network operators to offer differentiated quality of service for ICT applications (including M2M) will depend on their ability to actively manage network traffic, including the prioritisation of some services over others. Net neutrality regulations that prevent or restrict this are likely to have a significant impact on the ability to meet customers' requirements. Also, a 'patchwork quilt' of different net neutrality requirements across the globe could significantly impair a provider's ability to configure a consistent multi-country service.

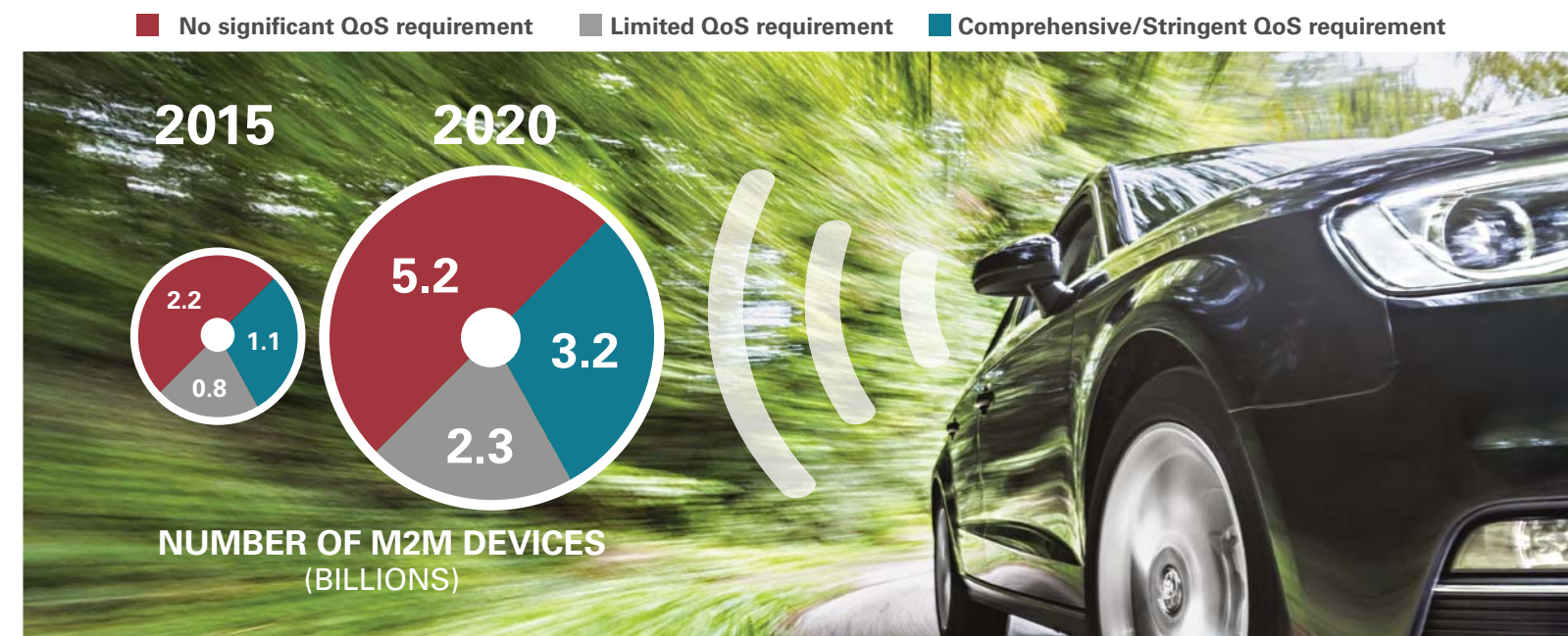
SERVICES THAT COULD BE IMPACTED BY NET NEUTRALITY RULES

Net neutrality regulations where the scope extends to business ICT services have the potential to have far-reaching impacts on the development of the market. This is because of the wide range of business services in the future that are likely to require differentiated quality of service over communication networks.

For example, videoconferencing requires a high guaranteed quality of service. It is likely that videoconferencing will be increasingly used in innovative ways to deliver services to customers across a number of industry sectors. For example, in the health sector videoconferencing could be used to deliver remote patient consultations in order to reduce costs and improve patient outcomes. In the banking sector, videoconferencing within branches or at ATMs could deliver personalised services (including bespoke financial advice) to a wider population of customers than currently available. Videoconferencing has been widely reported to lead to significant benefits to enterprises including operational efficiency and cost reduction.⁶⁴ The value of the global video conferencing market is expected to grow from \$3.3 billion in 2014 to \$6.4 billion in 2020; an average annual growth rate of 9.4% over this period.⁶⁵ This market may be at risk from net neutrality regulations that result in restrictions on network operators from offering businesses differentiated quality of service ICT products over the public internet.

A range of M2M application types will also require different levels of quality of service (see below).

Forecast trends in the number of M2M devices, by QoS requirements, 2015 and 2020⁶⁶



Examples of M2M services requiring differentiated Quality of Service



Low QoS

- Consumer white goods
- Fitness/training
- Street Lighting
- Vending machines
- In-Vehicle entertainment and internet access
- Modems, Routers & Femtocells



Medium QoS

- Vehicle Diagnostics/Navigation
- Roadside assistance
- Pet tracking
- Connected medical dispensers
- Fire alarms
- Smart Cities
- Public transport applications
- Residential Heating, Ventilation and Air Conditioning devices



High/Stringent QoS

- Smart Meters (Water, electricity, Gas)
- In-vehicle congestion/toll devices/emergency call services
- Stolen vehicle recovery
- Usage-based insurance (e.g. for vehicles)
- Clinical remote monitoring applications (e.g. heart monitors)
- Electronic point of sale

Source: Machina Research (2015), DNA of M2M, www.machinaresearch.com; Machina Research and Aegis Spectrum Engineering for Ofcom (April 2014), M2M applications characteristics and their implications for Spectrum

For some M2M products, customers are likely to place a high value on real-time/high-quality connectivity over communication networks (such as the ability of a M2M device to send messages to hospital staff when a patient needs emergency treatment).⁶⁷ Similarly, in energy smart grids, M2M communications can be used to deliver real time monitoring information to improve grid efficiency and to help reduce the likelihood, and duration, of power outages (as well as reduce carbon usage).

Enterprise customers interviewed as part of this study noted the importance of having high QoS for their M2M devices and the benefits that this delivered through their M2M applications. They were concerned that this may be impacted by net neutrality regulations.

Machina Research estimates that the number of M2M devices requiring some form of differentiation of quality of service is likely to grow significantly over the next few years making up over 50% of all M2M devices by 2020. Those M2M devices requiring comprehensive or stringent Quality of Service (QoS) standards are estimated to increase from 1 billion to 3 billion units.⁶⁸

Source: Machina Research (2015), DNA of M2M, www.machinaresearch.com.

CASE STUDY

MAHINDRA REVA

Mahindra Reva is currently India's only electric car manufacturer and launched India's first connected car in March 2013, with the mobile carrier connectivity services being provided by Vodafone. All of Mahindra Reva's cars are online and connected to their server.

Mahindra Reva uses a telematics platform enabling a central diagnostics team to remotely monitor vehicle performance data in real time. This allows the maintenance team to understand the root cause of the performance issue and quickly address many issues over-the-air. This is a significant benefit as it reduces the time to debug faults, particularly given that it indicated that service centres spend approximately 60 -70 per cent of their time on establishing the root cause of faults.

Therefore M2M capabilities with real time monitoring capabilities have allowed Mahindra Reva to be more efficient and lower costs.



Emergency services are also likely to value ICT services offering prioritised network access during an emergency where real-time data and information will be of critical importance:

- Fire rescue teams of the future are likely to require short, high bandwidth bursts of data to receive a 3D image of a burning building in a fire engine so they can familiarise themselves with building layouts before entering. Coastal maritime rescue teams will have similar needs.
- Prioritised communications is likely to be necessary as fire and rescue teams expand the use of connected drones to monitor emergency situations, for example, in a hostage situation, riot or natural disaster. As Cisco has observed:

“With the convergence of internet technologies and broadband wireless communications, mission-critical services for public safety emergency communications are undergoing tremendous change and growth. However, challenges and requirements are increasing for public safety and [for] those organizations responsible for providing network services to address the increasing complexity across mission-critical voice, data, and video communications.”⁶⁹

IBERDROLA

CASE STUDY

Iberdrola, a multinational utility company, currently uses M2M connectivity in its data concentrators (Iberdrola's meters are connected directly through electric wire, as part of its Power Line Consumer initiative). These are being rolled out in Spain to reach 11 million customers and cover 40% of the country by 2018. Iberdrola also plans to use M2M connectivity in its energy grid in Spain to enable real-time monitoring. While the M2M model is still evolving to meet the requirements of smart grid customers, Iberdrola hopes to eventually leverage M2M to become one of the solutions to achieve the quickest and most efficient way to deliver energy to customers. It will also be used to identify and rectify problems in the energy grid. For example, in case of an emergency, like adverse weather conditions, it is essential that Iberdrola has real-time M2M services in place to help restore electrical supply and reduce energy downtime, particularly if identified problems can be fixed remotely using M2M connectivity.

Iberdrola considered that, for utility companies, prioritised services are critical to ensuring real-time connectivity and full reliability to provide a high quality energy supply to its customers. It could also allow customers the flexibility in the future to use applications to control and manage their energy supply.

The potential socio-economic impact of net neutrality regulations

It is forecast that by 2020 over 50% of M2M applications (nearly 5.5 billion devices) will require some form of differentiated QoS.⁷⁰ Many of these devices will require access to fixed and mobile communication networks in order to provide services to customers. Hence, there are significant socio-economic impacts from net neutrality regulations that restrict the ability of network providers from offering differentiated quality of service for business services.

Regulatory restrictions on differentiated QoS are likely to impact the use of ICT services in a wide range of sectors. In their report for Ofcom, Machina Research and Aegis defined the types of services likely to require priority access to connectivity based on a range of customer requirements including:

- security: whether the data sent to or from the application needs to be subject to security measures, (e.g. encryption);
- criticality: the importance of the data sent to or from the application;
- sensitivity to delay: the impact on the overall service of a delay in receiving or transmitting data; and
- sensitivity to error: the impact on the overall service of communication errors, leading to partial or full loss of data sent or received.⁷¹

In the automotive and energy industries, some of the M2M applications that are likely to rely on high quality of service requirements include:

- electricity (smart metering);
- in-vehicle congestion & toll devices;
- stolen vehicle recovery;
- in-vehicle emergency call system; and
- usage-based insurance.⁷²

Machina Research⁷³ forecasts that, taken together, these 5 applications alone would account for over 4 billion revenue generating units globally by 2024

The economic benefits associated with these and a host of other ICT applications may be put at risk if requirements for differentiated QoS can no longer be met as a result of regulatory restrictions. The potential lost economic benefits could include:

- the reduction in energy emissions that could be achieved through smart meters and smart grids (estimated at 9% of emissions in the EU);⁷⁴ also the ability of smart grids to increase infrastructure capacity by up to 30% to meet growing demand;⁷⁵
- the cost savings and improved customer service realised through the increased use of videoconferencing in banks (a number of banks are moving towards videoconferencing in branches and over mobile);
- improved patient outcomes and significant cost savings achieved through telehealth (a market estimated to be worth \$240 million in 2013 and could be worth as much as \$1.9 billion by 2018 in the US alone);⁷⁶
- substantial GVA and employment generated by the connected/ autonomous car market (estimated to increase UK GDP by 1% by 2030⁷⁷) in addition to the reduced congestion, accidents and carbon emissions.⁷⁸

“The economic benefits associated with a host of ICT applications may be put at risk if requirements for differentiated QoS can no longer be met as a result of regulatory restrictions.”

Numbering and Licensing rules impacting global M2M services

The regulatory approach to M2M globally is evolving.⁷⁹ Some regulators are seeking to agree globally or regional consistent approaches, while others appear to be applying legacy regulations crafted to address consumer issues.

We have identified examples where specific regulations are having adverse impacts on the provision and use of specific M2M services. One such example is the application of national numbering regulation which can affect the use of a Global SIM.⁸⁰ Another is a licensing requirement that governs the location of certain types of infrastructure needed for service provision.

A Global SIM uses 'supranational' numbering allocated by the ITU for use in multiple geographies, reflecting the fact that enterprise customers typically require M2M services to be deployed in a number of different countries. Historically, it is the case that electronic communications services (in particular SIM based electronic communications services provided to consumers) have been provided on a national basis, using national numbering.⁸¹ Regulatory obligations have also tended to flow from the use of national numbering and are likely to have been developed with consumer protection principles in mind. For example, number portability has been implemented in many countries in order to facilitate the ability of consumers who wish to change service providers without have to give up their number. However, given that numbers for M2M services are not allocated to people, it is less obvious why number portability obligations should be imposed on M2M services. Despite this, a recent CEPT report identified several European countries where number portability obligations have been applied to numbers allocated to M2M services.⁸²

It is not only prohibitions on non-transitory roaming for M2M that create barriers to provision. Licence regulations governing the location of the infrastructure for service provision can also inhibit flexibility in the choice of M2M deployment models in certain industry sectors.

Equally, consumer focussed regulations in place which also affect the M2M market, for example Know Your Customer (KYC) obligations for all SIMs (including those used for M2M purposes such as vending machines), can also prove challenging and add to costs.

BRAZIL

There are specific provisions in the Brazilian national numbering plan which do not envisage the use of non-Brazilian numbering for SIMs which are used in Brazil on a non-transitory basis.⁸³

As a result, it is necessary to use a SIM with numbering from the domestic national numbering plan in order to roll out an M2M solution in Brazil. A global deployment model cannot be used. In practice, this means M2M services being provided via a locally licensed operator.

SAUDI ARABIA

In Saudi Arabia the licence to provide Automated Vehicle Location (AVL) Services (which has particular relevance for connected car functionality) states:

"The infrastructure for service provision including, but not limited to, elements such as transmitters, receivers, system administration equipment, subscribers' data storage devices, servers, call centres etc. used to provide the service must be located within the Kingdom."⁸⁴

INDIA

The National Telecom M2M Roadmap envisages the prohibition of foreign SIMs for M2M in India. The Roadmap further states:

"the government is of the opinion that foreign SIM should not be permitted in the devices to be used in India."⁸⁵

MIDDLE EAST

There are signs of an emerging trend in Middle Eastern states, involving the replication of the Saudi Arabian AVL regime.

For example Oman has adopted an almost identical condition in its licence for the provision of "Automated System[s] for Vehicle Management Service."⁸⁶

Such provisions create significant uncertainty when configuring a connected car solution across multiple markets that utilises centrally hosted network architecture.

