OECD Digital Economy Outlook 2015

OECD

OECD Digital Economy Outlook 2015

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please cite this publication as:
OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/9789264232440-en

ISBN 978-92-64-23227-3 (print)
ISBN 978-92-64-23244-0 (PDF)

Revised version, December 2015.
Details of revisions available at: *www.oecd.org/about/publishing/Corrigendum-DigitalEconomicOutlook2015.pdf*

Photo credits: © Victoria - Fotolia.com; © Jumpeestudio - Fotolia.com

Corrigenda to OECD publications may be found on line at: *www.oecd.org/publishing/corrigenda*.

© OECD 2015

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of the source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to *rights@oecd.org*. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at *info@copyright.com* or the Centre français d'exploitation du droit de copie (CFC) at *contact@cfcopies.com*.

Foreword

The OECD Digital Economy Outlook is a biennial series which examines and documents evolutions and emerging opportunities and challenges in the digital economy. It highlights how OECD countries and partner economies are taking advantage of ICTs and the Internet to meet their public policy objectives. Through comparative evidence, it informs policy makers of regulatory practices and policy options to help maximise the potential of the digital economy as a driver for innovation and inclusive growth.

This publication replaces and builds upon the OECD Communications Outlook and Internet Economy Outlook (formerly OECD Information Technology Outlook) to provide a more holistic overview of converging trends, policy developments and data in the digital economy on both the supply and demand sides.

The Digital Economy Outlook 2015 has been prepared by the OECD Secretariat under the guidance of the OECD Committee on Digital Economy Policy (CDEP), chaired by Jörgen Abild Andersen (Denmark). It has benefited from the input of delegates to the Committee and its Working Parties on Communications Infrastructure Services Policy (CISP), chaired by Tracey Weisler (USA), on Measurement and Analysis in the Digital Economy (MADE), chaired by Luis Magalhes (Portugal), and on Security and Privacy of the Digital Economy (SPDE), chaired by Jane Hamilton (Canada). A large part of its content builds on the responses by Member countries and Partner economies to the OECD Digital Economy Questionnaire sent in June 2014.

The Digital Economy Outlook has been declassified by the Committee on 8 May 2015.

The Secretariat team which drafted the Digital Economy Outlook is part of the OECD Directorate for Science, Technology and Industry headed by Andrew Wyckoff, and worked under the direction of Anne Carblanc assisted by Cristina Serra Vallejo for the overall coordination. Authors include, by alphabetical order, Brigitte Acoca, Frederic Bourassa, Agustín Díaz Pinés, Michael Donohue, David Gierten, Pedro Herrera Gimenez, Aaron Martin, Pierre Montagnier, Hajime Oiso, Sam Paltridge, Christian Reimsbach-Kounatze, Elettra Ronchi, Cristina Serra Vallejo, Vincenzo Spiezia, Sukham Sung, Rudolf van der Berg and Verena Weber. Contributions have been received from the OECD Public Governance and Territorial Development directorate, in particular from Arthur Mickoleit and Barbara Ubaldi. Geoff Huston from Potaroo and Karine Perset from ICANN have provided the team with useful insights as did Colin Blackman, Research Fellow at the Centre for European Policy Studies.

The sections on Brazil, Colombia and Egypt have been drafted respectively by Rafael Moreira and Lorrayne Porciuncula, by Alejandro Delgado and Sofía González, and by Dr. Noha Adly and Nevine Tewfik. We would like to thank the Ministry of ICT in Egypt and the Ministry of Information and Communication Technologies (ICT) from Colombia, in particular former Minister Diego Molano, for their collaboration to this edition.

Finally, the assistance of Teligen, a division of Strategy Analytics Ltc., CISCO, Matthew Zook from ZookNIC, Measurement Lab (M-Lab), Neftcraft and Shodan is gratefully acknowledged, as is the assistance of other colleagues in the OECD who have provided data for the analysis.

Table of contents

Executive summary 11

Chapter 1. **An overview of the digital economy** 15
1.1 Introduction 16
1.2 National digital strategies and ICT policy priorities 20
1.3 Main trends in the ICT sector 36
1.4 Uptake and use of ICTs across the digital economy 46
1.5 New and evolving business models 53
1.6 The Internet of Things 60
1.7 Trust, competition and network neutrality 62
1.8 Internet governance and policy outlook 71
Notes 76
References 77
Annex 80

Chapter 2. **The foundations of the digital economy** 83
2.1 The ICT sector 84
2.2 Communication market size and network development 103
Notes 128
References 128

Chapter 3. **The growing and expanding digital economy** 131
3.1 ICT adoption and use across economic and social activities 132
3.2 New and evolving business models and markets 144
3.3 Measuring the impact of the digital economy: Growth, productivity and jobs 160
Notes 167
References 167
Annex 170

Chapter 4. **Main trends in communication policy and regulation** 171
4.1 Industry consolidation and policy responses 174
4.2 Convergence: Service bundles and the rise of over-the-top operators 180
4.3 The network neutrality debate 185
4.4 Advanced fixed networks and regulatory issues 193
4.5 Wireless developments 198
Notes 205
References 206

Chapter 5. **Trust in the digital economy: Security and privacy** 209
5.1 The growing profile of digital security and privacy risks 210
5.2 The job market for security and privacy professionals 215
5.3 Privacy enforcement and security response 219
5.4 Other selected trends impacting trust 224
Notes 235
References 235

Chapter 6. **Emerging issues: The Internet of Things** 239
6.1 The Internet of Things: Developments, definition and main elements 240
6.2 Technical developments in the Internet of Things 247
6.3 Fostering public policy goals with the Internet of Things 259
6.4 Autonomous machines and public policy 272
Notes 276
References 277

Tables

2.1. Fixed broadband baskets, download speeds, minimum upload speed and bandwidth usage profile 116
2.2. Mobile baskets, comparison between September 2012 and September 2014, USD PPP 120
2.3. Elements included in the bundle baskets 121
2.4. Five views on top ten largest networks in the world, 2014 125
4.1. Mobile mergers in OECD countries 177
4.2. Recent entry into mobile markets in the OECD area 177
4.3. Examples of regulatory tools used to promote competition in spectrum auctions 202
5.1. Ratio of technological experts to total staff in privacy authorities for selected countries 220
6.1. A selection of IoT-related projects from Kickstarter 242
6.2. Number of devices per household 256

Figures

1.1. Strategic areas of Mexico's Prosoft 3.0 28
1.2. Top increasing ICT policy areas 34
1.3. Amount of venture capital invested in Internet-specific companies in the United States 37
1.4. Growth in monthly semiconductors worldwide market billings 38
1.5. Top ten exporters of ICT goods, 2013 38
1.6. Exporters of ICT services, 2013 39
1.7. Business expenditure in R&D, 2013 40
1.8. ICT-related patents, 2010-12 41
1.9. Share of ICT sector in total value added, 2013 42
1.10. ICT sector and total employment growth in the OECD area 43
1.11. Employment of ICT specialists across the economy 43
1.12. Growth in communication access paths by technology 45
1.13. How enterprises make use of selected ICT applications, 2014 48
1.14. Gaps in the use of enterprise resource planning software, 2014 48
1.15. Use of cloud computing by enterprises, 2014 49
1.16. Gaps in Internet usage by age, 2014 50

1.17. Top 30 central government Twitter accounts 53
1.18. Smartphone use of selected geo-location services, 2013. 55
1.19. Digital shares in content markets, US and EU, 2013. 57
1.20. Customer involvement in product development, 2013 60
A.1. Current ICT policy priorities, 2014 81
A.2. Evolution of ICT policy priorities. 82
2.1. Growth of the ICT sector, December 2007 – December 2014 85
2.2. Worldwide semiconductor market by region, 1990-2016. 86
2.3. Quarterly venture capital investments and trends of ICT VC shares in the United States, Q4 1995- Q4 2014. 86
2.4. Value added of ICT sector and sub-sectors, 2013 87
2.5. Evolution of ICT sector value added, 2001, 2007 and 2013. 88
2.6. Employment in the ICT sector and sub-sectors, 2013 89
2.7. Evolution of ICT sector employment, 2001, 2007 and 2013 89
2.8. ICT specialists in OECD countries, 2014 90
2.9. Share of national value added and employment accounted by foreign affiliates in the ICT sector, 2013 90
2.10. World exports of ICT goods, 2001, 2007 and 2013 91
2.11. OECD and major exporters of ICT services, 2001, 2007 and 2013 92
2.12. Trade in ICT goods and services – gross exports and value added, 2011 93
2.13. ICT and total business expenditure in R&D intensities, 2013. 94
2.14. Business R&D expenditures in the ICT sector, 2013 95
2.15. Specialisation in ICT-related patents, 2000-02 and 2010-12 96
2.16. Top 25 combinations between ICTs and other technologies in patent applications, 2000-02 and 2010-12 96
2.17. International cooperation networks in ICT-related patents, 2010-12 97
2.18. International cooperation networks in ICT-related science fields, 2011-12 98
2.19. Top 20 applicants' share in ICT and audio-visual-related designs, 2005-08 and 2010-13 99
2.20. ICT-related trademarks, top 20 applicants, 2005-08 and 2010-13 99
2.21. Trends in telecommunication revenue, investment and access paths, 1980-2013 104
2.22. OECD fixed (wired) broadband subscriptions per 100 inhabitants by technology, June 2014. 106
2.23. Growth of fibre connections among countries reporting fibre subscriptions, June 2012 – June 2014 107
2.24. Percentage of fibre connections in total fixed broadband subscriptions, June 2014. 108
2.25. OECD wireless broadband subscriptions per 100 inhabitants, by technology, June 2014. 109
2.26. Fixed (wired) broadband penetration by speed tiers, June 2014 109
2.27. Average and median advertised download speeds, fixed broadband, September 2014 111
2.28. Average advertised download and upload speeds, fixed broadband by technology, September 2014 112
2.29. Mobile broadband advertised speed ranges, logarithmic scale, September 2014 112
2.30. Actual download speeds, fixed or unspecified broadband, Akamai, M-Lab and Ookla, Mbit/s 113

2.31. Global IP traffic, 2005-13 114
2.32. Telecommunication revenue per communication access path, 2011 and 2013 114
2.33. Investment in telecommunications as % of total revenues, spectrum fees excluded, 2011 and 2013 115
2.34. Fixed broadband basket, low use, >1.5/2 Mbps, USD PPP 117
2.35. Fixed broadband basket, high use, >25/30 Mbit/s, USD PPP 117
2.36. Fixed broadband subscription price ranges, September 2014, all platforms, logarithmic scale, USD PPP 118
2.37. Fixed broadband prices per megabit per second of advertised speed, September 2014, USD PPP 119
2.38. Laptop mobile broadband basket, 2 GB, September 2014, USD PPP 121
2.39. Triple-play basket (30 Mbps download speed and 200 GB, unlimited fixed calls, premium pay television including sports and movies), April 2014, USD PPP 121
2.40. "Basic" quadruple-play – at least 10 Mbps broadband download speed and 25 GB capacity, fixed-line connection, basic pay-tv and 30-call mobile basket, April 2014, USD PPP 122
2.41. Routed AS numbers per 100 000 inhabitants, 2012 and 2014 123
2.42. IPv4 depletion per RIR, 2014 126
2.43. Routed IPv4 addresses per inhabitant, mid-2014 126
2.44. Numbers of IPv6 allocations per year, top ten OECD countries, 1999-2014 (year-end) 127
2.45. IPv6 user ratio, October 2014 127
3.1. Broadband connectivity by size, 2010 and 2014 132
3.2. Enterprises with a website or home page by size, 2009 and 2014 133
3.3. Diffusion of selected ICT tools and activities in enterprises, 2014 134
3.4. Use of enterprise resource planning software, by size, 2010 and 2014 135
3.5. Enterprises using cloud computing services by size, 2014 136
3.6. Enterprises using cloud computing services by type of services, 2014 137
3.7. Cloud computing services perceived effects in 15 EU countries 137
3.8. Internet users by age, 16-24 and 65-74 year-olds, 2014 138
3.9. The diffusion of selected online activities among Internet users, 2013-14 139
3.10. Diffusion of online purchases including via handheld devices, 2007 and 2014 140
3.11. Use of cloud computing by individuals in selected OECD countries by age class, 2014 142
3.12. Problems with the use of e-government services, 2013 142
3.13. Individuals who attended an online course, 2007 and 2013 144
3.14. Access to information on social networks, 2013 145
3.15. Sharing of information on social networks, 2013 146
3.16. Use of location-based services on smartphones, 2013 146
3.17. Purchasing of goods or services on smartphones 148
3.18. Mobile banking uptake 149
3.19. Dematerialisation of major content markets, 2013 151
3.20. Major players in online and mobile advertisement 154
3.21. Planned and implemented uses of data from electronic health record systems 156