ITALY

The use of E.164 numbers for M2M is currently under review.⁸⁷

GERMANY

The use of E.164 numbers for M2M is currently under review.⁸⁸

BELGIUM

The numbering regulations for M2M is currently under review.⁸⁹

UK

The UK regulator, Ofcom, is supportive of the use of supranational numbering for M2M, as reflected in its statement on "Promoting investment and innovation in the Internet of Things."⁹⁰

EUROPEAN UNION

A European Conference of Postal and Telecommunications Administrations (CEPT) report⁹¹ in 2013 recommended that the extra-territorial use⁹² of E.164 numbers should not be allowed, citing issues such as scarcity, competition and portability, tariff transparency and emergency calling. The report did, however, note that M2M could be considered as an exception.⁹³

The potential socio-economic impact of numbering and licensing rules on global M2M services

There is tangible evidence from Vodafone of the economic impact of regulations preventing the use of the Global SIM and Vodafone's Global Data Service Platform (GDSP) in Brazil. This provides an informative case study of how such regulations impact on service providers, enterprises and the wider economy.

CRF HEALTH

CASE STUDY

CRF Health, is a global leader in electronic Clinical Outcome Assessments (eCOA). It mainly uses M2M connectivity to send mobile data during clinical trials and to track the related fees. CRF Health has only used Vodafone's Global platform in a limited capacity and has not utilised the platform for more comprehensive reporting, monitoring or analysing of its services. However there are plans to do this in the future.

CRF Health highlighted cost and time savings to its business through the use of the Global SIM as compared to its previous solution. Previously, CRF Health had to wait some time, often days and even weeks, for SIMs to be activated by a third party. Additionally the SIM card needed to be in an active mode prior to shipping, which led to additional costs. Now, with the Global SIM, the SIM is automatically activated from the first data transfer; this has led to cost and time savings for CRF Health and its Customers.

The use of a single tariff has also led to positive outcomes for its customers. CRF Health can now provide accurate and predictable fees of particular trials and studies before they take place which has significantly improved its pricing model and allows customers to budget more effectively.

There are increasing risks, in a range of countries, that these could become more widespread in future as M2M regulation develops. This is the case in the EU, for example, where a number of Member States have consulted, or are in the process of consulting on a range of numbering regulations which could restrict the provision of M2M services via a Global SIM.

If this were the case, the economic impacts could be significant. The scale of the impact would depend on the number of jurisdictions imposing regulatory barriers, the scale and market potential of M2M services in each and the M2M solution that Vodafone would be required to implement to serve its customers as an alternative to the Global SIM and GDSP.

The economic impacts that would apply to Brazil as well as other countries that imposed similar regulatory restrictions could include:

- reduced direct economic contributions by service providers, resulting from the lost M2M revenues, and high set-up costs and increased operational costs developing and migrating customers to an alternative deployment model for M2M provision in jurisdictions where the global solution could no longer be used;
- reduced economic contributions of M2M customers associated with any lost revenues over the period of transition from a Global SIM to the alternative M2M solution and as a result of any increased costs involved in the use of an alternative M2M SIM solution (e.g. production, testing and monitoring costs);
- reduced economic contributions of suppliers in the value chain for both service providers and M2M customers as a result of their reduced activity over the transition period;
- less investment and innovation by M2M services users over the transition period; and
- reduced economic spillover benefits as a result of reduced M2M service provision over the transition period and lost benefits to customers from the use of services that deploy GDSP.

Vodafone's enterprise customers specifically highlighted the benefits to their business associated with the use of a single Global SIM in their installed base of multi-national M2M devices. The benefits that could be lost as a result of regulations preventing the use of the Global SIM include:

- efficiency benefits of being able to deal with a single provider to meet their needs across multiple countries;
- the coverage benefits of Vodafone's own global footprint (including that of its network partners);
- the ability to develop standardised global products without needing to tailor the production process to fit different national SIMs; and
- the associated time and cost savings.

Not having to change SIMs dependent on where the device is deployed was a particularly important benefit noted by the majority of Vodafone's M2M customers interviewed as part of this study. With a Global SIM solution, a single SIM can be embedded in all products during the manufacturing process, irrespective of where in the world the product will be sold. Companies we interviewed indicated that the ability to have one standardised manufacturing process, during which SIMs are embedded in every product, leads to time and cost savings in production. The Global SIM means that the end destination of the M2M device does not need to be taken in to account in the manufacturing process and SIM customisation does not need to occur.

Ultimately, it should be the enterprise customer that is the primary driver of the specific M2M deployment model, using the Global SIM or an alternative approach such as the GSMA's embedded SIM specification.⁹⁴ It is important that regulation does not unduly restrict the range of M2M deployment models available.



CASE STUDY

IMPACTS OF BRAZILIAN REGULATIONS PREVENTING THE USE OF A GLOBAL SIM

In order to comply with the Brazilian regulations governing the provision of M2M services, Vodafone had to develop and deploy a "local solution" to provide connectivity using numbering from the Brazilian national numbering plan via partnering with an existing Brazilian telecoms provider.

The direct impacts of this on Vodafone include:

- lost M2M revenues while the local solution was developed (approximately 2.5 years);
- additional cost associated with the development of a bespoke M2M solution for Brazil in conjunction with the local partner, including significant Capex;
- significant added complexity and time delays to develop, test and deploy the solution;
- higher operating costs on an ongoing basis.

If the regulations restricting use of the Global SIM for M2M were not in place, Vodafone indicated that its M2M solution could have been launched in Brazil with no additional cost or delay using the Global SIM and the GDSP, which is centrally controlled through the cloud.

Enterprise customers are also likely to be negatively impacted as a result of the regulatory requirements, in a number of ways including:

- lost revenues associated with their use of M2M connectivity in their products for the Brazilian market over the period of delay in deployment;
- additional costs and complexities associated with being required to use two SIMs in their devices (the Global SIM outside of Brazil and a local SIM in Brazil), including supply chain production costs, monitoring and testing costs; and
- loss of the service benefits associated with the GDSP.

More generally the Brazilian economy is likely to also have been negatively impacted by the regulatory restrictions resulting in delays to the deployment of M2M services by global enterprises. The economic contributions and wider economic spillover benefits associated with M2M use would not have been realised during this period. With potentially higher costs of M2M deployment, economic activity may be affected in the longer term. And with higher costs of M2M deployment, economic activity could potentially be affected in the longer term.

Data localisation regulations

CASE STUDY

ATLAS COPCO

Atlas Copco indicated that if regulations were introduced that prevented its use of the Global SIM it would pose significant challenges for it, in terms of adjusting the production process and changing the Global SIMs deployed in the installed base of devices.

It noted that some of its equipment has a lifespan of around 30 years; machines are often sold on second hand and it is not possible for Atlas Copco to know where the machine will end up when the SIM is installed in the production process. Some machines are also sold via dealers, or installed as an intermediary product in a manufacturing process. Devices can be shipped globally, particularly the smaller, lower value, high volume machines.

While technicians are deployed worldwide to maintain machines, it was highlighted that they are not IT technicians, therefore would require new, additional skills if SIMs were required to be installed and programmed for different jurisdictions. Atlas Copco also indicated that if regulations were introduced requiring different SIMs for different countries, i.e. it was not able to use the Global SIM, it would limit its M2M deployment to large regions, using large telecommunication providers, and it would not be able to deploy its M2M devices globally.

CASE STUDY

MSWIPE

Mswipe is an Indian company providing mobile payment services through the use of an M2M SIM. The Mswipe solution is based around a hardware device called the Wisepad that connects to a smartphone, tablet or PC via Bluetooth. Users can download the Mswipe application on their internet-enabled device and can accept payments from all major debit, prepaid and credit cards. Mswipe's gateway connections are optimized for 2G connections and payment details are sent via a Vodafone M2M SIM. Mswipe provides a bank-agnostic solution which allows small merchants to accept card payments using a mobile device and an M2M connection. The Mswipe terminal and connectivity allows for payments to be transferred quickly and directly to the merchant's bank account the next day.

Mswipe highlighted that the use of a Global SIM delivers significant benefits when it is rolling out solutions in different countries, particularly given the need for cross border acquirers to have a unified platform. Where it has had to develop local solutions this has added to logistical costs and reduced the ability to achieve economies of scale.

In a post-Snowden world, issues of data protection, security and law enforcement access are an increasing focus for policymakers, regulators, companies and individuals worldwide.

“Many countries, particularly in emerging markets, already limit the export of certain types of data through legal requirements or government authority licence obligations.”

Growing concerns around data privacy, data protection and state surveillance have prompted a number of governments and regulators to call for restrictions on the transfer of data (including machine generated data) outside of national borders.⁹⁵ We note the important distinction between data localisation regulations (where there are stringent regulations on data leaving the country) and the range of regulations that exist on cross-border transfer of personal data (where transfers can occur only if certain obligations are met).⁹⁶

As the volumes of data generated and transmitted continue to grow, and as the integrity and security of that data comes under more focus, more countries may look at ways to ensure that data about their own citizens, or data that they perceive to have national security implications remains secure, protected, and available for access where necessary. Many countries, particularly in emerging markets, already limit the export of certain types of data through legal requirements or government authority licence obligations.

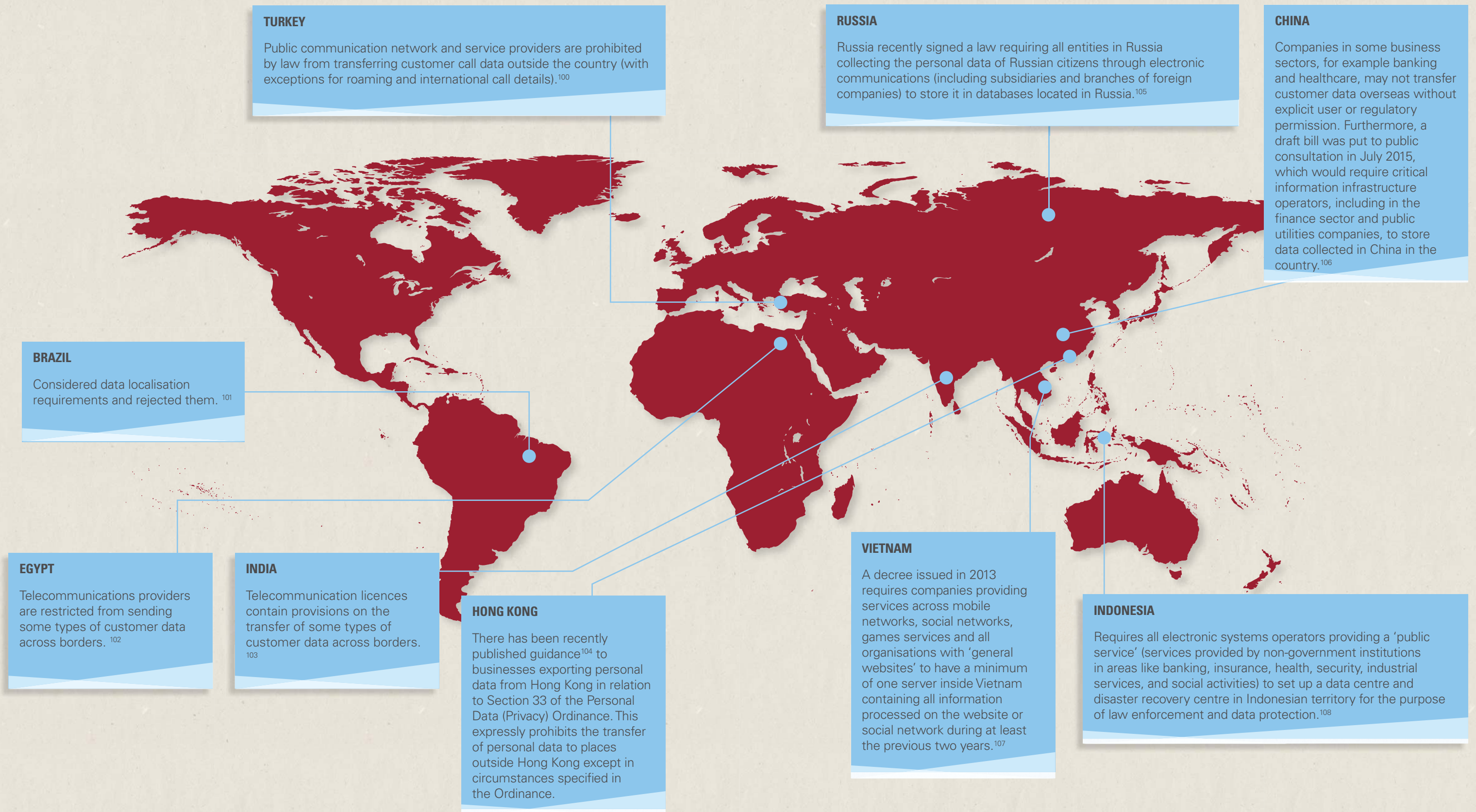
Some industry stakeholders have also identified an emerging perception in some countries that national 'data sovereignty' requirements are in place, even where they are not.⁹⁷

At the same time, there are some recent examples where industry agreed standards and self-regulatory initiatives have been introduced to address concerns around privacy and security. For example:

- one such industry standard is ISO/IEC 27018:2014, which establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment;
- the European Commission's recently established 'Alliance for Internet of Things Innovation' (AIOTI) has brought together many different companies in order to remove any barriers (e.g. interoperability, security) to the development of the 'Internet of Things' and the Digital Single Market; and
- the EC has also established the EU Rolling Plan for ICT Standardisation which aims at structuring governance of standardisation and pulling market forces towards convergent objectives.⁹⁸ A European Multi-Stakeholder Platform on ICT Standardisation has also been established bringing together all key stakeholders (including European Standardisation Organisations, the main international ICT bodies, industry and consumers) to achieve more coordinated action.⁹⁹

These examples provide evidence of proactive measures taken by industry players to provide alternative measures to data localisation laws and regulations in order to address legitimate public policy concerns.

Data localisation requirements in selected countries



The potential socio-economic impact of data localisation requirements

In a globalised information economy, providers of ICT will often deliver their products and services using centralised platforms and architecture, located across multiple jurisdictions. Therefore, any requirement for data localisation can impede effective service delivery as well as increasing costs and altering investment incentives. The economic consequences of this can be significant.

The European Centre for International Political Economy (ECIPE)¹⁰⁹ found that data localisation requirements and related data privacy and security laws could have substantial negative economic impacts:

- GDP losses ranging from 0.1% (India) to 1.7% (Vietnam); and
- negative impacts on domestic investment, exports and welfare.

Similarly, a 2013 report¹¹⁰ estimated that if cross-border data flows were seriously disrupted in the European Union it could result in:

- a reduction in EU GDP of 0.8% and 1.3%; and
- an 11% reduction in EU manufacturing exports to the US.

There is also evidence from Vodafone's customers of the economic impact of data localisation requirements.

CASE STUDY

CA TECHNOLOGIES

CA Technologies (CA), a large global independent software corporation, provides cloud services to Vodafone and its enterprise customers. One of the main products offered is Portfolio Project Management (PPM) which is a software as a service solution that helps Vodafone manage its solutions portfolio and validation process. PPM is an important service, as it manages data relating to both individuals and projects.

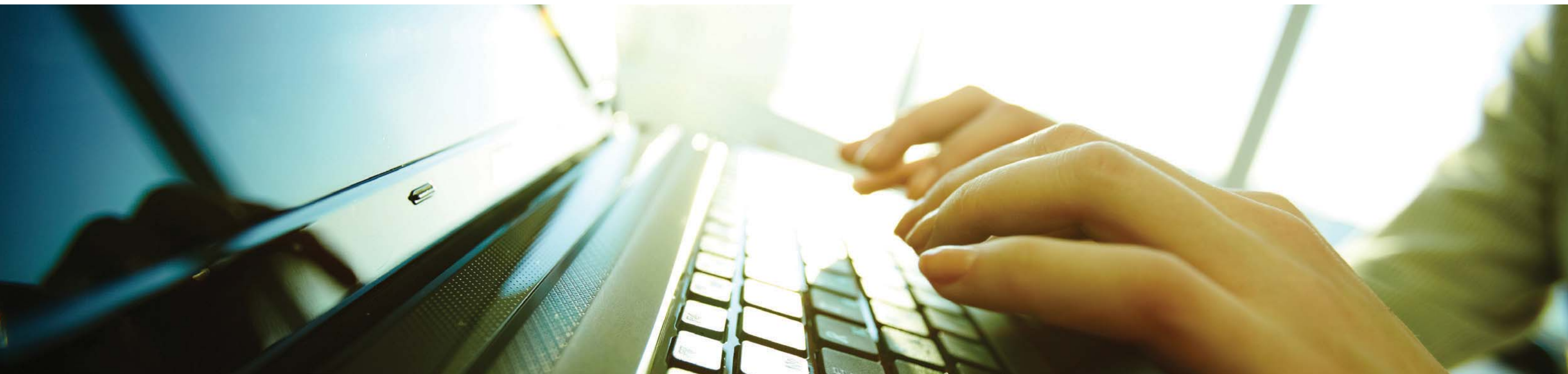
CA is keen to consolidate and provide its cloud services from a centrally managed platform to benefit from cost efficiencies it can pass on to its clients. However, it is facing constraints to this due to demands – from both customers and regulators – for data to be “on-shored”.

Regulatory barriers, leading to the need to support customers locally, result in CA facing a range of additional costs associated with developing local solutions:

- Each local solution incurs set-up and running costs.
- If CA were able to deliver all services through its central platform in Munich, costs would be significantly lower as CA would only need sales staff to sell the product in each local market and not the technical support staff that would be required for a local solution.
- The ability to achieve economies of scale are also inhibited where local solutions are deployed. Large customer volumes are required to achieve an acceptable return on investment.

Where local markets are small, it may not be commercially viable for CA to set up a separate solution in each market. And even where a data centre can feasibly be built, the extra costs associated with it will drive up costs for customers which could make the solutions prohibitively expensive.

CA are currently working on mitigating this situation, driving down operational costs directly by developing the solutions and indirectly through leveraging service providers with local presence to achieve the needed economies of scale by combining other solutions.



Policy recommendations

The current trend of countries introducing data localisation requirements mean that the economic impacts of such requirements may become more widespread.

CASE STUDY

GE

GE highlighted the impact of EU Member States' inconsistent interpretation of EU data protection laws. When GE sought to open a shared data centre in Hungary, Hungary's interpretation of EU law meant that GE could not transfer data to US data centre in Hungary and then back out again without signoff from the "owners" of the data. The shared data centre was delayed for a year while negotiations took place.

CASE STUDY

JAGUAR LAND ROVER

Data localisation issues also increase compliance costs and in smaller markets particularly, these costs can be high compared to the potential size of the market and Jaguar Land Rover revenues.

Potential socio-economic impacts of data localisation rules, include:

- increased costs to service providers and customers resulting from the additional capex and operating costs (exacerbated by loss of economies of scale) associated with developing in-country data centres and platforms where multi-jurisdiction architecture was previously in place;
- reduced economic contributions of service providers linked to lost revenues from the range of products and services that they may no longer be able to provide if local architecture is required;
- reduced economic contributions from enterprises if data localisation rules (or the costs associated with complying with these rules) remove the commercial viability of their digitalised products within the market;
- reduced range of services available to customers, preventing them from realising the benefits associated with their use, (e.g. cost savings associated with expense management solutions and SIM monitoring and management through the GDSP); and
- increased complexity and cost to industry due to the lack of consistency across jurisdictions, which hampers moves towards greater digitisation.

A number of Vodafone's customers we interviewed expressed concern about laws that restrict data flows in jurisdictions where they operate, and the fragmented approach that may result. Concerns were not only about the impact on services they purchase from Vodafone, but also on services they can offer to their own customers.

CASE STUDY

PANASONIC

Panasonic, a multinational electronics corporation, purchases M2M services and unified communications from Vodafone. The unified communication solution combines mobile telephony, mobile data and fixed telephony set-up across Europe and is used across its European entities.

Panasonic indicated that a single unified communications solution across Europe results in cost savings. For example, the service allows its employees to place internal calls across its European entities at a lower cost, and provides a single number reach and an integrated call plan.

Although the solution is still being rolled out and not all Panasonic users have been integrated, Panasonic estimated that it had reduced its annual operational costs by approximately 25% (approximately €1m).

To achieve these benefits more widely, Panasonic is analysing the possibilities to roll out a similar solution in other parts of its business outside of Europe.

To recap, the key findings of our study include:

- Effective government policy is likely to play an important role in fostering the digitisation of industry. The digitisation of the business sector can deliver significant economic growth across a wide range of industries. In particular, industries such as Healthcare, Automotive, and Energy are likely to experience transformational changes to how products and services are produced and consumed. However, governments can do more to improve the global compatibility of public policy and regulatory frameworks.
- Supply-side regulatory restrictions have the potential to hamper the development of the market. There are risks of unintended consequence from 'consumer' style regulation being inappropriately applied to emerging ICT services vital for the digitisation of industry. For example:
 - a requirement for enterprise M2M applications to use numbers from the National Numbering Plan; and
 - 'net neutrality' regulations that restrict the offering of differentiated quality of service applications to enterprise customers.
- A globally inconsistent regulatory approach could result in higher costs and poorer quality of services for multinational enterprises. Examples highlighted in this report include:
 - geographic restrictions on where machine generated data can be stored;
 - regulations that restrict the transfer of customer data beyond country borders; and
 - an emerging perception in some countries that national 'data sovereignty' requirements are in place, even where they are not.
- Some self-regulatory approaches are emerging that may address potential regulatory concerns around privacy and security.

To address the major regulatory threats to the digitisation of industry (particularly for those firms offering services in a global market) we recommend that policy makers and regulators:

- aim to develop effective demand stimulation policies for the digitisation of industries. Policies should be tightly focused on achieving specific economic and public policy objectives (such as the use of smart meters to promote energy efficiency or regulations similar to eCall to reduce car accidents);
- ensure that 'net neutrality' rules allow business customers to obtain specialised services necessary to fuel the digitisation of industry. Net neutrality regulations should take into account the different needs of consumers and businesses. Regulations designed for mass market internet services should not be applied to the business market. We recommend that policy makers should either exempt relevant business services from the scope of regulation or include a sensible materiality clause to ensure that business services using the industrial internet (where the quality dimension is likely to be important) are not unduly restricted commercially;
- remove unnecessary restrictions within local numbering plans for using ITU supranational numbering resources for cross-border M2M applications (where such restrictions cannot be justified on economic or public policy grounds); and
- remove unnecessary restrictions on the transfer of machine and user generated data across borders (where such restrictions cannot be justified on economic or public policy grounds) and instead rely on internationally recognised regulatory standards on data protection and privacy (such as those that apply in the European Union).

Appendix

Key notes and assumptions

Gross Value Added (GVA) is the measurement of the contribution to the economy of an individual producer, industry or sector. It estimates the difference between the value of the goods and services produced and the cost of the inputs – such as raw materials – used to create those goods and services. GVA is used to estimate Gross Domestic Product (GDP) which is a key indicator of the state of the economy.

Our analysis of Vodafone's M2M economic contribution is shown in gross terms. We have not assessed the net contribution of Vodafone's M2M services. Therefore, the analysis does not take in to account what the people and other resources would have been used for if Vodafone did not provide these services.

Vodafone's direct economic contribution in terms of GVA associated with the provision of M2M services is assessed using Vodafone's own data, available from its financial and human resources systems. The data contained in the financial accounts is prepared on an accruals basis for the financial year and so does not relate to cash spent in the year.

Vodafone's indirect economic contribution from its M2M services has been calculated using GVA multipliers. These multipliers were generated from analytical input-output tables and employment data available from Eurostat for European Union countries and either the World Input-Output Database (WIOD) or the relevant national statistics agency for non-EU countries.

To contextualise the contribution that Vodafone makes through the provision of its M2M services, economic data from a number of external public sources is presented. It should be noted that these data do not always correspond to the equivalent year of Vodafone analysis where data availability prevented this. These data generally also refer to calendar years as opposed to financial years.

To calculate Vodafone's GVA associated with the provision of M2M services globally we have used revenue data provided by Vodafone and have made assumptions, which were agreed by Vodafone, to estimate the costs associated with the provision of these services.

We have scaled up Vodafone's GVA to that of the whole industry based on the number of connections in the total market in quarter 1 2014.

For consistency with the Vodafone Group Plc Annual Report 2014 and the reporting of Vodafone's performance, the same Euro to GBP exchange rates have been used. The average exchange rate for the relevant years has been used.

Currency	Exchange Rate
Euro/GB Pound (€/£)	1.19
€/USD	1.33

End Notes

1. Work order dated 3 July 2014
2. Machina Research as at June 2015
3. Cisco, taken from <http://www.cisco.com/web/solutions/trends/iot/portfolio.html>
4. IHS Technology, 2014, The Cloud: Redefining the Information, Communication and Technology Industry
5. M2M connectivity can be delivered over a range of networks including cellular, low power wide area, metropolitan area networks, satellite, short range and wide area fixed.
6. CISCO, 2011, A Business Case for Connecting Vehicles.
7. European Commission, 2014, Smart grids and meters, <http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>
8. Vodafone, 2015, Vodafone Group plc Sustainability Report, 2014/15, at <https://www.vodafone.com/content/dam/sustainability/2015/pdf/vodafone-full-report-2015.pdf>
9. CEBR, December 2010, The Cloud Dividend: Part One
10. IDC, 2012, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up
11. European Commission, 2014, "A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change" at http://ec.europa.eu/priorities/docs/pg_en.pdf#page=6
12. Based on the Machina Research methodology of measuring the number of M2M Revenue Generating Units (RGUs) – (see www.machinaresearch.com).
13. PR Newswire, 2015, Global Video Conferencing Market Trends and Forecast 2014 – 2020, At: <http://www.prnewswire.com/news-releases/global-video-conferencing-market-trends-and-forecast-2014--2020-300045321.html>.
14. David Publishing, 2011, The Role of ICT in the Globalization of Firms, At: <http://www.davidpublishing.com/davidpublishing/Upfile/2/28/2012/2012022875515761.pdf>
15. GSMA, 2014, The Mobile Economy
16. Boston Consulting Group, 2015, The Mobile Revolution: How Mobile Technologies drive a Trillion dollar impact.
17. GE and Accenture, 2014, Industrial Internet Insights Report for 2015, p. 7 (www.gesoftware.com/sites/default/files/industrial-internet-insights-report.pdf)
18. For example, Cisco predicts that by 2020 there will be 50 billion "things" connected to the Internet, up from 25 billion in 2015. See <http://share.cisco.com/internet-of-things.html>
19. GSMA Intelligence, February 2014, From concept to delivery: the M2M market today
20. Machina Research as at June 2015
21. Berg, 2014, The Global Wireless M2M market
22. Machina Research as at August 2015
23. IHS technology as at January 2014
24. European Commission, 2014, Smart grids and meters, <http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>
25. GSMA, February 2013, Connected Car Forecast: Global Connected car market to Grow Threefold with five years
26. Office of the Privacy Commissioner of Canada, 2014, (Cloud Computing) Fact Sheet
27. IHS Technology, 2014, The Cloud: Redefining the Information, Communication and Technology Industry
28. IBM, 2014, Moving from the back office to the front lines
29. Oracle, Oracle Cloud Computing – An Oracle White Paper, May 2010
30. CEBR, 2010, The Cloud Dividend: Part One, December
31. IDC, 2012, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up
32. *ibid*
33. Gross Value Added (GVA) is the measurement of the contribution to the economy of an individual producer, industry or sector. This estimates the difference between the value of the goods and services produced and the cost of the inputs – such as raw materials – used to create those goods and services.
34. We scaled up Vodafone's overall M2M GVA to the wireless cellular M2M industry level, based on the number of global connections in the 1st Quarter of 2014. This is calculated as: market level GVA = Vodafone GVA * (total market cellular M2M connections / Vodafone cellular M2M connections). Although this is based on a number of assumptions, including that all providers have the same broad cost and revenue structure as Vodafone, the analysis provides an indication of the possible magnitude of the economic contribution made directly and indirectly by global wireless M2M providers.
35. Vodafone, July 2015, M2M adoption barometer
36. Vodafone, July 2014, M2M adoption barometer. The M2M Adoption Barometer found that there has been a significant increase in the number of executives saying that M2M is helping them deliver more consistent services across multiple geographies, which suggests that more respondents are looking at M2M beyond a local or national level.
37. Estimate as of June 2015 provided by RWE.
38. Automotive World, June 2014, Can the automotive industry help boost the global economy? Here: <http://www.automotiveworld.com/megatrends-articles/can-the-automotive-industry-help-boost-the-global-economy/>
39. GSMA, February 2013, Connected Car Forecast: Global Connected car market to Grow Threefold with five years
40. KPMG, March 2015, Connected and Autonomous Vehicles – The UK Economic Opportunity