3.22. Enterprises engaging with customers in product development, 2013 159
3.23. Global crowdfunding volumes 160
3.24. ICT investment by capital asset, 2013 161
3.25. The dynamics of ICT investment, 2001, 2007 and 2013 161
3.26. Contribution of ICT and non-ICT investments to GDP growth, 2008-13 162
3.27. Contribution of ICT and non-ICT investments to GDP growth, 2001-07 162
3.28. Labour productivity of the ICT sector and total economy, 2013 163
3.29. Growth in total labour productivity growth accounted for by the ICT sector, 2001-13 164
3.30. Contribution of the ICT sector to total employment growth in the OECD, 2001-13 164
4.1. Wired broadband speed tiers, number of broadband providers 175
4.2. Virgin Media's VIP Collection, United Kingdom 183
4.3. Operators applying some level of restriction, weighted according to their total number of users 184
4.4. Average termination charges for outgoing traffic, United States to regions (top), outgoing minutes from United States carriers to regions (bottom) 198
4.5. MTRs in OECD countries, USD 203
4.6. Average and maximum MTR in OECD countries, USD 204
5.1. Number of (ISC)^2 certified individuals worldwide, 2003-13 216
5.2. Total number of IAPP members, 2001-14 217
5.3. Annual income of a privacy professional in a Fortune 1000 company 218
5.4. Number of full-time employees in privacy enforcement authorities worldwide, March 2014 219
5.5. Attendants to the Annual FIRST Conference 224
5.6. Types of data breached in California, 2012-13 227
5.7. Use of DNSSEC validation, 2015 231
5.8. Company transparency reporting, 2009-14 233
6.1. Main enablers of the Internet of Things 244
6.2. Machine-to-machine applications and technologies by dispersion and mobility 248
6.3. Number of M2M SIM cards per country 257
6.4. Number of M2M/embedded mobile cellular subscriptions, per 100 inhabitants 257
6.5. Devices online, top 25 countries 259
6.6. Devices online per 100 inhabitants, top OECD countries 259

Follow OECD Publications on:

http://twitter.com/OECD_Pubs

http://www.facebook.com/OECDPublications

http://www.linkedin.com/groups/OECD-Publications-4645871

http://www.youtube.com/oecdilibrary

http://www.oecd.org/oecddirect/

This book has...

StatLinks

A service that delivers Excel® files from the printed page!

Look for the *StatLinks* at the bottom of the tables or graphs in this book. To download the matching Excel® spreadsheet, just type the link into your Internet browser, starting with the *http://dx.doi.org* prefix, or click on the link from the e-book edition.

© OECD 2015

Executive summary

The digital economy now permeates countless aspects of the world economy, impacting sectors as varied as banking, retail, energy, transportation, education, publishing, media or health. Information and Communication Technologies (ICTs) are transforming the ways social interactions and personal relationships are conducted, with fixed, mobile and broadcast networks converging, and devices and objects increasingly connected to form the Internet of Things.

How can OECD countries and partner economies maximise the potential of the digital economy as a driver for innovation and inclusive growth? What are the evolutions in the digital economy that policy makers need to consider and the emerging challenges they need to address?

The full potential of the digital economy has yet to be realised

Global trade for ICT manufacturing and especially ICT services continues to grow. Business Enterprise Expenditures on Research and Development and the recent increase in ICT-related patents reveal the key role played by the ICT sector in innovation. Broadband markets are expanding, with an increase in wireless broadband subscriptions - reaching close to 1 billion subscriptions in the OECD area - offsetting a decrease in fixed telephony. The performance of communication networks is improving with the deployment of fibre and 4G, while prices are declining, in particular for mobile services.

- There is significant potential to expand coverage and improve the quality of fixed and mobile broadband infrastructures. New OECD methodology for measuring advertised fixed broadband speeds will facilitate governments' ability to maintain progress towards the Internet of Things.
- With growing demands placed on networks and more spectrum resources needing to be allocated to mobile communications, the complementarity of fixed and mobile networks will need to be exploited. Fixed infrastructures are critical for offloading and backhauling wireless traffic and to enable better use of available spectrum. Policy makers are testing innovative licensing schemes to increase efficiency in the use of spectrum.
- The potential is huge for increased adoption and use by firms of ICTs and the Internet to boost growth and innovation, across all sectors. While most firms in OECD countries have a broadband connection – 95% of all enterprises with more than 10 employees in 2014 – few use enterprise resource planning software (31%), cloud computing services (22%) or receive electronic orders (21%). Differences among countries and between small and large firms remain considerable.

- New business models based on collaborative production methods, such as crowdfunding platforms, and new "sharing economy" platforms challenge existing regulation of established markets and call for balanced policy responses that enable innovation while protecting the public interest.
- The scope for further uptake is also significant for individuals. Consumers account for a small portion of e-commerce, with up to 90% of e-commerce being business-to-business transactions. Despite wide diffusion, intensity of Internet usage continues to vary, particularly for activities associated with a higher level of education such as e-government, e-commerce and online banking.

Boosting economic and social growth through national digital agendas

Governments in OECD countries are increasingly aware of the need to develop the digital economy in a strategic manner, to expand its benefits and respond to key challenges such as reducing unemployment and inequalities, and lifting people out of poverty. Today's national digital strategies cover issues ranging from business creation and productivity growth to public administration, employment and education, health and aging, environment and development. Overall, governments are increasingly aware that "Internet policy making" depends on a set of coherent, whole-of-government policies:

- Infrastructure – which provides a foundation for new business models, e-commerce, and new collaborative scientific and social networks - needs to be of high quality, accessible to all and available at competitive prices.
- With competition in the digital economy being challenged by several major shifts including technical convergence and the integration of business models among telecommunication providers and new Internet players, governments must also engage in efforts to protect competition, lower artificial barriers to entry, and strengthen regulatory coherence. The consolidation of mobile markets must not reduce innovation or the ability of other actors to compete.
- Encouraging higher uptake of ICTs is essential, particularly by government and businesses including SMEs.
- Trust in the reliability and security of online networks, services and applications need to be secured, and users assured that their privacy and consumer rights are protected. The OECD has called on leaders and decision makers to integrate digital security and privacy risk management in their broader economic and social risk management frameworks, rather than addressing these issues as separate technical and legal challenges. Cybersecurity strategies should be supplemented with national privacy strategies, so as to address privacy issues in a co-ordinated, holistic manner and identify the limitations society is willing to accept to serve collective public interests.
- Through ICT-related education, training and re-skilling, people must be equipped with the appropriate skills to make use of ICTs and to manage risks to their online social and economic activities, with a view to fostering entrepreneurship, employment and e-inclusion.
- Recognising the potential disruptive effects of going digital is critical. Governments will need to facilitate the transition of workers to new types of digital jobs.

Internet governance: A policy priority for the years to come

The Internet community is developing a proposal to transition oversight of the Internet's technical resources from the United States government to the global multi-stakeholder community. In September 2015, the United Nations will launch the post-2015 development agenda, setting sustainable development goals, which are likely to include increased access to ICTs and the Internet to create an inclusive and global digital economy. In December 2015, the mandate of the multi-stakeholder-led Internet Governance Forum (IGF) will come up for renewal.

Underlying these initiatives is the fundamental need to preserve the openness of the Internet. The conception of the Internet as an open platform, where businesses, citizens and governments can serendipitously innovate and develop applications and services, has enabled numerous innovations in the digital economy. In recent years, however, concerns have emerged that the economic and social benefits brought by the open and decentralised architecture of the Internet and by the free flow of trans-border data may be affected, directly or indirectly, by issues such as territorial routing, local content or data storage requirements, network neutrality, universal acceptance of multilingual domain names and the creation of alternative networks.

The benefits of, and risks to, an open Internet will be discussed by ministers and other high-level stakeholders at the forthcoming OECD Ministerial Meeting in 2016, along with other key issues pertaining to global connectivity, the Internet of Things, demand-side initiatives to foster innovation and trust in the digital economy, and ways to foster job creation and develop the skills needed to maximise the benefits of the digital economy.

© OECD 2015

Chapter 1

An overview of the digital economy

The expansion of the digital economy has acted as a driver of economic growth in recent years and is transforming society as a whole. This chapter provides an overview of the current situation and likely evolution of the digital economy, and a synthesis of the publication. It highlights progress made and challenges ahead, drawing on national strategies, and concludes with an examination of the broader context of Internet governance issues.

1.1 Introduction

The digital economy is growing quickly (OECD, 2013a). It permeates the world economy from retail (e-commerce) to transportation (automated vehicles), education (Massive Open Online Courses), health (electronic records and personalised medicine), social interactions and personal relationships (social networks). Information and Communication Technologies (ICTs) are integral to professional and personal life; individuals, businesses and governments are increasingly inter-connected via a host of devices at home and at work, in public spaces and on the move. These exchanges are routed through millions of individual networks ranging from residential consumer networks to networks that span the globe. The convergence of fixed, mobile and broadcast networks, along with the combined use of machine-to-machine (M2M) communication, the cloud, data analytics, sensors, actuators and people, is paving the way for machine learning, remote control, and autonomous machines and systems. Devices and objects are becoming increasingly connected to the Internet of Things, leading to convergence between ICTs and the economy on a grand scale (Chapter 6).

This publication documents evolutions and emerging challenges in the digital economy and highlights ways in which OECD countries and partner economies are taking advantage of ICTs and the Internet to meet public policy objectives. It provides evidence and case studies to help inform policy makers of regulatory practices and policy options to help maximise the potential of the digital economy as a driver for innovation and inclusive growth.

National digital agendas are critical for boosting economic and social growth

Going digital can bring countries closer to sustained prosperity. Governments in OECD countries are increasingly cognisant of the need to develop the digital economy in a strategic manner to expand its benefits and respond to key challenges such as reducing unemployment and inequalities, and lifting people out of poverty. The growing number of national digital agendas highlights the increasing recognition that effective "Internet policy making" depends on a set of coherent policies, developed in close co-operation with all stakeholders, that build on the country's strengths and take advantage of the open, decentralised and scalable nature of the Internet (OECD, 2011).