41. CISCO, 2011, A Business Case for Connecting Vehicles.
42. Estimated costs are \$3 trillion; converted to Euros using the USD: Euro exchange rate sourced from www.oanda.com on 17/12/2014
43. European Commission, 2015, A Digital Single Market Strategy for Europe – Analysis and Evidence, Commission Staff Working Document, Brussels SWD, 2015,100 final.
44. CISCO, 2011, A Business Case for Connecting Vehicles.
45. Forbes, 2013, Top Health Trend For 2014: Telehealth To Grow Over 50%. What Role For Regulation?, At: <http://www.forbes.com/sites/theapothecary/2013/12/28/top-health-trend-for-2014-telehealth-to-grow-over-50-what-role-for-regulation/>
46. American Hospital Association, 2015, The Promise of Telehealth for Hospitals, Health Systems and Their Communities, At: <http://www.aha.org/research/reports/tw/15jan-tw-telehealth.pdf>
47. FierceMobile Healthcare, 2013, Remote patient monitoring to save \$36B globally by 2018, At: <http://www.fiercemobilehealthcare.com/story/remote-patient-monitoring-save-36b-globally-2018/2013-07-17>
48. Gartner, May 2011, Telehealth Benefits and Adoption: Connecting People and Providers Across Canada, at: <https://www.infoway-inforoute.ca/en/component/edocman/333-telehealth-benefits-and-adoption-connecting-people-and-providers-full/view-document>
49. Virgin Media Business, 2013, The Cumbria and Lancashire Telestroke Network, At: <http://www.fiercemobilehealthcare.com/story/remote-patient-monitoring-save-36b-globally-2018/2013-07-17>
50. Wall Street Journal, 2015, Remote Patient Monitoring Lets Doctors Spot Trouble Early, At: <http://www.wsj.com/articles/remote-patient-monitoring-comes-to-health-care-1424145642>
51. Banking Technology, 2013, Banks must adopt video banking, says Celent report, At: <http://www.bankingtech.com/158542/banks-must-adopt-video-banking-says-celent-report/>
52. Banking Technology, 2014, Bank of America To Add Video Conferencing to 500 Branches, At: <http://www.banktech.com/channels/bank-of-america-to-add-video-conferencing-to-500-branches/d/d-id/1297024?>
53. Citi, 2013, Citi Unveils Next-Generation Banking Experience: “Citibank Express”, At: <http://www.citigroup.com/citi/news/2013/130123a.htm>
54. The Guardian, 2014, Barclays rolls out face-to-face video banking, At: <http://www.theguardian.com/business/2014/nov/30/barclays-roll-out-face-to-face-video-banking>
55. European Commission, 2014, “A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change” At: http://ec.europa.eu/priorities/docs/pg_en.pdf#page=6
56. Jayshree Chavanb, 2013, Internet Banking – Benefits and vchallenges in an emerging economy
57. Telefonics, 2014, The Smart Meter Revolution
58. European Commission, 2014, Smart grids and meters, At: <http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>
59. European Commission, 2013, eCall: automated emergency call for road accidents mandatory in cars from 2015, At: http://europa.eu/rapid/press-release_IP-13-534_en.htm
60. In the Netherlands, section 7.4a of the Dutch Telecommunications Act 1998 (as amended). In Chile, article 24H Ley General de Telecomunicaciones no. 18.168 de 1982 (as amended).
61. The code was signed by seven companies in 2011 who, at the time, covered 90% of all fixed-line broadband customers and 60% of all mobile customers in the UK. This code, which has since been signed by even more providers, “will ensure that consumers have access to more easily comparable information about the traffic management practices of different broadband providers” (Broadband providers launch new traffic management transparency code, 14 March 2011, www.broadbanduk.org/wp-content/uploads/2012/08/broadband_providers_launch_new_traffic_management_transparency_code_14_march_201111.pdf)
62. Federal Communications Commission Report and Order on Remand, declaratory Ruling, and Order, FCC 15-24, ‘In the Matter of Protecting and Promoting the Open Internet’.
63. Article 3(5) of the draft law states: Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality. Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for other end-users. See Council of the European Union (2015) Interinstitutional File: 2013/0309 (COD), 10409/1/15 REV 1.
64. PR Newswire, 2015, Global Video Conferencing Market Trends and Forecast 2014 – 2020, At: <http://www.prnewswire.com/news-releases/global-video-conferencing-market-trends-and-forecast-2014–2020-300045321.html>
65. Ibid.
66. Based on the Machina Research methodology of measuring the number of M2M Revenue Generating Units (RGUs) – (see www.machinaresearch.com)
67. Embedded Computing Design, 2014, Rise of the machines: The future of M2M in healthcare, <http://embedded-computing.com/articles/rise-the-machines-future-m2m-healthcare/>
68. These estimates include all M2M devices, not just those with connections to fixed and wireless communications networks.
69. Cisco, 2012, ‘Broadband Revolution: Roadmap for Safety and Security Mobile Communication Services’ At: <http://www.cisco.com/web/strategy/docs/gov/emergencyresponder.pdf>
70. Machina Research, 2015, DNA of M2M, At www.machinaresearch.com
71. See Machina Research and Aegis Spectrum Engineering for Ofcom, April 2014, M2M applications characteristics and their implications for Spectrum. At: stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf
72. These specific services were identified by Machina Research (DNA of M2M), 2015, www.machinaresearch.com) as being the major propositions requiring a high/stringent Quality of Service.
73. ibid
74. European Commission, 2014, Smart grids and meters, At: <http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>
75. EurActiv.com, 2015, Smart grids could be Europe’s shale gas, Commission says, At: <http://www.euractiv.com/sections/energy/smart-grids-could-be-europes-shale-gas-commission-says-313464>
76. Forbes, 2013, Top Health Trend For 2014: Telehealth To Grow Over 50%. What Role For Regulation?, At: <http://www.forbes.com/sites/theapothecary/2013/12/28/top-health-trend-for-2014-telehealth-to-grow-over-50-what-role-for-regulation/>
77. KPMG, March 2015, Connected and Autonomous Vehicles – The UK Economic Opportunity
78. KPMG, March 2015, Connected and Autonomous Vehicles – The UK Economic Opportunity
79. Current regulatory activity includes: European Commission activity to promote a Digital Single Market; an ongoing BEREC review; development of a National Telecom M2M roadmap in India; a US review of privacy and security risks associated with Internet of Things; Singaporean guidelines for submission of application for service based operator’s licence – Machine-to-Machine (M2M); and German, Italian, Belgian and UK consultations on M2M and Internet of Things.
80. This is Vodafone’s typical M2M deployment model which allows it to provide a single consistent M2M solution using supranational numbering to customers across a number of countries through the use of a Global SIM and associated platform. Vodafone is also a signatory to the GSMA’s embedded SIM specification, which provides an alternative remote provisioning and management of machine to machine (M2M) connections.
81. This has typically been done using E.164 numbers from a country’s national numbering plans. E.164 defines a general format for international telephone numbers which are limited to a maximum of 15 characters and are usually prefixed with a +.
82. CEPT/ECC, March 2014, Number Portability Implementation in Europe.
83. ANATEL Resolutions no. 83/98, no. 298/2002 and 301/2002 (numbering regulation).
84. Special Terms and Conditions of Type B Class License to provide AVL Services as issued by the Communications and Information Technology Commission (CITC) of Saudi Arabia.
85. Government of India, Ministry of Communication & Information Technology, Department of Telecommunications, 2015, National Telecom M2M Roadmap, At: <http://www.dot.gov.in/sites/default/files/Draft%20National%20Telecom%20M2M%20Roadmap.pdf>
86. Oman Telecommunications Regulatory Authority, 2013, Issuance of Regulation on the Provision of Automated System for Vehicles Management Service, At: <http://www.tra.gov.om/pdf/80-2013-ivms-dec.pdf>
87. Authority for Communications Guarantees, 2015, Fact-finding survey concerning Machine to Machine (M2M) communication services
88. Federal Network Agency (Bundesnetzagentur), 2013, Publication pursuant to Section 2 Telecommunications Numbering Ordinance; Machine-to-Machine (M2M) Communications
89. Vodafone has advised us that the Belgium regulator (BIPT) is reviewing the current arrangements for certain aspects of M2M numbering in Belgium (such as use of E.212 numbers related to Mobile Network Codes)
90. Ofcom, “Promoting investment and innovation in the Internet of Things, Statement, 27 January 2015, at <http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/IoTStatement.pdf>
91. European Conference of Postal and Telecommunications Administrations Electronic Communications Committee, April 2013, Report 194: Extra-Territorial Use of E.164 Numbers
92. Extra-territorial use of E.164 numbers is defined in the paper as “use of E.164 numbers of one country in another country on a permanent basis”.
93. See Executive Summary of the report, which states that “Extra-territorial use of numbers should only be permitted in exceptional cases which have been defined by an ECC Decision. Possible candidates are some nomadic voice services and some M2M services”.
94. GSMA, 2015, Remote SIM Provisioning for Machine to Machine, At: <http://www.gsma.com/connectedliving/embedded-sim/>
95. For example, Russia has recently introduced new data localisation laws (see www.globalregulatoryenforcementlawblog.com/2015/01/articles/data-security/russia-sets-a-new-deadline-for-data-localisation-and-removes-hong-kong-and-switzerland-from-adequate-privacy-protection-list/)
96. For example, many countries permit the transfer of personal data across borders if sufficient guarantees are in place to ensure the protection of that data, and applicable laws/regulations may provide for a number of alternative approaches to securing such guarantees.
97. For a discussion of this see European Commission, February, 2015, Workshop ‘Facilitating cross border data flow in Europe – on data location restrictions’.
98. European Commission, 2015, Rolling Plan for ICT standardisation.
99. European Commission, 2011, Decision on setting up the the European multi-stakeholder platform on ICT standardisation. At: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:349:0004:0006:EN:PDF>
100. Articles 51 (2), (6) and (7) of Law no. 5809 on Electronic Communication.
101. NisidePrivacy, 2014, Brazil Enacts “Marco Civil” Internet Civil Rights Bill, At: <http://www.insideprivacy.com/international/brazil-enacts-marco-civil-internet-civil-rights-bill/>
102. National Telecom Regulatory Authority, 2003, Telecommunication Regulation Law No. 10 of 2003

-
103. Government of India, Ministry of Communications and IT, License Agreement for Unified License, section 39.23 (viii)
-
104. Hong Kong Privacy Commissioner, 29 December 2014, Guidance on Personal Data Protection in Cross-border Data Transfer
-
105. Article 1(2) "On amendments to certain legislative acts of the Russian Federation for clarification of personal data processing information and telecommunication networks" (No.242-FZ)
-
106. Reforms from China's Standardisation Administration and the General Administration of Quality Supervision, Inspection, and Quarantine.
-
107. Articles 24, 25, 28, and 34, Decree No. 72/2013/ND-CP 'On provision and use of Internet services and online information' and Article 4, Circular 09/2014/TT-BTTTT 'Detailing management, use and provision of information on websites and social networks.
-
108. Transaction and Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction.
-
109. European Centre for International Political Economy, 2014, The Costs of Data Localisation: Friendly Fire on Economic Recovery
-
110. Matthias Bauer et al., March 2013, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce," European Centre for International Political Economy, 3, At: https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_Ir.pdf.
-

Contact us

Sean Kennedy

Director, Telecoms
Economics & Regulation

T +44 (0)20 7694 5468

E skennedy@kpmg.co.uk

Heather Sharp

Associate Director
Economics & Regulation

T +44 (0)20 7311 3469

E heather.sharp@kpmg.co.uk

Seamus McGowan

Assistant Manager
Economics & Regulation

T +44 (0)20 76941195

E seamus.mcgowan@kpmg.co.uk



AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Report

AIOTI Working Group 4 – Policy

15 October 2015



Table of Contents

- 1. Executive Summary**
- 2. Introduction**
- 3. Privacy**
- 4. Security**
- 5. Liability**
- 6. Net Neutrality**



1- Executive Summary

The Internet of Things ('IoT') has the potential to transform European industry and the activity underway within the Alliance for Internet of Things Innovation ('AIOTI') represents an important opportunity for European industry to promote sustainable IoT growth.

AIOTI Working Group 4 ('WG4') is the policy working group. At the time of writing, WG4 has over 200 members across various sectors of the economy. The scope of WG4, as per the AIOTI terms of reference, is to identify existing or potential market barriers that prevent the take-up of the IoT in the context of the Digital Single Market, as well as from an Internal Market perspective, with a particular focus on trust, security, liability and privacy. WG4 has also assessed the specific recommendations that can be provided on net neutrality and IoT, given the current relevance of net neutrality to the European policy debate, following agreement of the Telecoms Single Market legislative package.

In this document, which represents the initial output of the Policy group, WG4 highlights a number of key issues related to each of these areas. In so doing, WG4 also makes a number of recommendations to further inform both the policy debate and the activities of the Horizon 2020 Large Scale Pilots due to commence in 2016. We also make reference to other relevant stakeholders that are carrying out important activity in this field and which should be linked to the work of WG4.

WG4 makes the following policy recommendations:

- In relation to **privacy**, we make ten recommendations to address key concerns that have been raised in this area. These range from European Commission sponsorship of an accredited Privacy engineering program for European educational establishments, to adoption of Privacy by Design best practice by AIOTI members.
- In relation to **security**, we make specific reference to existing industry best practices on how IoT service providers can develop IoT enabled applications, which should inform the Large Scale Pilots. We also highlight the key stakeholder, technological and societal challenges in this area, and make recommendations in respect of each.
- In respect of **liability**, WG4 considers that the rapid development of IoT technology may raise certain product compliance, product liability and insurance-related issues in the future. At present we believe that these issues can be managed within the existing legal and regulatory framework. We propose that the emphasis should, in the main, be on the development of policy solutions to these potential challenges.
- In relation to **net neutrality**, we provide a number of case studies to help inform the activities of National Regulatory Authorities across Member States in light of the finalised text on net neutrality as set out in Telecoms Single Market package.



2 - Introduction

IoT is an innovation that is relevant to a wide range of different stakeholders across many kinds of markets. IoT brings together both the supply-side (i.e. those companies that may be active in designing the devices or providing the connectivity for IoT applications) and the demand-side (i.e. those companies that are integrating IoT technology within their operations and processes or providing IoT enabled products and services to end-users). Appropriate use of IoT data will also deliver many important socio-economic benefits. While IoT use is increasing rapidly, it is still in its nascent stages and the related technologies, business models and policies will undoubtedly evolve over a number of years.

To set the scene and provide a description of IoT, we refer to the previous definition of The Internet of Things by the ITU and IERC-Internet of Things European Research Cluster:

*'The Internet of Things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network.'*¹

IoT applications can be built using any number of technologies, and given it is a fast-moving market, it can be challenging to adopt precise technological definitions in a document such as this. WG4 has endeavoured to ensure that its policy recommendations are sufficiently flexible to cater for a range of IoT innovations, recognising of course that the specific risks (whether privacy, security, data management or liability) will differ according to the exact IoT use-case in question. In this document we refer to 'IoT applications' when we describe different types of IoT innovation. No precise legal meaning should be ascribed to this term.

It is also the case that certain IoT applications may prompt a wider societal debate. As WG4 notes in this report, the "ethical" implications of certain potential IoT innovations that involve automated decision making (such as autonomous cars) is a common topic among academics and in the popular press. WG4 believes that it is society that will ultimately determine whether such innovations take hold or not. WG4 hopes that the policy recommendations set out in this document will help improve individual understanding and awareness of potential policy challenges, and also solutions, related to growth of the IoT.

An important question that WG4 has considered in formulating the policy recommendations set out in this document is whether the emergence of IoT necessitates new regulation. Broadly speaking, WG4 does not believe that it does. Any regulatory proposal targeting the IoT should address only well-defined market failures that cannot be addressed through existing law and self-regulatory measures.² Furthermore, the IoT ecosystem is complex and fast-moving, creating a high risk of regulatory error.³ Therefore any regulatory solutions should be technologically neutral, flexible, and respect the global, open interconnected character of the Internet.⁴ On a related theme, WG4 does not make specific

1 ITU-T Y.2060, 'Overview of Internet of Things,' June 2012. White paper, 'Smart networked machines and Internet of Things,' Association Instituts Carnot, January 2011.

² European Commission, Better Regulation Guidelines, May 19, 2015, http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm, Better Regulation Toolbox, May 19, 2015 http://ec.europa.eu/smart-regulation/guidelines/toc_tool_en.htm

³ Shelanski, H. A. (2013) "Information, Innovation, and Competition Policy for the Internet", 161 U. of Penn. L. Rev. 1663 http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1025&context=penn_law_review

⁴ OECD Principles for Internet Policy Making, 2014 <http://www.oecd.org/sti/ieconomy/oecd->



recommendations in the context of ongoing legislative processes (in particular the ongoing review of the General Data Protection Regulation) as we do not consider it within WG4's mandate to do so.

Again on a related theme, interested parties may wish to note that previous work has been undertaken by DG Connect, DG Justice, ENISA, NIST and approximately 200 companies in relation to Cloud SLA Standardisation Guidelines. This activity considered topics such as performance, security, data management and Personal Data Protection in a Cloud environment and provides some context to the work of WG4.⁵

Finally, given the range of stakeholders relevant to IoT, WG4 has focused on those policy topics which are of 'horizontal' application (i.e. they have immediate relevance to both the supply-side and the demand-side of the market). There are other important topics relevant to the continued development of a vibrant European market for IoT, including harnessing use of IoT data, free movement of IoT data, access to spectrum, interoperability and numbering. These topics have not been considered by WG4 in this document, given the time available. WG4 remains ready to make policy recommendations in relation to these topics in the future.

[principles-for-internet-policy-making.pdf](#)

⁵See <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>



3 - Privacy

Regulatory and Policy Context

In considering privacy policy options to promote the development of the IoT across Europe, it is first necessary to highlight the outcome of the previous IoT policy review initiated by the European Commission, which concluded in May 2013.⁶

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

This report was commissioned by the European Commission and 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. It was written following an extensive consultation with industry and identified potential gaps in the regulatory framework in respect of privacy and data protection (in particular regarding liability and responsibility). It identified three policy options that could be pursued, namely ‘no action’, ‘soft law’ and ‘hard law’, as follows:

Figure 3.1 – IoT Policy options presented to the European Commission in May 2013

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

After consideration of these three options, the report recommended an initial soft law approach combining standards, monitoring, 'information remedies' and an ethical charter to facilitate IoT self-organisation⁷ and clarify the need for and nature of effective regulatory interventions.

There have been two subsequent privacy developments of note particularly relevant to the

⁶ http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=11701

⁷ In making the recommendation for an 'ethical charter', the report noted that that this recommendation did not receive consistent support among those responding to the EC public consultation on the development of the IoT. The report stated that 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-publicconsultation>.



work of WG4, which will now be considered.

Article 29 Working Party - Opinion 8/2014 on the Recent Developments on the Internet of Things – September 2014⁸

This Opinion identifies the main data protection risks that lie within three specific IoT developments (namely wearable computing, quantified self and home automation). Although the Opinion is limited in scope, it does however highlight most of the main privacy issues related to the IoT. Therefore it provides an appropriate framework for assessing how the AIOTI should respond to possible IoT privacy challenges, subsequent to the last Commission review. The Opinion identifies the following IoT challenges:

- Lack of control by the user over an IoT device and information asymmetry between the user of the IoT application and the developer of the application
- Quality of the user's consent being poor
- Privacy challenges associated with inferences being derived from data, and repurposing of original processing
- Intrusive bringing out of behaviour patterns and profiling
- Limitations on the possibility to remain anonymous when using services
- Security risks.

After consideration of these challenges, the Opinion then highlights the following recommendations, common to all stakeholders, which therefore provides some context to the work of WG4:

- Privacy Impact Assessments should be performed before any new IoT applications are launched.
- Stakeholders must delete raw data as soon as they have extracted the data required for their data processing
- Every IoT stakeholder should apply the principles of Privacy by Design.
- Data subjects and users must be able to exercise their rights and be "in control" of their data at any time
- The methods for giving information, offering a right to refuse consent should be made as user-friendly as possible
- Devices and applications should also be designed so as to inform users and non-user data-subjects.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – June 2015⁹

The key legislative initiative in the field of data protection and privacy that needs to be highlighted in order to adequately frame the work of WG4 is clearly the reform of the EU General Data Protection Regulation (GDPR).

At the time of writing, the relevant European institutions are negotiating the amendments adopted by the Parliament in March 2014 and the general approach of the Council (June 2015). A detailed analysis of the GDPR is outside of the scope of this report and the primary focus of our recommendations is not framed towards changing the GDPR text but how to work within the framework once it is adopted. However, in protecting individual privacy,

⁸http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

⁹ Interinstitutional File: 2012/0011 (COD)



policy makers should take into account that the IoT is characterised by cross-fertilisation of data, individualised approaches, ubiquitous devices – often without user interfaces – and free flow of data. As such, data protection legislation should consider the context of data use and reasonable expectations of users, and not take overly-prescriptive approaches to purpose limitation, notice, consent, profiling and cross border transfer. These remain concerns in the current negotiations.

In line with the WP29 Opinion, the current draft of the GDPR envisages use of Privacy Impact Assessments (where processing is likely to result in a high risk to the rights and freedoms of citizens) and use of data protection by design principles. The Regulation also emphasises that codes of conduct should help illuminate Privacy by default and by design principles. The principles and processes underpinning the GDPR will equally apply to those that are designing and developing IoT applications.

Starting point for AIOTI WG4 IoT Privacy policy recommendations

The starting point for the work of WG4 should therefore be to ensure that, where required, IoT applications are developed with privacy compliance in mind. We should also work to evaluate if and when a Privacy Impact Assessment is necessary in the context of the IoT, and develop a standardised approach to performing such assessments, in accordance with Privacy by Design best practice. Such an approach is consistent with both the recommendations of the Article 29 Working Party Opinion and the current scope of the GDPR. This should provide the correct frame of reference for the WG4’s policy recommendations and also provide guidance for those developing IoT applications in the context of the Large Scale Pilots.

Existing or potential privacy barriers to take up of IoT across Europe

Within this framework, WG4 has identified ten specific privacy barriers that may pose a threat to take-up of IoT across Europe, and which must be addressed. WG4 believes that the adoption of these ten policy recommendations provides a comprehensive basis for addressing privacy concerns associated with IoT.

	Privacy Barrier	AIOTI WG4 response
1	‘Privacy Engineering’, an integral component of a Privacy by Design approach, is not yet embedded within the engineering community	<p>Context - Education programmes are needed to create a new type of professional, the privacy engineer. European students are gaining engineering qualifications but privacy is not part of the curriculum.</p> <p>Case study – the UK government recently announced funding for a £10m IoT research hub¹⁰. The Research Hub will combine a small number of leading universities. The research focus will be on the challenges associated with privacy, security and trust in the IoT, including the various interactions, policy and governance, beliefs and behaviours between people and the IoT systems.</p> <p>Policy recommendation - DG Education and Culture to raise awareness within relevant EU academic institutions. It should consider schemes for sharing educational materials as recommended by PRIPARE¹¹. It should consider sponsoring an accredited ‘Privacy Engineer’ scheme.</p>

¹⁰ <https://www.epsrc.ac.uk/newsevents/news/iothub/>

¹¹ <http://pripareproject.eu/research/> see WP4



2	<p>There is no commonly applied framework for privacy risk that can be translated into engineering objectives to help companies implement their own privacy impact assessments.</p>	<p>Context – Privacy Impact Assessments are an important way of identifying privacy risk. However, these can be complex. We need a commonly accepted way of analysing privacy risks for IoT applications and a standardised method to carry out such assessments.</p> <p>Case study 1 – The ‘Privacy Risk Framework Project’, established by the Center for Information Policy Leadership¹². This project aims to develop a methodology and tools to apply, calibrate and implement abstract privacy obligations and to prioritize compliance based on the actual risks (likelihood and severity) and benefits of the proposed data processing. It also aims to build consensus about privacy harms to individuals (tangible, intangible, societal).</p> <p>Case study 2 - There are positive examples of industry associations communicating to their members the use of risk-based methodological approach to privacy. One such example is the ‘Milton Keynes LPWAN IoT demonstrator’, facilitated by Digital Catapult, and which has been highlighted as a case study as part of the Society for Motor Manufacturer and Traders’ (SMMT) Connected & Autonomous Vehicles Forum. This approach differentiates between four different classes of data that may be collected on the platform, with the different levels of potential harm involved, as follows: (i) data from internet of things devices (ii) Personal data (iii) data that has ownership and rights and (iv) data closed in organisations. This may not be the final answer, but it shows the ways in which some analysis is developing.</p> <p>Policy recommendation – AIOTI members should encourage their industry associations to adopt privacy risk frameworks¹³ which they should then communicate to all members for use in developing IoT applications.</p>
3	<p>There is a lack of widely acknowledged and endorsed privacy engineering approach</p>	<p>Context - examples of best practice are available, such as iPEN¹⁴, PRIPARE¹⁵ and the Privacy Patterns repository¹⁶ in the EU and NIST¹⁷ in the USA</p> <p>Case Study Example ‘IoT Privacy Engineering approach’, developed by Vodafone, as follows:</p>

¹²https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centres_Privacy_Risk_Framework_Workshop_I_Initial_Issues_Paper.pdf

¹³ See for instance ISO29134, CNIL privacy assessment methodology (<http://www.cnil.fr/english/news-and-events/news/article/privacy-impact-assessments-the-cnil-publishes-its-pia-manual/>), NIST risk management framework (http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf)

¹⁴ <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN>

¹⁵ <http://pripareproject.eu/>

¹⁶ www.privacypatterns.eu

¹⁷ <http://csrc.nist.gov/>



		<p style="text-align: center;">Privacy Engineering and Assurance – Privacy activities for an IoT approach</p> <p>Policy recommendation –Connect/DG Grow to support best practice on privacy engineering in IoT. AIOTI members should encourage their industry associations to adopt a privacy engineering approach¹⁸ which they should then communicate to all members for use in developing IoT applications.¹⁹</p>
4	<p>There is insufficient usage of pseudonymised and anonymized data by those designing and developing IoT applications</p>	<p>Context – use of pseudonymised and anonymised data would go a long way to addressing privacy concerns associated with IoT applications.</p> <p>Case Study – The Article 29 Working Party has also provided guidance on the types of anonymization techniques that can be used to ensure that a data holder’s private data is not re-identified, while still allowing the data itself to remain practically useful.²⁰</p> <p>Policy recommendation – the use of pseudonymised or anonymised data should be encouraged as the ‘default’ design principle for IoT applications. This can of course be subsequently changed as required in accordance with Privacy Impact Assessment and Privacy by Design best practice. But having it encouraged as ‘default’ will go some way to encouraging more widespread use. More broadly, the provision of less stringent rules in the case of processing of anonymised or pseudonymised data will be a real incentive for the adoption of these techniques, as well as other Privacy Engineering Technologies, by the industry. The chosen method of pseudonymisation and anonymisation must</p>

¹⁸ For instance PRIPARE contribution: http://pripareproject.eu/wp-content/uploads/2015/08/WG5_N94_PRIPARE_Contribution_SP_Priv_engineer_frmwk_v2.pdf

¹⁹ Accountability is also a relevant concept here (see section 4 for more details on accountability).

²⁰ Opinion 05/2014 on Anonymisation Techniques. at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf



		however be proven to be resilient against inversion attacks, as it has been demonstrated that certain methods are vulnerable to re-engineering the original privacy sensitive data ²¹ .						
5	Lack of commonly understood and acknowledged knowledge bases of documented solutions to various recurring privacy problems.	<p>Context - ‘Privacy knowledge bases’ are an important part of an effective Privacy by Design approach. There is, however, insufficient sharing of best practice which would address potential consumer concern, Industry should be proactive in sharing examples and best practice.²²</p> <p>Case Study – Vodafone Automotive Usage Based Insurance (UBI) product: example application of Privacy by Design principles</p> <table border="1"> <thead> <tr> <th>Privacy by Design Principle</th> <th>UBI Product</th> </tr> </thead> <tbody> <tr> <td> <p>1. Proactive not Reactive; Preventative not Remedial</p> <p>Privacy by Design is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. It does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.</p> </td> <td> <p>The UBI product adopts proactive privacy. It has been subject to legal reviews as well as checks against industry guidance, and consumer-protecting controls such as the ability to check and dispute records. These are built into both the technology and the partner contracts</p> </td> </tr> <tr> <td> <p>2. Privacy as the Default Setting</p> <p>Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the product, by default.</p> </td> <td> <p>The UBI solution is designed around a philosophy of privacy as the default setting.</p> <p>For example, datasets for driving records (held by Vodafone and its partners) and policyholder records are only brought together in an aggregated statistical data in order to allow the Insurance provider to prepare the premium, to provide insurance services and respond to a customer request.</p> </td> </tr> </tbody> </table>	Privacy by Design Principle	UBI Product	<p>1. Proactive not Reactive; Preventative not Remedial</p> <p>Privacy by Design is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. It does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.</p>	<p>The UBI product adopts proactive privacy. It has been subject to legal reviews as well as checks against industry guidance, and consumer-protecting controls such as the ability to check and dispute records. These are built into both the technology and the partner contracts</p>	<p>2. Privacy as the Default Setting</p> <p>Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the product, by default.</p>	<p>The UBI solution is designed around a philosophy of privacy as the default setting.</p> <p>For example, datasets for driving records (held by Vodafone and its partners) and policyholder records are only brought together in an aggregated statistical data in order to allow the Insurance provider to prepare the premium, to provide insurance services and respond to a customer request.</p>
Privacy by Design Principle	UBI Product							
<p>1. Proactive not Reactive; Preventative not Remedial</p> <p>Privacy by Design is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. It does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.</p>	<p>The UBI product adopts proactive privacy. It has been subject to legal reviews as well as checks against industry guidance, and consumer-protecting controls such as the ability to check and dispute records. These are built into both the technology and the partner contracts</p>							
<p>2. Privacy as the Default Setting</p> <p>Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the product, by default.</p>	<p>The UBI solution is designed around a philosophy of privacy as the default setting.</p> <p>For example, datasets for driving records (held by Vodafone and its partners) and policyholder records are only brought together in an aggregated statistical data in order to allow the Insurance provider to prepare the premium, to provide insurance services and respond to a customer request.</p>							

²¹ “Model Inversion Attacks that Exploit Confidence Information” and Basic Countermeasures”, M. Fredrikson, S. Jha, T. Ristenpart, 2015 ACM Conference on Computer and Communications Security (CCS).