The conditions that underpin the digital economy are closely interdependent. Infrastructures used to enable communication within and across borders need to be of high quality, accessible to all and available at competitive prices (Chapter 2). They provide a foundation for applications and services based on new business models, the development of e-commerce, enhanced production methods, and new collaborative scientific and social networks (Chapter 3). All these positive outcomes are dependent on building trust in the reliability and security of online networks, services and applications. Users must also be assured that their online privacy and consumer rights are protected (Chapter 5). Finally, people must be equipped with the appropriate skills to make use of ICTs and digital

processes and to manage risks to their online economic and social activities (Chapters 3 and 5). Ensuring that all these conditions are met requires a whole-of-government approach.

The analysis of national digital strategies confirms the relevance of such an approach for OECD countries and emerging economies, such as Brazil, Colombia and Egypt. On the supply side, all countries aim to further develop telecommunications infrastructures and to promote the ICT sector. On the demand side, they strive for higher uptake of ICTs by government and by businesses and SMEs in particular. Fostering the development of digital local content creation remains an important goal alongside improvements in public administration, healthcare, transportation and education. Strengthening digital security and privacy also ranks high, although the resources allocated to improving digital privacy protection are persistently lower than for security. Countries are also increasingly considering the need to promote ICT-related education, training and re-skilling in conjunction with measures to foster entrepreneurship and employment. In so doing, several countries also aim to further e-inclusion, especially for older people and disadvantaged social groups (Section 1.2).

However, leveraging the innovation and growth potential of the digital economy also calls for governments to facilitate the transition towards going digital and to recognise the potential disruptive effects. Accordingly, policy makers in charge of the digital economy in OECD countries and partner economies are starting to work with their counterparts in labour and education to leverage the potential of new digital markets for employment growth, and to facilitate the transition of workers to new types of digital jobs.

Despite passing several milestones, the digital economy has not yet reached full potential

Overall, the outlook for the ICT sector in 2015 is positive although the sector has not yet fully recovered in all countries from the double-dip crisis that struck the world economy in 2007 and 2009. ICT venture capital investment is on the rise and back to its highest level since the dot-com bubble. The share of ICT goods and services in OECD total value added has remained stable, while ICT global trade has continued to grow for ICT manufacturing and especially ICT services. ICTs play a key role in innovation activities, as demonstrated by Business Enterprise Expenditures on Research and Development (BERD) in the ICT sector and the recent increase in ICT-related patents (Chapter 2).

Broadband markets continue to grow with an increase in wireless broadband subscriptions offsetting a decrease in fixed telephony, confirming a trend towards mobile-fixed substitution. Fixed and mobile broadband subscriptions reached 344.6 million and 983.4 million subscriptions, respectively in June 2014, with corresponding annual growth of 3.7% and 14.2% over the past two years in the OECD area. Telecommunication revenue and investment levels remain relatively stable. However, the performance of communication networks is improving with the deployment of fibre and the mobile telephony norm Long Term Evolution (4G), while prices are declining, in particular for mobile services (Chapter 2). Overall, global Internet traffic grew by 20% annually and the number of people using the Internet reached 2.9 billion worldwide.

Although ICTs and the Internet already contribute significantly to digital economies worldwide, efforts to improve broadband speed, ensure access to Internet addresses for 1 billion users in developing economies (Chapter 2), and increase the use of broadband to generate wealth (Chapter 3), hold considerable potential to boost growth in the years ahead.

Available evidence for OECD countries reveals significant potential to expand coverage and improve the quality of fixed and mobile broadband infrastructures. The new OECD methodology for measuring advertised fixed broadband speeds (up to and over 1 Gbit/s) allows governments to identify key areas that require attention with a view to transforming the digital economy and maintaining progress towards the "Internet of Things" (Chapter 6). With regard to mobile broadband, governments are increasingly aware of the growing demands placed on networks and are conscious of the need to allocate more spectrum resources to mobile communications. Accordingly, policy makers are testing innovative licensing schemes to increase efficiency in the use of spectrum. They also now recognise the role of fixed infrastructures as a critical building block for offloading and backhauling wireless traffic and to enable better use of available spectrum (Chapter 4). The complementarity of fixed and mobile networks is one reason why emerging economies with less developed fixed networks face greater challenges in leveraging the rapid growth of wireless services. In OECD countries, around three quarters of smartphone use occurs on private Wi-Fi access via fixed networks.

Uptake by business, individuals and governments of digital opportunities enabled by broadband is central to achieving economic and social benefits (Chapter 3). Many developing countries are concentrating on the demand side with a particular focus on promoting entrepreneurship and use of ICTs by SMEs. In OECD countries, the opportunities created by the digital economy have begun to transform established industries, including banking, transportation, retail, energy, health, and publishing and media. In the case of the content industry the amount of digital content is growing with considerable room for dematerialisation, especially for books and videos. New business models based on collaborative production methods, such as crowdfunding platforms, now provide entrepreneurs with capital through peer-to-peer (P2P) lending or offer P2P currency exchange models. Similarly, in the sphere of domestic activities, new "sharing economy" platforms allow people to rent, exchange or share their apartment or car. All these initiatives challenge existing regulation of established markets and call for balanced policy responses that enable innovation while protecting the public interest.

The most recent data confirm the huge potential for increased adoption and use of ICTs and the Internet to boost growth through innovation in goods, services and business organisation, across all sectors (Chapter 3). While most firms in OECD countries have a broadband connection – 95% of all enterprises with more than 10 employees in 2014 – few use enterprise resource planning software (31%), cloud computing services (22%) or receive electronic orders (21%). E-commerce sales account on average for just 16% of total turnover, and up to 90% of e-commerce comes from business-to-business transactions (i.e. consumers account for a small portion of e-commerce). Differences among countries and between small and large firms remain considerable.

The scope for further uptake is significant for individuals as well. Despite wide diffusion – in 2014, about 81% of the adult population in the OECD used the Internet of which over 75% used it every day –intensity of Internet usage continues to vary across OECD countries and among social groups. Activities such as sending emails, searching for product information or social networking show little variation across countries, but differences are large for activities associated with a higher level of education such as e-government, e-commerce and online banking. The breadth of Internet activities carried out by users with tertiary education is on average 58% higher than for those with lower secondary education and below. About 70% of OECD students use the Internet at school but

only a few – between 12% and 2% depending on the country – use computers every day for practise and drilling sessions (OECD, 2014a).

Governments increasingly use ICTs to achieve public sector transformation and to shift from a citizen-centred to a citizen-driven approach. This trend is reflected notably by their use of social media to communicate and engage with citizens. At present, 28 out of 34 OECD countries have a Twitter account for the head of government or government as a whole and 21 have a Facebook account (Chapter 3).

Vigilance is essential to ensure competition and trust

To maximise the potential of the digital economy for productivity, innovation, growth and jobs, governments need to do more than encourage broadband expansion and uptake of ICTs and the Internet. They must also engage in further and renewed efforts to protect competition, lower artificial barriers to entry, strengthen regulatory coherence, improve user skills, and build trust in essential infrastructures and applications.

For example, competition in the digital economy is being challenged by several major shifts including: (i) technical convergence towards Internet Protocol (IP) fixed, mobile and broadcasting networks; (ii) increasing integration of business models among telecommunication providers and new Internet players providing over-the-top applications; and (iii) offers of bundled voice, video and data services. These changes necessitate regulatory reform in most countries, in order to apply the same rules to offers of similar services, and to ensure technological neutrality. A good example of this is the provision of privileged (unmetered) access to specific Internet applications in bundled offers ("zero-rating"), which can potentially enhance competition or inclusiveness in some circumstances and damage them in others. Likewise, policy makers and regulators need to remain vigilant to ensure that consolidation of mobile markets does not harm users or reduce the level of innovation resulting from competitive markets. They also need to ensure that mergers between fixed and mobile players, which have the potential to enhance competition, do not instead reduce the capacity of other actors to compete (Chapter 4).

Trust is also critical to economic and social interactions, and especially to virtual relationships conducted in a globally interconnected environment. ICTs and the Internet provide many benefits to users, but existing survey data show that concerns about security and privacy risks still affect user trust in digital products and services (EC, 2015). Businesses are increasingly taking steps to address these risks, with one estimate putting overall expenditure on privacy programmes among Fortune 1000 companies at USD 2.4 billion per year (IAPP, 2014).

Data security breaches continue to be a significant problem, however, leading to increasing interest by policy makers in mandatory breach-reporting obligations. Other indications of elevated attention in security and privacy risk include an uptick in cybersecurity insurance as a means to transfer risk, the continued development of national cybersecurity strategies, improved cross-border co-operation particularly in privacy enforcement, the growing engagement of courts, the emergence of transparency reports by companies as a means to address the "trust gap", and growing opportunities for skilled security and privacy professionals.

Tensions between the need to address security and privacy challenges and the need to avoid a drop in innovation and productivity remain acute. The OECD has called on leaders and decision makers to integrate digital security and privacy risk management in their

broader economic and social risk management frameworks, rather than addressing these issues as separate technical and legal challenges. Nevertheless, additional steps must be taken, in particular to supplement cybersecurity strategies with national privacy strategies, so as to address privacy issues in a co-ordinated, holistic manner (as called for in the OECD Privacy Guidelines) and enable stakeholders to clarify the depth of protection to be afforded to individuals and the limitations society is willing to accept to serve collective public interests (Chapter 5).

Internet governance and policy are high on the political agenda

With the growing pervasiveness of ICTs and the Internet across economies, the importance of Internet policy making and Internet governance has increased among stakeholders of the international community and are high on the agenda of many governments (Section 1.8). [1]

The next two years (2015-16) are set to shape the future Internet governance landscape. In particular, the outcomes of the following distinct but inter-related processes will be critical. The international community is developing a proposal to transition United States Government oversight of the Internet Assigned Numbers Authority (IANA) to the international Internet community. In December 2015, the mandate of the multi-stakeholder-led Internet Governance Forum (IGF) will need to be renewed and the high-level intergovernmental World Summit on the Information Society Conference (WSIS+10) will review the 2005 Tunis Agenda and propose a way forward. In September 2015, the United Nations will launch the post-2015 development agenda, setting sustainable development goals, which are likely to include increased access to ICTs and the Internet to create an inclusive and global digital economy. In this context, fostering innovation on the demand side and the development of content and applications in emerging countries will become a goal in upcoming years.

Underlying these initiatives is the fundamental need to preserve the openness of the Internet. The conception of the Internet as an open platform, where businesses, citizens and governments can serendipitously innovate and develop applications and services, has enabled numerous innovations in the digital economy. In recent years, however, concerns have emerged that the economic and social benefits brought by the open and decentralised architecture of the Internet and by the free flow of trans-border data may be affected, directly or indirectly, by issues such as territorial routing, local content or data storage requirements, network neutrality, the stalled transition to IPv6, universal acceptance of multilingual domain names and the creation of alternative networks.

The benefits of, and risks to, an open Internet will be discussed by ministers and other high-level stakeholders at the forthcoming OECD Ministerial Meeting in 2016, along with other key issues pertaining to global connectivity, the Internet of Things, demand-side initiatives to foster innovation and trust in the digital economy, and ways to foster job creation and develop the skills needed to maximise the benefits of the digital economy.

1.2 National digital strategies and ICT policy priorities

ICTs and the Internet are essential for the economy and for society as a whole. Their impact is so profound that no sector remains unaffected. The implications for policy making are thus far-reaching. While traditional ICT-related policies tended to focus on the ICT sector, recent policies have become more horizontal, covering issues ranging from business creation and productivity growth to public administration, employment and education,

health and aging, environment and development. ICT-related policies focus on enabling the positive economic and social conditions necessary for development and growth.

Most OECD countries and partner economies have established or are close to adopting national strategies addressing policy priorities related to the digital economy. Out of the 34 countries[2] that responded to the *OECD Digital Economy Outlook 2015* questionnaire, 27[3] have an overarching national digital strategy, many of which were established or revised between 2013 and 2014. A few countries do not have an overall strategy, either because it is under development or review (e.g. Austria and Switzerland) or because their digital economy policy comprises several strategies and policies associated with specific issues and/or sectors, which collectively form a national digital economy framework (e.g. the Russian Federation and the United States).

National digital strategies are cross-sectoral by nature and in many instances are designed explicitly to boost countries' competitiveness, economic growth and social well being. Denmark's *ICT Growth Plan*, for example, is designed to support "growth in the ICT sector as well as ICT-based growth in the private sector more generally".[4] Germany's Digital Agenda 2014-2017 highlights "the increased exploitation of the potential of innovation in order to achieve further growth and employment"[5] as its primary objective (in addition to enhancing high speed networks and trust). Italy's Strategy for the Digital Agenda 2014-2020 aims to "ensure economic and social growth, through the development of skills in business and the dissemination of digital culture among citizens".[6] Mexico's National Digital Strategy (2013) aims to make Mexico to "the leading country in digitization in Latin America … with a similar level of digitization to the OECD average by 2018".[7] Specifically, the strategy will focus on fostering innovation and entrepreneurship in the digital economy, improving the quality of education through ICTs, contributing to government transformation, guaranteeing universal access to health services and increasing civil participation. Turkey's Information Society Strategy and Action Plan 2014-2018 aims to promote "growth and employment in accordance with the 10th National Development Plan (2014-2018) and the 2023 Goals of the Turkish government".[8]

Some national strategies, such as that of Australia, plan to make the country "a leading digital economy by 2020".[9] The Plan France Numérique also aims to build a more competitive digital economy in addition to targeting youth and preserving and reinforcing social values. [10] Japan's ambitious Declaration to be the World's Most Advanced IT Nation aims to achieve its goal by 2020, [11] while the Information Economy Strategy of the United Kingdom intends to "help the UK accelerate in the global race, focusing on [its] strengths".[12] The tendency to focus on a country's strength emerges as a characteristic of national digital strategies across some OECD countries.

The various national digital economy strategies of EU member countries reflect the objectives set out in the Digital Agenda for Europe (EC, 2010), the first of seven flagships initiatives established under the "Europe 2020" strategy for smart, sustainable and inclusive growth. The aim of the Digital Agenda is "to maximise the social and economic potential of ICT, most notably the Internet, a vital medium of economic and societal activity". To help EU member states achieve this objective, the Digital Agenda contains 132 "actions",[13] grouped around seven challenging priority areas including: (i) achieving the digital single market; (ii) enhancing interoperability and standards; (iii) strengthening online trust and security; (iv) promoting fast and ultra-fast Internet access for all; (v) investing in research and innovation; (vi) promoting digital literacy, skills and inclusion; and (vii) promoting ICT-enabled benefits for EU society.

Typically, national digital economy strategies build on and sometime integrate pre-existing national strategies related to ICTs, for example, national broadband strategies, e-government strategies and cybersecurity strategies. They often co-exist with other complementary national strategies such as national innovation strategies or development strategies. The forthcoming Digital Agenda for Austria, for example, is building on existing national strategies such as Broadband Austria, e-Health in Austria,[14] eFit 21 – Digital Agenda for Education[15] and e-Accessibility in Austria[16] among others. Sweden's ICT for Everyone – A Digital Agenda for Sweden[17] builds on a number of ICT-specific strategies including the national Broadband Strategy, [18] the E-Government strategy,[19] ICT for a greener administration[20] and the e-Health Strategy.[21] In addition, Sweden's national digital strategy is complemented by the National Strategy for Regional Growth and Attractiveness[22] and the Swedish Innovation Strategy.[23]

Key pillars of national digital economy strategies

The following list reflects the key pillars of many present national digital strategies, with the majority emphasising demand-side objectives (3-8).

1. Further develop telecommunications infrastructure (e.g. access to broadband and telecommunication services) and preserve the open Internet.
2. Promote the ICT sector including its internationalisation.
3. Strengthen e-government services including enhanced access to public sector information (PSI) and data (i.e. open government data).
4. Strengthen trust (digital identities, privacy and security).

Additional demand side objectives, prominent in many national digital strategies include the following:

5. Encourage the adoption of ICTs by businesses and SMEs in particular, with a focus on key sectors such as (i) healthcare, (ii) transportation and (iii) education.
6. Advance e-inclusion with a focus on the aging population and disadvantaged social groups.
7. Promote ICT-related skills and competences including basic ICT skills and ICT specialist skills.
8. Tackle global challenges such as Internet governance, climate change and development co-operation.

Broadband capacity, coverage and resilience

All national digital strategies promote the development of national telecommunication infrastructure and services. Typical objectives include: increase broadband capacity and speed; increase broadband coverage to better connect remote areas; and improve the resilience of existing broadband infrastructure. Many strategies add a further objective: expand mobile broadband and allocate spectrum efficiently.

Digital Canada 150, for example, includes the pillar "Connecting Canadians" which states that "all Canadians, especially those living in rural areas, should have access to high-speed broadband and affordable wireless services so that they can participate and benefit from the digital economy".[24] To achieve this objective, Canada plans to invest CAD 305 million over five years to extend and enhance access to high-speed broadband networks with the aim of reaching a target speed of 5 megabits per second (Mbps) for up to 280 000 additional Canadian households.[25]

The United Kingdom's Information Economy Strategy foresees the provision of high-speed broadband to enterprise zones that are presently not served. To this end, Broadband Delivery UK (BDUK), which forms part of the United Kingdom Department for Culture, Media and Sport, is implementing projects such as the Super Connected Cities Programme (SCCP) to support broadband growth in cities. SCCP will fund cities to provide access to high-speed wireless broadband in publicly owned buildings and remove barriers to rapid private sector deployment.

The overall objective of Sweden's national digital strategy, ICT for Everyone – A Digital Agenda for Sweden, is to achieve world-class broadband by 2020, with access guaranteed for 90% of all households and businesses at a minimum speed of 100 Mbps. To reach this target, the Swedish government plans to establish good market conditions and eliminate obstacles to development. This includes ensuring that relevant regulation is in place.

A primary objective of Digital Czech v 2.0 – The Way to the Digital Economy,[26] is to support the development of high-speed Internet networks at speeds of 30 Mbit/s for all inhabitants of the Czech Republic and 100 Mbit/s for at least half of all households by 2020.

Australia's national digital strategy intends to narrow the gap in online access between capital cities and regional areas in households and businesses by 2020. Portugal's Agenda Portugal Digital (APD),[27] adopted in 2012, aims to promote the development of broadband infrastructure to facilitate access for all citizens to broadband speeds equal or over 30 Mbps by 2020. Accordingly, the Portuguese government launched five public tenders for the deployment of high-speed networks in rural areas, involving 139 municipalities covering more than 1 million people and investments worth EUR 156 million. Luxembourg's Digital Lëtzebuerg[28] envisions an ambitious roll out of countrywide ultra-high broadband connections and plans to offer 100% of the population the possibility to opt for a 1 Gbit/s downstream / 500 Mbit/s upstream or faster domestic connection by 2020.

Likewise, the US national broadband plan, Connecting America: The National Broadband Plan,[29] released by the FCC on March 2010, seeks to ensure that all people living in the United States have access to broadband capability. The plan set an ambitious goal of providing at least 100 million homes with affordable access to actual download speeds of minimum 100 Mbps and actual upload speeds of minimum 50 Mbps by 2020. It also recommended that the FCC make 500 MHz of spectrum newly available for broadband use by 2020 and set forth a number of recommendations aimed at improving the utilisation of existing infrastructure and fostering further infrastructure deployment. The vast majority of recommendations in the plan do not require new government funding; rather, they seek to drive improvements in government efficiency, streamline processes and encourage private activity to promote consumer welfare and national priorities. The principal funding requests relate to: (i) improving public safety networks, (ii) speeding deployment of Internet services to unserved geographical areas, and (iii) increasing broadband adoption efforts. For example, the plan recommends that Congress consider public funding of approximately USD 6 billion for the creation of a federal grant programme to support the establishment of a nationwide, wireless, inter-operable broadband public safety network.

Resilience is a major topic in the national digital strategies of a number of countries. Japan's strategy, for example, aims to secure IT infrastructure environments at the world's highest levels. This not only includes policy measures to secure fair competition among businesses with a view to enabling the use of low-cost, high-speed broadband environments; it also incorporates measures to ensure the use of ICTs during large-scale

natural disasters through higher resilience and redundancy of ICT infrastructures. The measures presented include: (i) redundancy in international IT infrastructure including undersea cables; (ii) regional distribution of data centres (which are currently concentrated in the Tokyo region); and (iii) regional collaboration to encourage distribution of Internet exchanges and backup systems.

Luxembourg's Digital Lëtzebuerg, foresees the roll out of broadband with a particular focus on ultra-high bandwidth in dedicated business areas, which will feature guaranteed redundant fibre access.

The Digital Agenda for Norway, ICT for Growth and Value Creation,[30] aims to increase the security and robustness of telecom networks. The Ministry of Transport and Communications will work with providers and the Norwegian Post and Telecommunications Authority to consider additional measures for increased network security, robustness and preparedness. These measures are directly related to policies on security risk management for the digital economy, discussed further below.

Development of the ICT sector: New technologies, goods and services

The other supply-side objective present in all national digital strategies is increased support for the ICT sector, typically in the following areas: (i) research and development programmes, (ii) promotion of standards, (iii) venture capital investments, (iv) foreign direct investment, and (v) export of ICT goods and services.

Many research and development (R&D) programmes focus on emerging technologies, in particular the Internet of Things, cloud computing and big data analytics. The Plan France Numérique, for example, plans to invest EUR 150 million (USD 162 million) to support R&D through five strategic digital technologies and services: (i) connected objects, (ii) supercomputing, (iii) cloud computing, (iv) big data analytics, and (v) security of information networks. Germany's Digital Agenda 2014-2017 intends to promote investment in: (i) industrial ICT applications, (ii) IT security research, (iii) microelectronics and (iv) digital services. Furthermore, two *Big Data Solution Centres* have been established in Berlin and Dresden to promote innovation related to big data (i.e. data-driven innovation) in industrial applications (Industry 4.0), science (e.g. life sciences) and healthcare.

Japan's national digital strategy aims to support the development of (i) internationally cutting-edge network technologies, in particular ultra-high-speed network transmission technologies; (ii) data processing and analysis technologies, including pattern recognition technologies; (iii) device, sensor and robotics technologies; (iv) software development and non-destructive testing; and (v) highly developed multilingual speech translation systems. Korea's National Informatization Master Plan[31] foresees investments in mobile platform technologies worth KRW 35 billion (USD 32 million). Poland's Strategy for Innovation and Economic Efficiency "Dynamic Poland 2020"[32] anticipates support for the development of the "Internet of Things" with particular emphasis on the energy sector (e.g. smart meters and power control systems). Finally, Digital Canada 150 plans to allocate CAD 1.5 billion to the Canada First Research Excellence Fund to help post-secondary institutions excel globally in research into (ICT) areas that create long-term economic advantages for the country. In addition, CAD 15 million will allocated to support research in quantum technologies and CAD 20 million will be assigned to support innovative R&D, with a view to linking small and medium-sized enterprises (SMEs) with universities, colleges and other research institutions.