²² There are examples from other industries that provide examples of best practice in a multi-stakeholder environment, such as the GSMA’s Mobile Privacy Guidelines for App developers (<http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development>) and the GSMA’s Privacy Accountability Framework for the implementation of the App Guidelines (<http://www.gsma.com/publicpolicy/accountability-framework-for-the-implementation-of-the-gsma-privacy-design-guidelines-for-mobile-app-development>).



		<p>3. End-to-End Security – Full Lifecycle Protection</p> <p>Privacy by Design extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion.</p>	<p>UBI is subject to stringent information security policies and practices. . Delivery partners, including insurers, are contractually obliged to offer comparable levels of security.</p>
		<p>4. Visibility and Transparency – Keep it Open</p> <p>Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike.</p>	<p>The UBI product allows consumers to interrogate their driving records from a smartphone or PC, providing complete transparency of the data collected. Data is provided, with uploads from the in-car device at the end of each journey or uploads daily through the batch procedure.</p>
		<p>5. Respect for User Privacy – Keep it User-Centric</p> <p>Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.</p>	<p>The UBI product has been designed from the outset to respect driver privacy, through architecture and design, to the driver experience and interface.</p> <p>The policyholder can review their driving records, and the derived driving behaviour scores, through a web portal interface or through a smartphone. If the policyholder has reason to believe that the telematics record is erroneous, the policyholder can register or dispute data where appropriate to maintain their driving behaviour profile.</p>
<p>Policy recommendation – AIOTI members should share and publicise case studies of how they have embedded a Privacy-led approach within their IoT application development. They should store these resources in an ‘AIOTI Privacy</p>			



		Knowledge Base' to be made available to Large Scale Pilots.
6	There is currently no 'Privacy Design' technology guideline or standard.	<p>Context -Technology standardisation is not subject to a mandatory Privacy Assessment to understand the privacy impacts of the technology in question.</p> <p>Case study 1 - there is experience of defining privacy and security standards in a Cloud environment, as per ISO/IEC 27018²³ and ISO/IEC 27034²⁴.</p> <p>Case Study 2 – activity is already underway by the European Commission²⁵ (Mandate 530) for European standard(s) addressing privacy management in the design and development and in the production and service provision processes of security technologies and European standardisation deliverable(s) giving practical guidelines for the practical implementation of the requested European standards.</p> <p>Policy recommendation – the European Commission should place greater emphasis on adoption of this technologically neutral 'Privacy by Design' methodology in the context of its Digital Single Market activity. It should also ensure that IoT applications are considered within scope of the practical guidelines and liaise internationally as required. AIOTI members should encourage their industry associations to participate to the current standardisation work (CEN/CENELEC JWG8, ISO/IEC JTC1/SC27/WG5, OASIS).</p>
7	Data subjects and users may not be able to exercise their rights and be "in control" of their personal IoT data, and so may not be able to give adequate consent where this is required.	<p>Context - this is a legitimate concern that may be associated with certain IoT applications, however it does not need regulation to address it. Industry needs to proactively respond to this concern. There are already good examples of best practice here. Transparency to the end user is key.</p> <p>Case Study 1 – Digital Catapult 'Personal Data & Trust Program' in the UK.²⁶ The Network aims to build and nurture a community that brings together industry, the public sector, funders, research organisations, individual researchers and innovators to support the UK in becoming the global leader in trust and responsible innovation with personal data (see reference to 'Data Sharing and Trust Frameworks' in slide below), as follows:</p>



²³ Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors at http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

²⁴ Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts at http://www.iso.org/iso/catalogue_detail.htm?csnumber=44378

²⁵ <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#>

²⁶ <http://www.digitalcatapultcentre.org.uk/personal-data-and-trust-network/>



		<div style="text-align: right; color: #e91e63;"> <h3>Personal Data & Trust program</h3> </div> <div style="display: flex; align-items: center;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); background-color: #ccc; padding: 5px; margin-right: 10px;">Engage</div> <div> <p>Personal Data & Trust Innovators Network: A members based organisation, drawing together SME's, Corporates and Academics who are actively working on the topics.</p> </div> </div> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); background-color: #ccc; padding: 5px; margin-right: 10px;">Unlock</div> <div> <p>Living Data Labs: Is a facility created by the Catapult and it's partners to "industrialise" the experimentation and development of new products based on permitted consumer data.</p> </div> </div> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); background-color: #ccc; padding: 5px; margin-right: 10px;">Accelerate</div> <div> <p>Data Sharing & Trust Frameworks: Is the focus of the Catapults drive to help an ecosystem emerge, which gives the consumer control over their data, businesses to reduced costs and develop new services.</p> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 20px;">   </div> <p>Case study 2 – The European Commission has recently agreed new EU-wide technical standards that will help users of Radio Frequency Identification (RFID) smart chips and systems comply with EU Data Protection rules and the Commission's 2009 recommendation on RFID (see IP/09/740).²⁷ People using electronic travel passes, or buying clothes and supermarket items with RFID tags in the label, will know that smart chips are present thanks to the RFID sign.</p> <p>Policy recommendation: The European Commission should highlight and coordinate examples of best practice across the EU, and publish information on best practice privacy-effective solutions. . There are opportunities for regulatory authorities and industry to work together more closely in this area (e.g. research on end-user consent and IoT applications)</p>
8	<p>Data associated with IoT applications can be cross-correlated in way that that creates privacy risk – i.e. 'repurposing of original processing'.</p>	<p>Context - As the Article 29 Working Party Opinion highlights, data originally collected through a device (e.g. the accelerometer and the gyroscope of a smartphone) can then be used to infer other information with a totally different meaning (e.g. the individual's driving habits). The Opinion states that, at each level (whether raw, extracted or displayed data), IoT stakeholders should make sure that the data is used for purposes that are all compatible with the original purpose of the processing and that these purposes are known to the user.</p> <p>Case study – The GSMA's guidelines on use of mobile phone data in responding to the Ebola outbreak²⁸ show the steps that need to be taken before such data can be used for a different purpose. Consistent with these guidelines, mobile operators will anonymise CDRs and adopt robust technical and organisational measures to protect them against unauthorised access and use. The analysis of the anonymised records by third parties (including research agencies, aid agencies and governments) and the sharing of any output from the analysis will take place under legal contract(s) based on these guidelines.</p>

²⁷ http://europa.eu/rapid/press-release_IP-14-889_en.htm

²⁸ <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-October-2014.pdf>



		<p>Policy recommendation – AIOTI members to highlight their own examples where data can be repurposed in a way consistent with applicable law, keeping in mind that applicable law is still under debate for the GDPR. Examples to be stored in the AIOTI Privacy Knowledge Base.</p>
9	The rules are not enforced	<p>Context – Regulatory authorities should enforce existing horizontal rules against those who do not comply.</p> <p>Case study - The FTC in the USA has shown that existing horizontal legislation can be equally applied to IoT applications.²⁹</p> <p>Policy recommendation – there is a place for robust, harmonised and predictable law enforcement.</p>
10	Not all companies place sufficient importance on privacy	<p>Context – there is a perception that some companies do not do enough to put privacy at the centre of their activity. There is also a perception that only companies with data protection obligations (e.g. data controllers or data processors) place importance on privacy while suppliers (e.g; sensors, IoT capabilities, IoT platforms) do not do enough.</p> <p>Case study 1 –Vodafone has privacy principles which are aligned with the OECD privacy principles, and include an explicit commitment to use of Privacy by Design.³⁰ ISO29100 also provides a list of principles. These principles equally apply to IoT applications.</p> <p>Case study 2 –The European Commission³¹ (Mandate 530) for European standard(s) addressing privacy management in the design and development and in the production and service provision processes of security technologies involves all types of stakeholders including suppliers.</p> <p>Policy recommendation – all AIOTI members to publicly commit to develop IoT applications and subsystems consistent with Privacy by Design and AIOTI knowledge base best practice.</p>

²⁹ <https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>

See also <https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices> for further information on the FTC's activity in this area

³⁰ http://www.vodafone.com/content/index/about/sustainability/sustainability_report/issue_by_issue/privacy/our_approach.html

³¹ <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#>



4 - Security

Regulatory and Policy Context

Security cannot be studied in isolation. Other aspects such as safety, reliability, resilience, and privacy are tightly linked as illustrated in Figure 4.1 below. Security does, in particular, tend to go ‘hand in hand’ with privacy when considering potential barriers to growth of IoT across Europe. Therefore many of the principles underpinning WG4’s recommended approach to Privacy (for example a focus on the importance of a design led approach which is context dependent and usage of pseudonymised and anonymized data) will also be relevant here.

Figure 4.1 - Interdependencies of security with privacy and other domains.



As with technological progress in general, IoT brings benefits and improved productivity to users and organizations. Successful adoption of IoT systems depends on many factors, including security levels, related features, and measures to protect their assets and associated services. Protection of IoT related applications and services and the information they generate is necessary to ensure sustainable trust in IoT environments. Ongoing media reports of alleged security failures associated with IoT applications show that the public’s perception of security issues associated with IoT applications have brought attention to security in IoT and highlighted the importance of adequate security support.

Security is a visible aspect of IoT applications and services, and there are numerous initiatives and projects relevant to the security work of WG4, some generally applicable to security in ICT and some specific to IoT. Regulatory activities such as the EU General Data Protection Regulation, the ePrivacy Directive review or the NIS Directive draft have some impact on security emphasis in IoT.

In member states, national ‘Big Data’ or IoT strategies, cybersecurity strategies reviews and a number of other initiatives have addressed security in IoT or adjacent spaces more directly. In international standards bodies, several direct projects focusing on IoT have appeared, such as IoT work in JTC1 SC10 and SC27. European mandates on cybersecurity standardization pursued in ETSI, CEN, and CENELEC also address standards and issues relevant to IoT.

Among some of the activities, we can mention:



- **ENISA** (European Union Agency for Network and Information Security). ENISA has undertaken several projects relevant to IoT, starting in 2008. It developed a view of risks specific IoT applications, and has considered IoT in multiple other reports³².
- **NIS Platform** - The Working Group on Secure ICT Research and Innovation of the Network and Information Security ('NIS') Platform has produced a Strategic Research Agenda ('SRA') in the area of secure information and communication technologies. This SRA complements and underpins the EU NIS Directive, and provides input to the secure ICT Research & Innovation agenda at national and EU level, including the Horizon 2020 programs. The SRA has outlined multiple viable research areas and takes into consideration IoT challenges mainly in Privacy, Identity management, technical trust, lightweight cryptography and several other fields. It uses the example of smart building in smart cities and is organized around three main areas of interest:
 - Individuals' Digital Rights and Capabilities (Individual layer).
 - Resilient Digital Civilisation (Collective layer).
 - Trustworthy (Hyperconnected) Infrastructure (Infrastructure layer)
- **UK Government Cyber Essential Scheme** : Although IoT concerns were not specifically within the scope of the Cyber Essential Scheme, the different outcomes are equally applicable for those developing IoT applications. The key considerations in this respect are Trust ("Social acceptance") and Cyber-security ("Technological challenges").
- **Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)** as defined by the German Federal Office for Information Security (BSI).
- There is also **detailed sector specific activity** that has been previously undertaken, such as the 2011 CEN/CENELEC/ETSI Mandate 490 on smart grids (including the security and data privacy issues on the roll-out of smart metering systems), and the 2009 CEN/CENELEC/ETSI Mandate 441 on smart meters, as well as the guidance on software in smart meters, provided by WELMEC. Much work has also been undertaken in the context of Smart Grids for connected systems, particularly those built on open architecture.
- **ISO/IEC JTC 1/SC 27** maintains an expert committee dedicated to the development of the Information Security Management System (ISMS) family of standards. Through the use of this family of standards, organizations can develop and implement a framework for managing the security of their information assets. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.
- **NIST CPS PWG** (Cyber Physical Systems Public Working Group) included significant EU participation and produced a reference architecture to address a number of issues relating to trustworthiness, security, and privacy.³³

³² See for example, <https://www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel>

³³ <http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf>



Starting point for WG4 IoT Security Policy recommendations

WG4 believes that a fit-for purpose security model for IoT should address the following policy objectives:

- It should be able to offer an adequate, affordable and ‘desired’ security level relevant to each application, matching users’ needs and business requirements.
- As IoT applications have different connectivity requirements, they also need several scales of security, recognising that IoT applications may operate on a single platform/device or on several platforms/devices.
- Security requirements should offer flexibility that doesn’t impede innovation of the technologies. The ‘time to market’ and ‘time on market’ considerations should be taken into account, without jeopardising the essential security needs.
- The model should also meet the desired security protection goals and privacy protection goals, e.g. confidentiality, integrity, availability, anonymity.

WG4 further believes that privacy-impacting IoT applications that deal with personal data should:

- Guarantee privacy and confidentiality of data exchanged through or in transit on the networks or stored in the IoT application or in the Cloud³⁴.
- Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways).
- Preserve integrity of a connected device (or system) for trustable solutions and services.

For those developing IoT applications as part of the Large Scale Pilots, it is vital that Security issues are addressed as part of the design and development phase. As the Large Scale Pilots address a variety of industry sectors, each should tailor security requirements according to their sector, to fulfil the adequate prerequisites, and balance the security risks to cost, throughout their life cycle.

Existing or potential security barriers to take-up of IoT across Europe and associated WG4 policy recommendations

Diverse stakeholders

Specific challenges include:

- The scale and diversity of IoT connected products will be enormous and their components may be developed by many different providers and not all of them may be able to provide the same level of security.
- Metrics and approaches associated with composite security necessary to support IoT infrastructure have not yet been developed.
- Access control for a large installed base of IoT applications can be onerous (i.e. to provide seamless access control which is fully scalable across all types of such IoT applications)
- There can be a security/go-to-market ‘trade off’ – IoT applications may be driven by disruptive products that are quick to market and may only spend a short period of time on the market – and security has cost implications.
- There may be interoperability and complexity challenges due to the more varied ‘industrial value-chain’ associated with IoT applications.