The promotion of ICT-related standards is also a prominent feature of many national digital strategies. The second pillar of the Digital Agenda for Europe promotes "Interoperability & Standards" across EU member countries to ensure "that new IT devices, applications, data repositories and services interact seamlessly anywhere".[33] Achievements should be realised through improved standard-setting procedures and the promotion of better use of standards. The UK's Information Economy Strategy also places significant emphasis on interoperability and standards. According to the strategy, the Government has "to bring together a range of stakeholders [including bodies in the standards field] to align programmes, to build on existing knowledge and to put the United Kingdom in the best position to influence future standards at an international level". The strategy envisions a focus on "the use of standards for IPv6 and securing DNS". It also calls for better definitions for concepts such as cloud computing, 5G mobile and the Internet of Things "to enable ideas to be easily incorporated into standards and services". In a number of national digital strategies, promotion of standards is considered in relation to specific sectors. In Germany, for example, the strategy focuses on standards that optimise interoperability between ICT goods and service providers and "traditional" manufacturing, in line with Germany's promotion of "Industrie 4.0".

National digital economy strategies also promote investment in the ICT sector through venture capital. The Business Development Bank of Canada is due to make investments worth CAD 300 million in ICT companies according to Digital Canada 150. The strategy also anticipates funding of CAD 100 million to the Canada Accelerator and Incubator Program to support digital entrepreneurs and CAD 15 million annually to internships in SMEs. Germany also highlighted the importance of VC investments to globalisation of the ICT sector, with a particular focus on support for IT start-ups. Specific measures cited in the Digital Agenda 2014-2017 include: (i) information and advice for founders; (ii) improvements to financing through internationally competitive conditions for VC and crowd investments; (iii) "matching" start-ups to traditional businesses with related economic activities; (iv) targeted support of founders including their links to other German start-ups; and (v) the creation of international start-up "hubs" including incubators.

In France, the Plan France Numérique includes support for start-up incubator programmes. EUR 200 million has been allocated to Halle Freyssinet, an incubator site expected to accommodate more than 1 000 start-ups once operational in 2016. EUR 15 million of this amount has been dedicated to international promotion to attract potential investors and start-ups to the site. Several national digital strategies, including the Plan France Numérique, emphasise the importance of attracting foreign direct investment. Luxembourg's Digital Lëtzebuerg, for example, aims to maintain a positive environment for existing ICT companies while attracting new digital businesses. Egypt's national digital strategy[34] aims to attract investments to expand existing ICT companies and generate job opportunities (Box 1.1).

Some countries also emphasise the need to strengthen the export capacities of the ICT sector. Poland's Strategy for Innovation and Economic Efficiency "Dynamic Poland 2020" aims to promote the international expansion of the ICT sector, with a focus on outsourcing related activities. Hungary's National Infocommunications Strategy[35] also cites investments to promote the digital economy, including through the development of ICT services eligible for export. Mexico's development agenda Prosoft 3.0 seeks to establish the country as the second largest exporter of IT globally and quadruple the value of the sector. Prosoft 3.0 outlined eight strategic areas with key objectives for the next ten years (Figure 1.1).

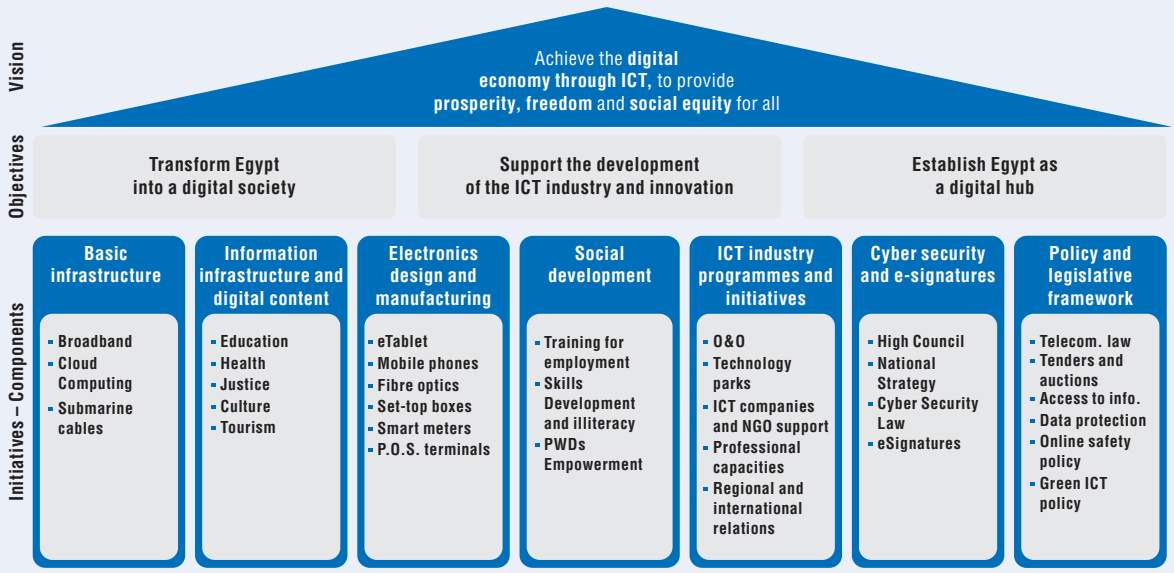
Box 1.1. **The Egyptian national ICT strategy**

The Egyptian ICT strategy has remained steadfast in its underlying objectives: (i) establish a strong ICT infrastructure as the backbone for development of the ICT sector, (ii) create spill-over effects to improve the general quality of life and increase job opportunities, and (iii) contribute to national economic development and GDP, estimated to reach 4% in 2014/15. In the aftermath of the 2011 revolution, the new government has persisted in supporting the ICT sector, which has remained resilient to national and global shocks and maintained the growth levels achieved in previous years.

The ICT strategy of the Ministry of Communications and Information Technology (MCIT) for 2014-2020 is entitled "Achieve the digital economy through ICT, to provide prosperity, freedom and social equity for all". The strategy involved multi-stakeholder input from NGOs, academia and multinational corporations, whose co-operation is central to implementing a series of strategic business plans with a focus on citizen participation and empowerment. The three main strategic objectives are: (i) transformation of Egypt into a Digital Society, (ii) development of the ICT Industry, and (iii) establishment of Egypt as a global digital hub.

The Digital Society is the primary strategic objective of the overall strategy and also the name of an ambitious business plan targeting the integration of government databases and supporting systems, in ways that enable the seamless delivery of services to help grow the economy, raise the standard of living and ensure better governance. The plan involves the utilization and deployment of ICTs to increase the efficiency of the government performance and facilitate services provision for citizens[1]. This will be achieved by building an ICT ecosystem that promotes the efficiency and transparency of internal government operations and the ubiquitous availability of quality e-services to all citizens and businesses. A national digital platform will be developed to ensure the seamless integration of different governmental systems and databases.

MCIT has identified seven pillars to achieving the objectives set out in the strategy: (i) basic infrastructure; (ii) information infrastructure and digital content; (iii) electronics design and manufacturing; (iv) community development; (v) ICT industry programmes and initiatives; (vi) cybersecurity and e-signatures; and (vii) policies and legislative frameworks. The seven pillars have been translated into strategic business plans for implementation.



Box 1.1. **The Egyptian national ICT strategy** *(cont.)*

The origins of the **Basic infrastructure** strategy date back to the "e-Misr" plan launched in 2011, which aimed to diffuse broadband services throughout Egypt, including underserved areas. Broadband supply will be ensured through regulatory interventions, legislative reforms and investment in infrastructure upgrade. The broadband strategy also responds to greater demand for bandwidth, coupled with consumer appetite for video content, news and multimedia services.

Cloud computing is another major component covering private as well as governmental practices, with a view to increasing the efficiency and cost effectiveness of IT systems. The main objectives are: (i) setting up the government cloud, (ii) providing cloud services to SMEs, and (iii) building cloud farms to serve the region and Africa. The model presents an affordable method of accessing needed infrastructure and applications, thus potentially serving the SME community as well as the governmental sector.

The Information infrastructure and digital content strategic business plan aims to support the government in achieving social justice targets, and to extend simple, affordable and ubiquitous access to knowledge and services, including to marginalized and remote segments of society. The plan supports programmes designed to promote and generate the development of digital content and services related to various sectors of the economy, particularly those of highest value to citizens and the overall economy (e.g. education, healthcare and justice, etc.). In addition, it encourages the use of open source material and the development of mobile applications and technologies in view of the available human skills, high mobile penetration (112%) and potential market demand both locally and regionally.

The plan also aims to preserve Egyptian identity through the conservation of natural and cultural heritage, drawing on knowledge generation among users. It fosters and enhances creativity with a view to moving towards sustainable development and a knowledge-based society. The plan rests on four pillars: promoting Arabic culture and Egyptian identity; responding to demands for new skills and qualifications; developing a competitive industry and new investment opportunities; and safeguarding Egypt's cultural heritage and reinforcing its international reputation. A key component of the plan is the use of open government data and user-generated content.

The Electronics design and manufacturing strategic business plan is geared towards maximising the potential of human resources available in the country, with both industries acting as important catalysts for quantum leaps in economic growth and development. The twin objectives of this plan are to increase industry revenues to EGP 70 billion by 2020 and EGP 560 billion by 2030, and to create 30 000 new jobs by 2020 and 300 000 by 2030. Achievement of these objectives relies on a foreign direct investment attraction programme geared towards ODMs/OEMs, and the creation of mega manufacturing sites in Egypt. In addition, the strategy aims to encourage the fabless design sector to develop technology and create innovative companies in Egypt. The plan aims to position Egypt among the top ranks of countries supplying software development skills and services to the rest of the world.

The Community development strategic business plan highlights social responsibility and targets women, inhabitants of remote and underprivileged areas, people with disabilities or reading difficulties, older people, orphans, street children and slum-dwellers, with the aim of using ICTs to improve quality of life. The plan supports and empowers the various segments of Egyptian society, enhances the role and presence of civil society associations, and aims to develop Egypt as a significant regional and global model in the use of ICT for social responsibility.

The ICT industry programmes and initiatives strategy capitalises on Egypt's unique geographical location and massive human talent pool, comprising highly qualified telecommunications engineers and IT professionals, which have enabled the creation of a strong outsourcing and offshoring industry. The strategy builds on these resources with a view to transforming Egypt into a digital hub for the delivery of Internet, telecommunications and digital services to the region and Africa. An important part of the strategy is the development of the new Suez Canal zone, which aims to generate approximately 120 000 job opportunities and USD 860 million over five years[2]. The plan is divided into two streams. The first lays

Box 1.1. **The Egyptian national ICT strategy** *(cont.)*

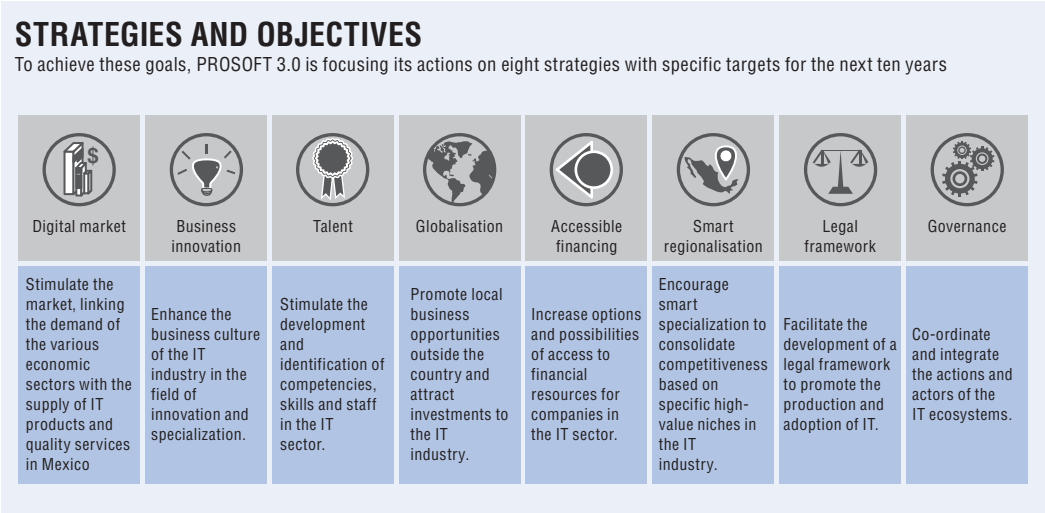
the foundation for the development of export capacity in the ICT sector. The sector's export capacities in the zone will be optimised through the creation of an international centre availing telecom services, and establishing the legal and infrastructural foundations of a technology park to attract local, regional and international companies. Key locations will also be identified to attract international investment for the establishment of a regional centre for electronic industries, especially mobiles and related components. The second stream concerns the enabling role played by the ICT sector in relation to other sectors, both locally and internationally, in particular the development of state of the art navigation, shipping and port logistical services. On the security front, the multi-stakeholder High-Level Cyber Security Council is mandated to protect data privacy and security in the digital society as part of the Cybersecurity and e-signatures strategy.

The policy and legislative framework strategic plan is an overarching tool that aims to ensure the legislative and procedural requirements for all other ICT projects and initiatives, and to create the appropriate environment needed for investment, as well as the protection of citizens' rights. This will be achieved by building a suitable environment for investment, including the development of existing legislation through multi-stakeholder participation, regulation and protection of citizens' rights to govern and regulate the business process. Over the past 15 years, the ICT sector has proven an indispensable engine for growth and development in Egypt, permeating all other sectors in the country. Investment and enhanced security are indispensable prerequisites for its continued work. The overall required investment for the National ICT Sector Strategy 2020 was estimated at nearly EGP 120 billion. Allocation of venture capital, investment banks and public-private partnerships, and local and international investors are forecast to cover around 88% of the total planned required investment.

For more details about Egypt's national digital ICT strategy, please consult *www.mcit.gov.eg*

1. The plan also foresees the development of a national identity smart card for citizens to access such service. In order to exploit potential synergies, MCIT is currently working on making the appropriate ecosystem available. The ecosystem includes as its main corner stone the establishment of a National Council for the Digital Society, which aims to institutionalize and coordinate: (i) strategic investments in, and the deployment of, digital government services across the various government entities and sectors, (ii) the change management and process re-engineering needed, as well as (iii) the regulation and synchronisation of services offered to Egyptian citizens by affiliated entities.
2. The establishment of technology parks represents a major business plan. They are a tool to promote local economic development. Building on the accumulative experiences of the Smart Village and the Technology Park in Maadi, the geographical map of the new technology parks will cover 9 of Egypt's governorates including within the new Suez Canal zone.

Figure 1.1. **Strategic areas of Mexico's Prosoft 3.0**



Source: Secretaría de Economía, Mexico.

Open data and e-government

Some national digital strategies highlight the use of open data citing improved interoperability as a main benefit. The Digital Agenda 2020 for Estonia,[36] for example, aims to open up public sector data for business innovation and promote the joint use of technologies and data (including cloud computing). It also aims to ensure cross-border interoperability of Estonian service infrastructure to facilitate the use and provision of cross-border services for both citizens and enterprises. In Japan, the Declaration to be the World's Most Advanced IT Nation highlights the key role of ICTs in enabling public service delivery at any time, by anyone, anywhere, via a one-stop e-government portal through which public sector data can be accessed. Promotion of open data usage ranks high in Japan's government.

Today's national digital strategies recognise that governments can act as catalyst for the digital economy. This is noticeable in the case of open data initiatives, where the public sector can stimulate data-driven innovation by opening up public sector information, including data. E-government initiatives are also used to stimulate the adoption of a wide range of applications needed for e-health and e-commerce. In this respect, a major trend in the current set of national digital economy strategies is the ongoing effort to promote trust in the digital economy through the establishment of (i) digital identities for all citizens, and (ii) electronic document verification systems (including e-billing systems).

Digital identities and e-authentication

A number of national digital strategies have prioritised the creation of national digital identities for citizens. The Digital Agenda 2020 for Estonia, for example, plans to develop existing national electronic identity cards (including mobile IDs) and promote their use in Estonia and across borders. Italy's Strategy for the Digital Agenda 2014-2020 also highlights the issue of digital identity with government spending of EUR 50 million foreseen to guarantee safe and secure access to digital services provided by the public administration and private entities, for all citizens and businesses, while ensuring a high degree of usability with mobile devices. Japan has also launched a large-scale initiative to establish a national digital identity for all citizens, with significant government investments linked to introduction of the "Number System", which will provide an infrastructure for IT utilization in the future. The individual numbers and corporate numbers are designed to enable accurate and rapid information confirmation and identity verification.

While not all national digital strategies aim to provide government digital identity management services, some support the deployment of secure authentication services. Digital Canada 150, for instance, foresees the creation of "new authentication services for consumers, including the Credential Broker Service and GCKey, to make it easier to manage and secure online usernames, identities and passwords". In the United Kingdom, the Information Economy Strategy anticipates the government "work[ing] closely with industry, privacy advocates and consumer groups to develop an Identity Assurance solution for HMG [Her Majesty's Government] services that leverages existing capabilities and sets informed industry standards". It is expected that "knowledge and skills applied during the development of this IDA [identity assurance] solution will create a centre of excellence within HMG across a range of digital, technology and service sector disciplines (e.g. identity and authentication technology, design, cyber security, research, business transformation, mobile communications, digital service and platform development)." A complementary measure consists of promoting international interoperability by aligning

the United Kingdom's IDA approach with that of other national governments, international standards bodies and major industry associations. Finally, some national digital strategies also promote document verification services, including digital signatures. Australia, for example, plans to expand the use of the Document Verification Service and investigate the use of trusted third-party credentials by the government. In Hungary, the National Infocommunications Strategy plans to boost the electronic commerce market not only by reinforcing electronic payments, but also by promoting electronic invoicing and e-signatures.

Trust: Digital privacy and security

These efforts are consistent with a key objective of many national digital strategies – to increase trust in the digital economy. The protection of privacy is seen as critical for trust, however effective implementation still raises challenges. The "Protecting Canadians" pillar of the *Digital Canada 150* strategy details existing forms of protection "in place for families and businesses through some of the most modern and effective privacy and anti-spam laws in the world". In the Czech Republic, the national digital strategy calls for the Office for Personal Data Protection to monitor the development and application of new forms of technology, and propose solutions in the event that self-regulatory mechanisms fail. The strategy also calls for the modification of existing legislation if necessary. Mexico's National Development Plan calls for measures to ensure personal data protection, while also encouraging accountability in the use of these data. Finally, the United Kingdom's Information Economy Strategy calls for the government to continue efforts "to drive and influence EU and international discussions in key areas such as privacy and data protection and the digital single market to ensure that growth opportunities are not inhibited by new or existing levels of regulation, while providing a proper balance of protection and security for citizens".

Although protection of privacy features prominently in many national digital strategies, this is not reflected in budget allocations – no country has yet allotted funding for privacy-related measures. This may be linked to the persistent perception that privacy is a legal matter under the purview of specialised enforcement authorities rather than a strategic horizontal objective. In some cases, however (e.g. Luxembourg's Digital Lëtzebuerg), dedicated R&D funding for ICT security and cryptology may provide spillover benefits for privacy-enhancing technologies.

Measures linked to cybersecurity appear frequently in national digital economy strategies, including references to R&D support measures and national cybersecurity strategies (e.g. Digital Canada 150 refers to Canada's Cyber Security Strategy). Cybersecurity measures may include public information on cyber risk and measures to combat cybercrime. Australia's national digital strategy, for instance, describes a number of actions to address digital security concerns including the development of a "National Plan to Combat Cybercrime" and the release of "Digital Citizenship Best Practice Principles" to address security risks. In Hungary, the National Infocommunications Strategy has allocated EUR 17 million to IT security with the aim of maximising protection of networks, IT infrastructure and public administration e-services, as well as disseminating information on digital risk management. Korea and Japan have also highlighted cyber security in their respective strategies, with the former earmarking government funds worth KRW 246 billion.

Some national digital strategies also aim to strengthen the national cybersecurity industry. The United Kingdom's Information Economy Strategy reiterates commitments made in the National Cyber Security Strategy to award 11 leading universities the status of Academic Centre of Excellence for Cyber Security Research, sponsor 78 PhDs and fund two Research Institutes. In addition, the strategy calls for the development of new routes to transfer cyber expertise between research institutions, industry and Government Communications Headquarters (GCHQ), otherwise known as the Cyber Growth Partnership. It also calls for collaboration with the Information Economy Council on areas of mutual interest, including R&D and skills, and for renewed commitment to develop and exploit innovations in cyber security. In Germany, the Digital Agenda 2014-2017 anticipates efforts to strengthen the security of online services via secured ICT infrastructures and to reinforce the IT security industry.

ICT adoption in education, healthcare and transport

Many national digital strategies aim to promote adoption of ICTs and the Internet in key areas such as education, healthcare and transport.

Promoting ICT adoption in education ranks high among national digital strategies with one frequently stated aim being to capitalise on the digital revolution to improve the effectiveness of the education system and ensure the development of basic and advanced ICT skills. Measures range from a focus on infrastructure (e.g. better connecting education institutions) to promotion of ICT-related curricula, teacher training and promotion of online learning environments (e.g. massive open online courses). In the United States, the Schools and Libraries Program is allocated USD 3.9 billion per year to provide schools and libraries with access to robust high-speed broadband connections. In 2014, the FCC freed up programme funds to address the broadband connectivity gap facing many schools and libraries capable of supporting individualised learning, especially in rural areas, and maximised the available options for purchasing affordable high-speed connectivity.

National digital strategies typically include a series of complementary measures. Australia's National Digital Economy Strategy aims to provide schools, registered training organisations (RTOs), universities and higher education institutions with the connectivity to develop and collaborate on innovative and flexible educational services, the resources to extend online learning resources to the home and workplace, and the facilities to offer students and learners the opportunity for online virtual learning. Its first action in this regard will be to complete the development of a new curriculum encompassing digital learning. Complementary efforts include partnering with industry to promote digital careers and encouraging access to virtual classes for vocational education and training (VET) students.

In the case of Canada, spending worth CAD 36 million over four years is foreseen to support the Computers for Schools Program, which provides students and interns with access to digital equipment and skills training. The United Kingdom's Information Economy Strategy describes a series of measures to promote ICTs in education with a view to ensuring a sufficient level of ICT skills in the economy. It further calls for a group combining the supply and demand sides of skills provision to develop a digital skills strategy. Specific actions for consideration include promoting the benefits offered by massive open online courses (MOOCs) to support ICT learning, workforce re-skilling and increased digital literacy. Other complementary measures include encouraging stakeholders from the private sector and

education institutions to agree on actions to improve employment outcomes for computer science courses, and to accelerate the uptake of e-skills apprenticeships.