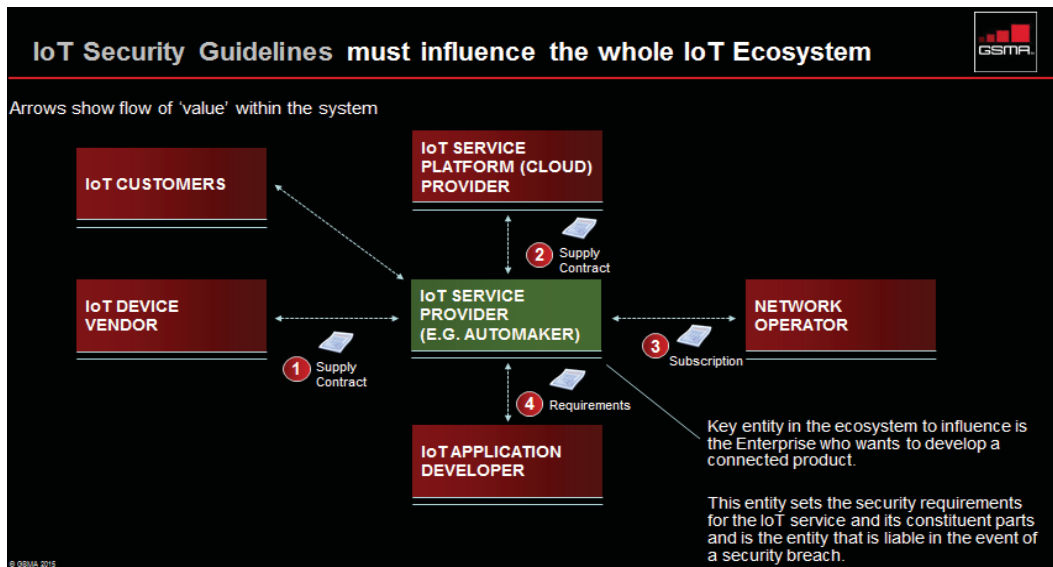
³⁴ WG4 notes that previous work on security and privacy in a Cloud context has previously been undertaken and which led to the formulation of the EC [Cloud SLA Standardisation Guidelines](https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines) (available at <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>)



WG4 policy recommendations

- There are examples of industry best practice that we can leverage to promote best practice across the diverse IoT ecosystem. One example is the ongoing GSMA activity to develop a set of security guidelines for the IoT. Another is the oneM2M project. By way of example, the GSMA guidelines (that will be included in the AIOTI Security Knowledge Base) are underpinned by principles that they must influence the whole IoT Ecosystem and are industry agnostic, as follows:

Figure 4.2 – GSMA’s IoT Security Guidelines



Technological

Specific challenges include

- Securing connections with an increasing amount of devices based on different technologies, and acquired from various suppliers on the global market.
- Multi-criticality: e.g. security under real-time and non-real-time requirements.
- Verification and certification of complex systems and reconciliation of the cycles of security requirement with 'time to market' response.
- Cyber-Security solutions to protect a system when its attack surface is increasing:

WG4 policy recommendations:

- Embed 'safe and secure software'³⁵ design and development methodologies across all levels of device/ application design and development and implement security into that life cycle at the same time.
- Design, deliver and operate adaptive and dynamic end-to-end security over

³⁵ For example, in ISO 27001:2013 certification, a similar concept to "Safe & Secure software" is defined by referring to generally accepted safe coding practices (see for example https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide and <http://cwe.mitre.org/top25/>). The ISMS (Information Security Management Systems) Controls related to software development practices in ISO 27001:2013 generally includes a SECURE DEVELOPMENT POLICY which states that safe development practices as stated above need to be observed.



heterogeneous infrastructures integrating IoT, networks and cloud infrastructures. We recommend underlying standardised OS and hardware security features where architecture permits. The deployment should not be specific or propose a modification of existing OS and hardware already integrated by IoT.

- Develop best practices confirming minimum requirements for provision of secure, encrypted and integrity-protected channel, mutual authentication processes between devices and measures securing that only authorised agents can change settings on communication and functionality.
- Develop a 'New identity for Things' – To date, Identity and Access Management (IAM) processes and infrastructure have been primarily focused on managing the identities of people. IAM processes and infrastructure must now be re-envisioned to encompass the amazing variety of the virtualized infrastructure components. For example, authentication and authorization functions will be expanded and enhanced to address people, software and devices as a single converged framework.
- Develop a Common Authentication architecture – WG4 recommends investigation of a Secure Identity and Trusted Authentication mechanism, for example one which takes into account different authentication standards and will provide a single-sign-on solution for IoT applications moving between different systems.
- Certification – the certification framework and self-certification solutions for IoT applications have not been developed yet. The challenge will be to have generic and common framework, while developing business specific provisions. This framework should provide evaluation assurance levels similar to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), which should serve as the reference.

Societal

Specific challenges include:

- To ensure that potential societal concerns related to security of IoT applications are adequately addressed and so do not unduly restrict take-up of IoT applications.

WG4 Policy recommendations

- The ten recommendations as set out above in relation to privacy are relevant in addressing societal concerns associated with IoT.
- In particular, industry must promote use of privacy/security by design framework (see privacy section above in relation to the Mandate 530 activity which is addressing privacy management in the design, development, production and service provision processes of security technologies.³⁶ This methodology will enable enable manufacturers and/or service providers to design solutions consistent with this approach.

³⁶ <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#>



5 - Liability

Are there legal and regulatory barriers in existing EU laws?

The IoT means a remarkable number of devices can be connected to, and can operate through, a multitude of different technologies and services (which are often provided by many third parties). This raises complexity in terms of dealing with product liability risks. Privacy, security, safety and reliability are intertwined: product liability issues cannot be considered in a vacuum, and need to be considered in the full context of the IoT and associated potential legal risks.

In terms of whether there are legal and regulatory barriers in existing EU laws, WG4 considers that the existing regime needs to be evaluated carefully as the market develops, with an identification of key areas where *some* change may need to be introduced.

Identifying issues raised by IoT

Interdependency

Increasingly, the development of IoT technologies creates sophisticated interdependencies between product and service producers:

- By the nature of its design, an IoT product is dependent on third party technologies to perform its basic functions and to maximise the benefit to the user.
- These dependencies are not static: they can increase, and become more complex, over the life of the product.

Any interdependency gives rise to a number of questions. For example:

- Who is responsible for certifying the safety of the product?
- Who is responsible for ensuring safety on an on-going basis?
- How should liabilities be allocated in the event that the technology behaves in an unsafe way, causing damage?

Further, any interdependency can also give rise to challenges in identifying the root cause of product failures, and in determining where fault lies in the event of a problem. Issues relating to liability when products involve third party components are (of course) not new. They are, however, emphasised when products are increasingly connected and complicated in both design and system integration.

Product vs. service

By their nature, IoT devices utilise electronic data to perform functions. Where that data is not embedded in the device, it can give rise to questions as to the applicability of laws intended to deal with "product liability". Again, this is not isolated to the IoT industry.

The distinctions between "products" and "services" made by courts and authorities when dealing with product liability in the past have been, often, unhelpful. The principles developed previously in this area may not be apt for dealing with the technology being developed now: some evolution in the "products" vs "services" debate is likely to be required. In the UK for example, digital content will soon be regulated (for the purposes of consumer protection) separately from goods and services under the Consumer Rights Act 2015 ("CRA").



Legal implications of "ethical" considerations

IoT technology is increasingly able to replace decision-making functions that were previously only capable of being made through human judgement. The "ethical" implication of this is a common topic among academics and in the popular press. One of the emerging questions is whether there should be a legal or regulatory response to these ethical challenges.

Designers of innovative products are already mindful of new (and significant) areas of legal exposure that may arise in future. In order to support an environment where innovation is encouraged, it may be necessary (in some cases) to legislate to "protect" innovators who produce beneficial technology that is deployed to manage certain risk scenarios. This is to ensure that the risk of potential liability does not act as a deterrent to the development and commercialisation of beneficial technology.

Accountability

The concept of 'accountability' is related to, but distinct from, liability. A detailed analysis of this relationship is outside the scope of this document. However, it is important for companies active in the IoT environment to have policies and procedures in place to ensure and demonstrate compliance by way of adoption of internal policies and mechanisms, which can include certifications³⁷, seals, third-party audits³⁸ attestations³⁹, logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all operations under an organisation's sphere of responsibility. This will demonstrate compliance to external stakeholders, including supervisory authorities that are relevant for the particular industry/market. A pro-active approach to accountability should help address some of the perceived concerns related to liability of certain IoT applications.

Cross-border issues

Consumers are increasingly sophisticated and can circumvent hurdles that sellers put in place to prevent the use of products and/or software in non-intended countries. This is an issue, of course, that is not restricted to the IoT; but IoT technology can give rise to cross-border issues with a higher level of complexity to be resolved.

Product liability issues

"Strict liability" for IoT technology?

At the heart of product liability law in Europe is the "no-fault" liability regime introduced by Directive 85/374/EC (the "Product Liability Directive"). This imposes liability for damages caused by a defective product on the "producer" of that product. Generally, the "producer" is either the manufacturer or the EU-importer.

37 E.g., ISO/IEC 27018 and ISO/IEC 27001 certifications, CSA STAR certification.

38 "Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third-party organisation. In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion." See A.29WP05/2012, Section 4.2, p.22.

39 E.g., SOC 2 attestation, CSA STAR attestation



Are certain IoT technologies "products" within the meaning of this legislation?

Some clarification may be needed over time in that regard. At a broader policy level, there arises the question of whether it is appropriate to extend a "no fault" liability regime to technologies that are more in the nature of a service than a product.

The Product Liability Directive was the result of a long period of negotiation and consideration, and it involved a careful balancing of many (and sometimes competing) interests in order to produce a workable and appropriate liability regime for products. It should not be assumed that the same "balance" will be achieved if this regime is extended to risks beyond its original remit. Consideration of whether the Product Liability Directive is fit for purpose should recognise the benefits of the current developed framework, and should not be rushed: careful thought is prudent before any legislative changes.

Product liability issues generally

Are there outstanding questions around who can be identified as the "manufacturer" or the "importer" of certain IoT technologies?

As connected products develop and become more complicated in both design and connectivity, for certain IoT applications it may become more difficult to prove the elements required for product liability claims to succeed (e.g. defect/negligence etc; identity of the proper defendant). This is brought more sharply into focus in the context of IoT products, in light of the interdependencies and level of complexity involved.

Product safety issues

Who is responsible for pre-market testing and certification?

It is important to assess how requirements for pre-market product testing and certification should be managed when dealing with complex products that operate interdependently with third party technologies, and where those interdependencies may change over the life of the products. It is also necessary to assess who is responsible for such testing and compliance and what level of responsibility should they be held to.

Again, while these questions are not novel, they may be challenging when dealing with certain IoT products. This is because of the level of complexity involved with certain IoT products, and the intertwined nature of diverse products, services, and providers.

Standards

The European product regulatory regime relies heavily on the development and application of standards – a system more flexible and efficient than reliance on prescriptive regulations. However, current technical standards are often inadequate to deal with emerging and innovative technologies, as they were not designed with such technologies in mind, and are not sufficiently flexible. IoT, by its nature, is both emerging and innovative: an on-going challenge will be the development of appropriate standards. Naturally, some work is being done in this area, a referenced by the activity underway within the AIOTI Standards Working Group.

The process for drafting new, and developing existing, standards can be lengthy and require considerable resources and stakeholder involvement. If not done well, standards can lead to



insufficient flexibility for manufacturers of innovative products to demonstrate compliance. While some European standards provide a presumption of compliance with the essential safety requirements of applicable EU product safety law, it is possible for manufacturers to prove compliance with the essential safety requirements by other means (for example, by undertaking adequate internal testing or meeting the requirements of international standards). The basic principle of the New Approach Directives allows flexibility for innovation that still creates safe products.

This is not an issue specific to IoT devices, but a challenge for innovative products (even in established industries) and services generally.

Insurance considerations

The difficulties in the allocation of liability highlighted above present a challenge for the companies involved in the development of IoT technologies, insurers and legislators alike.

Developers of IoT applications need to consider carefully the risks they are running when participating in the development of IoT technology, and the different ways they might be fixed with liability if their involvement is causative of malfunctions leading to injury or damage.

Insurers will need to be ready to offer insurance products which respond to the risks run by companies in a cost effective way. Where the scale and complexity of potential liabilities is too great to be managed at corporate level through conventional liability insurance, it may be necessary to develop arrangements whereby there is a "pooling" of risk. At its simplest, this could be an arrangement whereby all the participants in the development of a particular technology pay in to an insurance scheme designed to meet the cost of claims arising from the operation of that technology. Such schemes are often statutory in nature.

Legislators may also need to consider existing requirements in relation to insurance to ensure they are meaningful in light of developments in IoT technology.

Case studies where change may be required – autonomous vehicles and drone technology

An example of mandatory insurance is motor insurance covering individual users of vehicles. It will be necessary to determine whether this model will be appropriate in an age where the car is not operated by an individual user but by a remote operating system; the way in which the current insurance is required may no longer be relevant. It has been recognised that existing laws concerning manufacturer defects are substantially sufficient for determining liability in an accident involving a car with *some* level of autonomy. However, it has also been stated that a framework for determining liability on the transition of control from the vehicle to the driver of semi-automated technology would provide clarity including the application of current civil and criminal law, so this could be an area of future focus.⁴⁰

Increasingly, drone technology is also in the spotlight in general as new risks and potential legal liabilities emerge. This is an area where insurance considerations are being discussed, and it will be worthwhile to be mindful of the development of (and issues that shape) that discussion.

⁴⁰ See <https://www.kpmg.com/BR/.../Connected-Autonomous-Vehicles-Study.pdf>



Recommendations at policy level/ in legislation

Product liability/safety recommendations

While the perception may be that the IoT raises issues so novel that significant legislative and regulatory intervention is needed, on closer analysis it is apparent that many of the issues are not new or unique to IoT technology.

Case studies of existing regimes that can be flexibly applied – nanomaterials and Consumer Protection Regulation

In most respects, existing regimes are well-equipped to respond to the new challenges within the current structures. Previous experience shows that this process of consideration, clarification, and (as needed) evolution can be the appropriate regulatory and legislative response:

For example, REACH⁴¹ and CLP⁴² do not explicitly refer to nanomaterials. However, nanomaterials are regulated by REACH and CLP because they are covered by the definition of a chemical "substance" in both Regulations. There has been much consideration given to whether the regulatory regime needs to change to specifically refer to nanomaterials – but there has been no knee-jerk reaction in response.