E-Health care is another prominent area targeted by many national digital strategies. As with education, some measures focus on ensuring high-quality broadband connectivity across the healthcare system. But in most cases, measures aim to further the development of tele-medicine or the deployment and better use of electronic medical healthcare records. Italy's Strategy for the digital Agenda 2014–2020, for example, has allotted investments worth EUR 750 million to improve the cost-quality ratio of health-related services by reducing waste and inefficiency. Measures include electronic health records for all citizens, electronic pharmaceutical prescriptions, and online booking with a view to optimising health-related resources and reducing waiting times.

Some measures also target specific social groups, especially the elderly population. Australia's National Digital Economy Strategy, for example, aims to increase the share of high-priority consumers able to access individual electronic health records to 90% by 2020. These include older people, mothers and babies, and those with a chronic disease as well as their caretakers. The main steps include: (i) expanding the Medicare Benefits Schedule (MBS) for tele-health items; (ii) implementing video consultations for the after hours GP Helpline and Pregnancy, Birth and Baby Helpline; and (iii) evaluating outcomes from tele-health trials and developing action plans to address challenges.

In Austria, the initiative e-Health in Austria aims to address key challenges related to e-health financing, interoperability, and co-ordination among health institutions and stakeholders. Similarly, Germany's Digital Agenda 2014-2017 aims to improve co-ordination and interoperability between key stakeholders and their IT systems, and to address emerging IT security risks related to increasing digitisation of the healthcare system.

Lastly, some national digital strategies target transportation and logistics. Japan's national digital economy strategy plans to use ICTs to create a safe, economic and environmentally friendly road traffic system. It also aims to further internationalise and expand Japan's agriculture-related IT industry. Other national digital strategies emphasise the use of R&D or other policy measures to target sectors of strategic economic importance. Germany's Digital Agenda 2014-2017, for example, includes initiatives to increase digitisation and automation in manufacturing, and measures to promote information on best practices for industry and smart service applications.

E-inclusion: ICT adoption by households

The promotion of ICT adoption by households and individuals aims to advance social policy objectives such as e-inclusion. This objective still requires ICT supply-side policies, such as expanding broadband access to underserved areas, especially those home to disadvantaged social groups. However, supply-side measures are often supplemented by initiatives to increase the level of digital literacy and raise awareness about risks and opportunities online. One example of an initiative to further e-inclusion at multiple levels is the Low Income/Lifeline Program in the United States, which was approved for a comprehensive overhaul in 2012. A key objective in the modernisation process will be to ensure broadband availability for all low-income Americans. Lifeline builds on efforts by the FCC to close the broadband adoption gap and address digital literacy. The Commission aims to establish a Broadband Adoption Pilot Program using USD 13.8 million in savings from other reforms to test and determine how Lifeline can be used to increase broadband adoption among Lifeline-eligible consumers.

The Digital Agenda for Europe anticipates a multifaceted approach to e-inclusion. Under its activity "inclusive digital services", the Agenda calls for the European Commission to examine "how best to meet demand for basic telecom services in today's competitive markets, what role universal service could play in achieving the objective of broadband for all, and how universal service should be financed" (EC, 2010). It also calls for "concerted actions to make sure that new electronic content is also fully available to persons with disabilities". To promote accessibility, the Agenda calls, for instance, for the systematic evaluation of "accessibility in revisions of legislation undertaken under the Digital Agenda … following the UN Convention on the Rights of Persons with Disabilities".

Australia's National Digital Economy Strategy also includes supply and demand-side considerations, for example, under Action 24, to provide "free Wi-Fi access to remote Indigenous communities". At the same time, the strategy targets the aging population with measures to boost the Keeping Seniors Connected programme. Similar measures are found in a significant number of national digital strategies. For example, Germany's Digital Agenda 2014-2017 recognises the lack of confidence exhibited among elderly people in ICTs and has called for an examination into ways to increase their skills and trust.

Digital skills and jobs

All national digital strategies recognise improvement of skills and competences as a means to further e-inclusion. Key actions identified by the Digital Agenda for Europe to further e-inclusion relate to the development of skills and competences essential for the digital economy. Action 10 proposes "digital literacy and competences as a priority for the European Social Fund regulation (2014-2020)". Other measures include "promot[ing] a higher participation of young women and women returners in the ICT workforce through support for web-based training resources, game based eLearning and social networking". Digital Slovenia 2020[37] aims to ensure inclusiveness by raising awareness of the importance of ICT for the development of all segments of society. Ireland's National Digital Strategy[38] aims to reduce by half the number of "non-liners" (people who have not yet engaged with the Internet) by 2016. One measure envisioned in the Strategy is "awareness raising campaigns with industry stakeholders to convey to 'non-liners' what they could do online, and to highlight to existing users other ways they could use and benefit from further digital engagement". Ireland's strategy also foresees the introduction of a new training grants scheme (BenefIT) to fund digital skills training for citizens, and the development of an online mapping resource to identify digital skills learning opportunities.

A number of countries have identified ICT-related skills as the key to increasing job creation opportunities. The Czech Republic describes a number of measures in Digital Czech v 2.0 to increase ICT-related skills levels. These include collaboration between the Ministry of Labour and Social Affairs and the Ministry of Education, Youth and Sports on a strategy to increase digital literacy and develop e-skills among citizens. The goal is to ensure that new employees have adequate ICT skills and to support current employees during periods of transition due to ICT-related activities or the effects of globalisation. In Spain, the Digital Agenda[39] aims to promote digital inclusion and literacy, and to ensure the training of new ICT professionals. In Italy, the Strategy for the Digital Agenda 2014–2020 plans to invest EUR 12 million to promote digital skills and increase digital literacy levels, widen the curricula of topics related to digital skills, increase the number of ICT skills training courses, boost the number of graduates in fields related to ICT and raise the level of digital skills among civil servants. In Australia, e-inclusion is supported via measures

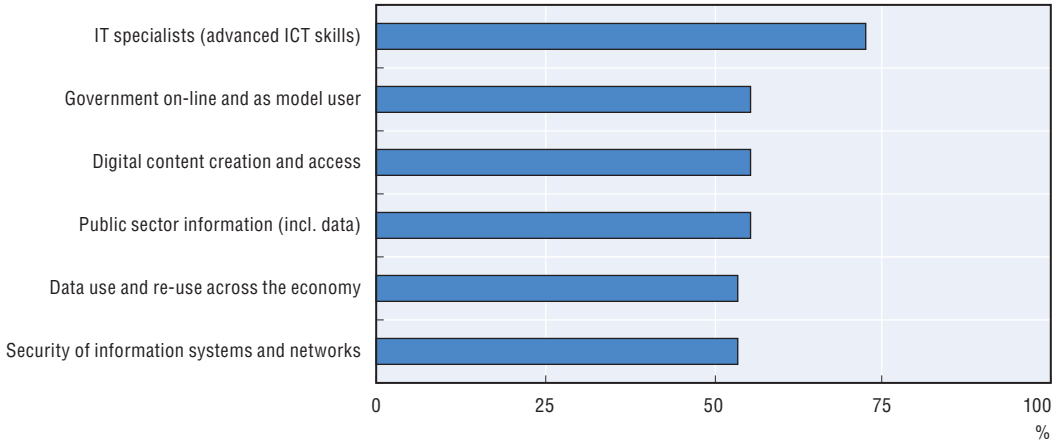
that directly target the labour market. The National Digital Economy Strategy aims to double the level of telework[40] to 12% of Australian employees and implement measures to raise awareness of telework in the labour market, such as organising an annual National Telework Week.

ICTs and global challenges

Very few national digital strategies have an international dimension. Among those that do, key issues are Internet governance, climate change and development co-operation. Germany has called for multi-stakeholder engagement around issues addressed in the Digital Agenda 2014-2017 and active involvement in international policy debates held at the International Telecommunication Union (ITU), the Internet Governance Forum (IGF) and the OECD. Germany's Agenda also addresses development co-operation issues such as the need for "cyber capacity building" and "cyber security capacity building" in developing countries. It also calls for the government to examine and consider the potential of digital technologies in Germany's Africa Strategy. Sweden also highlights international development co-operation in its strategy, ICT for Everyone – A Digital Agenda for Sweden. Strategic areas include the role of ICT in societal development with a focus on ICT for global development, and related issues such as research and innovation, ICT for the environment, gender equality, freedom on the net and copyright.

Overall, the analysis of national digital economy strategies show that ICT policies have changed considerably over the past decade and have been embraced by mainstream economic and social policy priorities looking to create positive framework conditions for growth and development. The above analysis is consistent with the results of the OECD Digital Economy Policy Questionnaire on countries' ICT policy priorities. In 2014, 26 out of 29 countries considered rolling out broadband Internet infrastructure to be their current top priority. For 19 out of 28 countries, digital privacy and security ranked second and third. But when asked to rate the likely evolution of their priorities in the near future, countries placed skills development as the top objective, followed by public service improvements and digital content creation (Figure 1.2).

Figure 1.2. **Top increasing ICT policy areas**



Note: ICT policy areas have been selected and ranked based on the majority rule for a particular prioritisation.

Source: Based on 31 detailed responses (including 25 OECD countries) to the OECD DEO Policy Questionnaire 2014 on current and future policy priorities, sent on June 2014.

StatLink http://dx.doi.org/10.1787/888933224095

The role of governments as active contributors in digital economy developments cannot be underestimated. Over one third of countries responding to the questionnaire placed government use of digital technologies and public sector information high on their future digital agenda. The need for governments to take an active role in the digital economy is reflected both in the OECD Recommendation of the Council on Public Sector Information, which was adopted in 2008 and reviewed in 2014, and the OECD Council Recommendation on Digital Government Strategies, adopted in 2014 (OECD, 2008, 2014f).

Box 1.2. **Brazil's national digital economy strategy**

In the past decade, the digital economy has grown exponentially in size and importance in Brazil, as can be attested by the ascending curves in subscriptions, value added, output and employment. Parallel to the growth in both salaries and demand of ICT goods and services, the Brazilian government has prioritised a sectoral approach of enhancing infrastructure, fostering the ICT industry, ensuring availability and affordability for underserved populations and connecting public institutions. A few recent and central national policies have been selected and are presented below.

Enhancing infrastructure

Having identified the need for greater investment in infrastructure, the Brazilian government established the National Broadband Plan (PNBL) by presidential decree (no. 7175/2010) in 2010. The PNBL consisted of expanding the fibre network to the interior regions of the country, installing submarine cables and a South American optical ring, and reducing tariffs on networks and access terminals. The PNBL was structured around six pillars of action with the central goal of achieving broadband coverage of 40 million households:

- *Price of telecommunication services*: offer fixed broadband (1 Mbps) to the value of USD 14.35 per month in all municipalities by the end of 2014, with tax cuts for broadband in rural areas (700 MHz and satellite ground small stations).
- *Transparency and competition*: implement a new regulatory framework for trade in wholesale broadband (30% reduction), auction orbital positions for satellites, and reduce barriers to entry for new retailers in copper and coaxial cable networks.
- *Speed and quality*: auction 2.5 GHz frequency bands; roll out 4G mobile service to all World Cup capitals; and set regulations for quality management applied to fixed and mobile broadband, and bidding terms for the frequency range of 700 MHz.
- *Price of access terminals*: remove taxes on personal computers, modems, tablets, smartphones and routers subjected to national production; exempt terminals aimed at rural service from all federal taxes and reduce taxes on M2M modules.
- *Expansion of terrestrial networks*: build new international traffic routes (submarine cables and South American optical ring); set new financing mechanisms for producers of optical fibre; develop a special taxation regime for machinery, instruments, equipment and building materials; and roll out telecom network infrastructure.
- *Telecommunications service coverage*: subsidise broadband connection to all urban public schools, issue bidding of 2.5 GHz frequency bands, accelerate the diffusion of 3G, and develop geostationary satellite for defence and strategic communications.