In addition, the UK Consumer Protection from Unfair Trading Regulations (which implemented the Unfair Commercial Practices Directive in the UK) has been used by a National Consumer Protection authority in enforcement action against deceptive trading practices by third parties on social media, which did not exist when the Unfair Commercial Practices Directive Act was adopted in 2005.⁴³ This shows how existing regulation can be relied upon to cater for subsequent developments in technology.

Overall, WG4 considers that there must be a balance between ensuring consumer protection and efficient mechanisms for allocating responsibilities, and ensuring that the measures do not stifle beneficial innovation or lead to unwanted competitive disadvantages.

In some respects, the legal and regulatory principles may benefit from some clarification, where traditional definitions and distinctions allow room for uncertainty. In many cases, the current system/current laws and regulations could be leveraged by using new guidance/guidelines from the European Commission. In this way, the application of such laws can grow with innovation instead of struggling to keep up.

Any policy responses need to be implemented in a way that is sufficiently flexible to deal with the rapid development of technology, while also protecting the overall objectives outlined above.

⁴¹ The Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) provides an over-arching legislation applicable to the manufacture, placing on the market and use of substances on their own, in preparations or in articles.

⁴² Regulation 1272/2008 on classification, labelling and packaging (CLP) of substances and mixtures that must be classified and labelled.

⁴³ See "Investigation into inadequate disclosures in respect of commercial blogging activity", UK Office of Fair Trading, Case CRE-E-25932, 2010



This fundamentally means that policy-makers must maintain close dialogue with industry participants and other stakeholders to ensure:

- unnecessary regulation is avoided
- the approach taken is effective
- the approach is fit for the future, and
- excellent and beneficial innovation is promoted.

Insurance recommendations

Insurers and other risk management experts should be included in the discussions as the management of risk is going to be a key factor in allowing innovators to make progress.

Legislative changes in relation to insurance (especially compulsory insurances such as motor insurance) may be necessary over time to reflect the real changes the IoT makes to the risks run by different constituencies. The best example of this is motor insurance because the IoT will fundamentally change the way that cars are used. Currently, motor insurance laws are drafted on the basis that a human will have control of the car. Fully autonomous vehicles will remove control from the human and give it to a system. This will mean that, in this instance, product liability insurance will be more important than driver insurance. The various participants in the development of IoT technologies may explore the pooling of risk to deal with liabilities on a large scale.

Conclusion

The rapid development of IoT technology may raise a number of product compliance, product liability and insurance-related issues for certain IoT products. While aspects of the IoT give rise to special considerations in these areas, WG4 considers that at present the compliance and liability issues do not give rise to a clear need for new legislation or new types of regulation. Many of the product liability risks highlighted with regard to existing IoT products are not unique to these products and platforms. Such risks exist in established industries and, certainly, with regard to connected technologies in general. In light of this, WG4 considers careful consideration and dialogue should take place before the existing regulatory regime is amended.

It is possible to conceive of future IoT innovations that potentially challenge existing legal regimes (such as the autonomous car). Policymakers should maintain a watching brief with respect to how such technology develops. Forward-thinking responses may be needed to deal with the product liability issues associated with such IoT applications. Changes may be necessary to existing insurance legislation. Issues arise around the distinction between a "product" and a "service", and some clarification in that area may be needed to avoid uncertainty. However, these are not new issues in themselves, and do not give rise to insurmountable challenges within the existing regime.

Key to the development of IoT is striking the balance between ensuring consumer safety and promoting good innovation. Related to this is how to ensure the development of regulatory policy is sufficiently flexible to deal with the needs of an industry that is constantly evolving and which will be considerably different in just 5 years' time. An attempt to deal with the liability issues raised by the IoT through regulation that is not sufficiently flexible will generate inefficiencies and costs, which will benefit only those who operate outside those regimes. The development of policy solutions to the challenges that are raised needs close and on-going dialogue between policy-makers and industry. This will, hopefully, ensure that the approach taken is effective, fit for the future, and promotes excellent and beneficial innovation in an efficient way.



6 – Net Neutrality

Regulatory and Policy context

Given projected requirements for IoT quality of service differentiation, net neutrality is a subject which is of particular relevance to the growth of IoT across the EU. Machina Research estimates that the number of M2M devices requiring some form of differentiation of quality of service is likely to grow significantly over the next few years making up over 50% of all M2M devices by 2020. Those M2M devices requiring comprehensive or stringent Quality of Service (QoS) standards are estimated to increase from 1 billion to 3 billion units.⁴⁴ Net Neutrality is also an important topic for WG4 as it is of ‘horizontal’ relevance – i.e. regulation could materially impact on both IoT suppliers and customers alike. It is therefore an important part of the policy landscape affecting the broader IoT ecosystem.

In terms of the overarching regulatory framework, a political agreement, incorporating provisions on net neutrality, was reached on the Telecom Single Market Regulation (the ‘Regulation’) in July 2015 between the European Parliament, Council and Commission.⁴⁵ This text represents the most comprehensive pan-European net neutrality legislation to date and has been assessed by WG4 as part of its analysis of net neutrality and the IoT.⁴⁶

It will be important to the success of the Internet of Things to interpret these rules and understand how they play out in the IoT ecosystem. Clarification by regulators will be necessary to allow IoT actors to obtain legal certainty as to how their networks and services will be interpreted in this context. Misinterpretation of the rules could lead IoT providers to avoid launching, or restricting, certain services to avoid the risk of falling foul of the Regulation.

The Body of European Regulators of Electronic Communications (BEREC) has been charged under the Regulation with laying down guidelines for implementation of the net neutrality provisions by national regulatory authorities (NRAs) within nine months of the adoption of the Regulation. WG4 considers that thought should be given to how these rules will play out in the IoT context and would like to take this opportunity to provide recommendations on the issues at hand.

Service categories under the Regulation

In terms of application of the net neutrality rules, there are three categories of service that matter in IoT’s relation to the Regulation.

Internet Access Services

Internet access services (IAS), broadly speaking publicly available electronic communications services that provide access to the internet, are subject to the traffic

⁴⁴ Source: Machina Research (2015), DNA of M2M, www.machinaresearch.com.

⁴⁵ This text is expected to be formally adopted by the Council and Parliament in September/ October and enter into law in November 2015. It will apply from end of April 2016 or, in certain circumstances, end of December 2016.

⁴⁶ WG4 notes that some provisions relating to an open internet already exist under EU law. The 2009 revision of the Telecoms Framework ensures that internet users are able to access content, applications and services of their choice, introduced transparency measures and enabled minimum quality of service requirements to prevent service degradation. Moreover, at the national level, the Netherlands and Slovenia already adopted net neutrality laws in 2012 and 2013 respectively.



management and related consumer protection requirements of the Regulation.⁴⁷ Therefore, certain IoT applications will run over IAS and will be affected to the extent that the IAS provider is required not to discriminate against their application within the terms of the Regulation.

Specialised Services

‘Specialised services’, although not defined as such in the Regulation are services other than internet access services that are optimised for specific content, applications or services. The Regulation notes that such specific quality levels may be required by some new machine-to-machine services.

The Regulation introduces two important safeguards in the Regulation to ensure that specialised services are not used to circumvent the net neutrality rules and do not negatively impact the general quality or availability of the internet access service:

- The first of these states that optimization for specific content, applications or services must be necessary to meet a specific quality level.⁴⁸
- The second safeguard only allows for the provision of such services if there is sufficient capacity to do so alongside any IAS provided.

Therefore, certain IoT services will fall under the ‘definition’ of specialised services, and hence will need to take care not to impact the quality or availability of IAS and to assess whether optimization is necessary to meet the quality level envisaged.⁴⁹

Services which are neither IAS nor Specialised services

The third category of service are those which are neither IAS nor specialised services and hence fall outside the scope altogether and are not subject to any requirements. The important distinction between these and specialised services appears to hang on whether these services are being provided by providers of electronic communications to the public.⁵⁰

Many more IoT services will fall entirely outside the scope of the Regulation as they do not relate to public provision of electronic communications.

Case studies

In order to inform the policy discussion around the application of Net Neutrality rules to IoT applications, WG4 sets out five IoT case studies which we believe will help clarify the regulatory environment and ensure there are no barriers to IoT take-up across the EU. For

⁴⁷ Article 2(2) “internet access service” means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used

⁴⁸ Regulators will have the powers to verify if this is objectively necessary as opposed to granting general priority over comparable content, which would be infringing the non-discrimination requirement for traffic management in the provision of Internet access services and the ban against paid prioritization.

⁴⁹ It is worth noting that in this circumstance, the statutory responsibility is on the service provider in question to meet the obligations. Other actors in the IoT ecosystem may need to design their elements of the solution with this in mind but are not directly responsible.

⁵⁰ This is defined in the Regulation as: Article 2(1) “provider of electronic communications to the public” means an undertaking providing public electronic communications networks or publicly available electronic communications services;



each IoT case study, WG4 considers the position vis-à-vis the Regulation, given the approach that the Regulation takes to IAS and specialised services.

1. Telecommunications service provider offers IoT services alongside IAS

Case study

A telecommunications service provider offers an Internet access service to a location over the same connection. An example could be offering home security and automation (incorporating video and door security) and Internet access to a residential household. The home and security automation services are connected over the Local Area Network to the access network in order to allow for remote control and other functionality.

Analysis

In this case, a provider of electronic communications to the public (the IAS in particular) is offering the home security and automation service and hence the automation service qualifies as a specialised service. They would therefore be subject to the optimisation as necessary requirement and to not negatively impact the quality or availability of the IAS by making sure there is sufficient capacity to offer this alongside the IAS.

Recommendation

In order to determine whether optimisation is necessary (consistent with the requirements of the Regulation), WG4 believes it should be measured against the specific requirements as requested by the customer. As such, in this instance the home security service would require optimisation to guarantee reliability of data transmitted in the case of a burglary. Without reliable data the purpose of the service itself would be defeated – it is therefore a necessary requirement.

2. IoT application strikes deal with telecommunication service provider for quality of service

Case study

The IoT application provider has an interest in establishing a guaranteed quality of service for their offering and pays the telecommunications service provider (in this case a mobile operator) to make such an agreement. The end user subscribes to an Internet access service provided by the telecommunications service provider alongside the IoT application.

An example could be a smart grid fault repair that provides real time service repair in emergency situations. The fault repair functionality sends signals via a mobile network in the case of an incident. The smart grid operator wants to guarantee that such a signal always gets through immediately, over and above the IAS provided to the end-user in the home for IAS, and hence contracts with the mobile operator to provide such service levels.

Analysis

Given the provision of the IAS, the mobile operator has the responsibility to ensure that the fault repair functionality is subject to the requirements of the specialised service, namely the necessary optimization requirement and impact on the IAS. From the point of view of the smart grid operator, they do not have any direct obligations but will have to make sure their service is devised in a way that will allow the service provider to meet their obligations.



Recommendation

In this case, it is hard to imagine that the service would impact the IAS in a meaningful way. The mobile operator is likely to be serving a large population with the same capacity such that prioritisation of the smart grid repair functionality is unlikely to have a significant impact and in any case, that prioritization would be an irregular occurrence and hence not have a general impact on the quality or availability of the IAS.

3. Provision of independent IoT application/ service over best-effort IAS

Case study

This is likely for many consumer-facing IoT applications, such as smart thermostats that connect over the LAN for remote control, or wearables that connect locally to a mobile device in order to upload location and health data.

Analysis

The IoT application or service has no specific deal in place with the telecommunications provider and offers their service over the best-effort Internet without additional guarantees of quality of service. Technical requirements such as low latency or packet loss are not deemed necessary in order to offer the service at the requisite level.

Recommendation

Under these circumstances, the application does not qualify as either an IAS or a specialised service and the IoT provider has no direct obligations to meet any of the provisions under the Regulation.

4. Private IoT network

Case study

The IoT networks in this situation are not available to the public. In many cases these will be the internal corporate networks of private or public sector entities.

Analysis and recommendations

To examine the implications for the implementation of the Regulation's net neutrality rules, we will break these private networks down into three subgroups

1) Private networks managed by a telecommunication service provider that do not include internet access

- Under the first subcategory, a telecom service provider manages a private network that is not an IAS. Take smart farming as an example. A smart agriculture network may collect information on crop yields, soil mapping, fertilizer applications, weather, machinery and animal health. A telecom service provider may provision and manage such a network but would not be providing any internet access services to the owners of the farm. Such private networks should not be subject to any of the provisions of the Regulation.

2) Private networks managed by a telecommunication service provider that include internet access

- Under this second subcategory, a telecom service provider's offer to an enterprise or other entity may include an internet service alongside other types of network. Such



an example may include an optional closed WiFi service offered by a telecommunications service provider to a car owner (in addition to the vehicle diagnostics service provided to the automotive manufacturer) and which is not an IAS, given it is limited only to the passengers within the car.

3) Private networks where the telecommunication service provider does not have a role beyond backhaul.

- In the third subgroup, either the enterprise itself manages the private network or a third party uninvolved in the provision of IAS does. In this situation, the role of the telecom service provider (if at all) is limited to backhaul at the point at which the private network connects to the public network. The Regulation would not be applicable to such a network.

5. Non-traditional ‘internet access provider’ alongside IoT services

Case study

Like the second subcategory in the section above, this situation involves the provision of a private network alongside internet access, but in this case at least one part of the internet access is publicly available. One could consider a smart city where sensor networks and other interconnected technologies are used to manage traffic flows, waste and water or save on energy from lighting, alongside an RLAN network for use by all citizens (e.g. the public network includes access to government and local information services).

Analysis

In many cases these networks will share capacity, with priority given to the private networks whose use cases are more essential than the public network. The pertinent question, therefore, is whether such public provision of internet access qualifies as an IAS and as a result whether the private networks are seen to be specialised services.

Recommendation

WG4 considers that this scenario should be interpreted based on Article 14.6 of the original Commission proposal on the draft Regulation. This article was deleted when the Parliament and Council decided to focus the Regulation specifically on roaming and net neutrality, but gives us our best indication of the Commission’s thinking. It states “*An undertaking, public authority or other end user shall not be deemed to be a provider of electronic communications to the public solely by virtue of the provision of public access to radio local area networks, where such provision is not commercial in character, or is merely ancillary to another commercial activity or public service which is not dependent on the conveyance of signals on such networks.*”

As an IAS is a publicly available electronic communication service by definition, and a provider of electronic communications to the public is one who provides such services, it follows from the clause that public access to RLANs should not be considered access to an IAS, as defined in the Regulation. WG4 considers that the provision of internet access to the public under the scenario envisaged in this section does not qualify as the provision of an IAS, which is subject to the open internet access provisions. Furthermore, the private IoT networks running in parallel to the public offering would not qualify as specialised services and hence would not be subject to the requirement not to negatively impact the quality of the IAS or the necessary optimisation requirement.