Four years after implementation of the PNBL, Brazil has experienced a substantial increase in fixed and mobile broadband subscriptions. However, fixed broadband infrastructure and full mobile broadband coverage, speed and quality continue to be a challenge. While 3G coverage reached 3 827 out of 5 570 municipalities in 2014, 4G connections served only 118 cities, yielding a total of 2.83 million subscriptions.

Box 1.2. **Brazil's national digital economy strategy** *(cont.)*

Fostering ICT and innovation

In 2012, the Ministry of Science, Technology and Innovation (MCTI) launched the Strategic Programme for Software and Information Technology Services (TI Maior), a broad programme designed to enhance Brazil's performance in the ICT sector. The programme focused on economic and social development through ICTs, innovation, entrepreneurship, scientific and technologic production, innovation and competitiveness.

As part of the TI Maior programme, Brazil integrated initiatives to promote start-ups, develop ICT skills, attract R&D centres, and enhance the creation of software and technology ecosystems around key areas.

- *Global R&D centres initiative*: a set of incentives was designed to attract R&D centres to Brazil. They included the provision of institutional advisory, tax reduction and research grants. This resulted in the announcement of several centres (Microsoft, EMC, Intel, SAP, Huawei and Baidu), yielding a total investment of USD 400 million and the creation of more then 300 highly skilled jobs over the next three years.
- *Digital Ecosystems initiative*: in order to foster technology ecosystems around key areas such as health, education, agriculture, sports, aerospace, telecommunications, finance, energy petroleum, mining and defence, this initiative disbursed more than USD 80 million in incentives for software creation.
- *Start-Up Brazil*: designed to accelerate the development of technology-based start-ups, this initiative has selected and funded 100 start-ups per year since 2013. Each start-up was supported with mentoring and received a grant of around USD 90 000.
- *Brasil Mais TI*: conceived to develop ICT skills, this initiative offers a comprehensive programme of online courses coupled with intermediation of job postings. Over three years it has trained 208 000 young people through courses of 16 to 380 hours.

Building a strategy for the future

Despite advances, many improvements are yet to be made regarding the deployment of infrastructure to connect households and businesses, and the adjustment of regulatory and institutional frameworks for the future digital economy. Brazil's ICT sector remains comparably small and dedicated largely to the domestic market, and increased levels of investment in R&D are needed to boost innovation and productivity. Competition can be strengthened to ensure "bottom up" innovation and may also play an important role in promoting greater equity.

In many OECD countries, the economic crisis has led politicians to refocus resources towards using the digital economy as a platform for promoting growth and productivity. Key challenges for the future include improving ICT adoption among businesses, increasing R&D investments, reviewing the General Telecommunication Law of 1996, ensuring competition in the face of market consolidation and adopting a strategic vision for sustainable growth.

1.3 Main trends in the ICT sector

The core of the digital economy is the ICT sector. After a couple of challenging years during the global financial crisis, the overall outlook for the ICT sector is positive and a number of indicators, especially those directed at the future development of the sector, indicate that the sector is getting back on its feet. This section provides an overview of the main developments and trends in the ICT sector in general, and then takes a closer look at communication markets and the Internet.

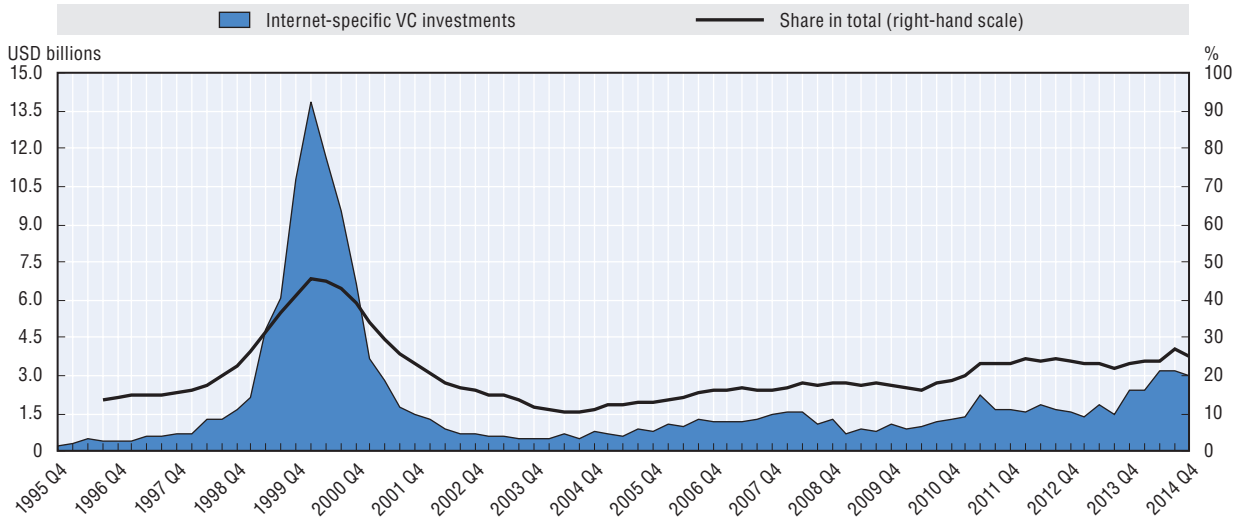
US venture capital investments are at their highest level and the semiconductor market is growing

Venture capital investments in ICTs and the development of the semiconductor market are two leading indicators for the future development of the ICT sector. The

increasing share of venture capital (VC) investments in ICTs reflects upcoming business opportunities in the sector. Venture capital investments in the United States reached almost USD 15 billion, their highest level since the dot-com bubble, and the share devoted to investments in the ICT industries reached 67% in the last quarter of 2014 (see Chapter 2, Figure 2.3). It is also worth noting that one quarter of all US venture capital investments are dedicated to companies whose business models are fundamentally dependent on the Internet (Figure 1.3).

Figure 1.3. **Amount of venture capital invested in Internet-specific companies in the United States**

USD billions and year-on-year growth, 4Q moving average



Source: Based on PricewaterhouseCoopers/National Venture Capital Association MoneyTree™ Report based on Thomson Reuters data, February 2015.

StatLink http://dx.doi.org/10.1787/888933224107

The second indicator for future development of the sector is the growth rate of the semiconductor industry, where cyclical fluctuations appear ahead of other ICT industries. Since mid-2013, growth rates have increased steadily (Figure 1.4). According to the World Semiconductor Association, this trend is expected to continue over the next two years (see Chapter 2, Figure 2.2).

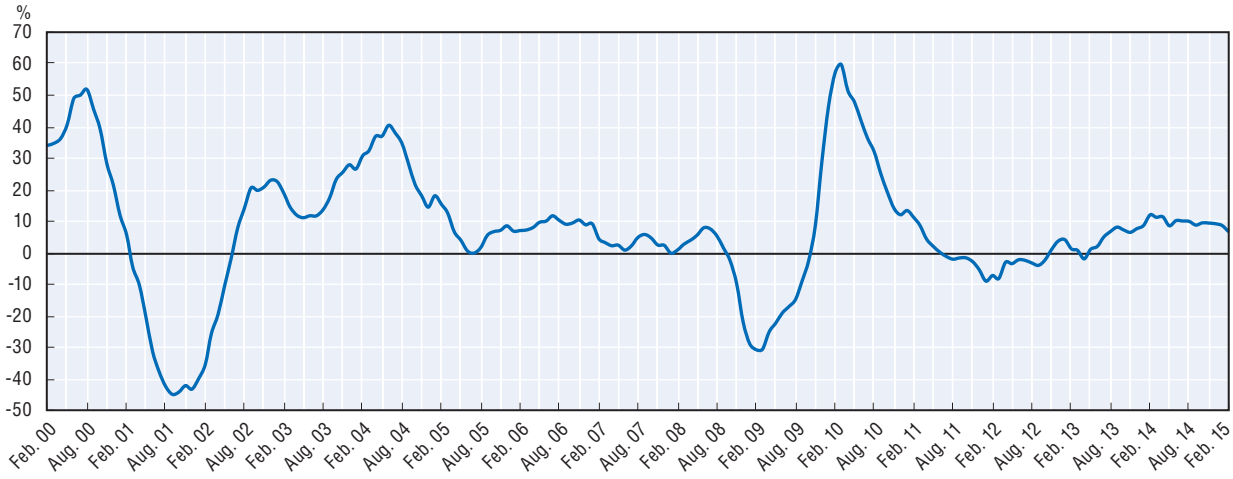
Trade in ICT services is growing faster than trade in ICT goods

International trade in ICT goods and services underscores the positive developments mentioned above. Trade data from 2001 to 2013 show continued growth in ICT trade with exports in ICT services growing faster than exports in ICT goods.

Between 2001 and 2013, world exports of manufactured ICT goods grew by 6% per year, reaching USD 1.6 trillion (see Chapter 2, Figures 2.10a and 2.10b). Production and exports of ICT goods are increasingly concentrated in a few economies (Figure 1.5). The shares of Japan and the United States in world exports of ICT goods halved from 2001 to 2013, due in part to offshoring of production. Korea is the only OECD country to increase its share of the world market for ICT goods over the same period.

Figure 1.4. **Growth in monthly semiconductors worldwide market billings**

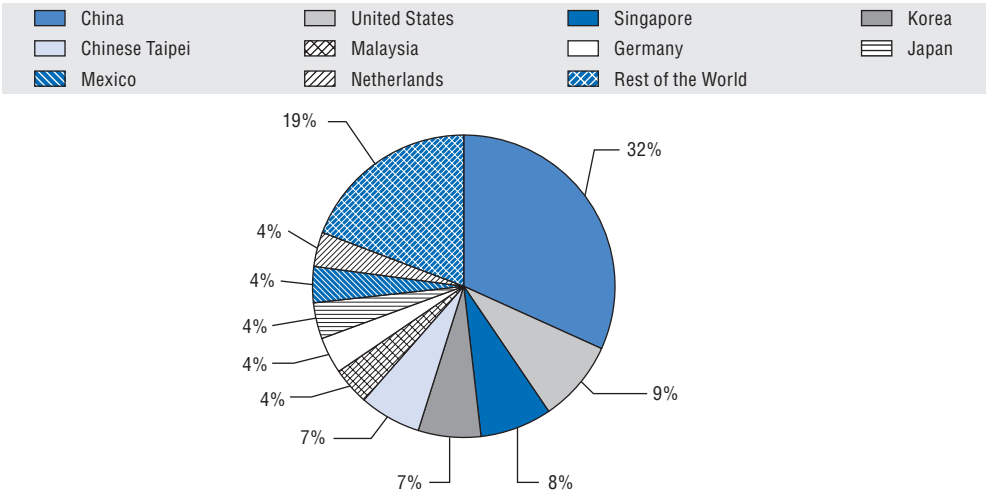
Year on year growth, three-month moving average



Source: Based on World Semiconductor Trade Statistics (WSTS), April 2015.

StatLink http://dx.doi.org/10.1787/888933224117

Figure 1.5. **Top ten exporters of ICT goods, 2013**



Notes: World is estimated based on the 103 BTDIxE declaring countries that reported ICT exports in all three years. World excludes re-imports for China and re-exports for Hong Kong China. China's ICT exports are adjusted for re-imports.

Source: OECD, Bilateral Trade Database by Industry and End-use category (BTDIxE), February 2015.

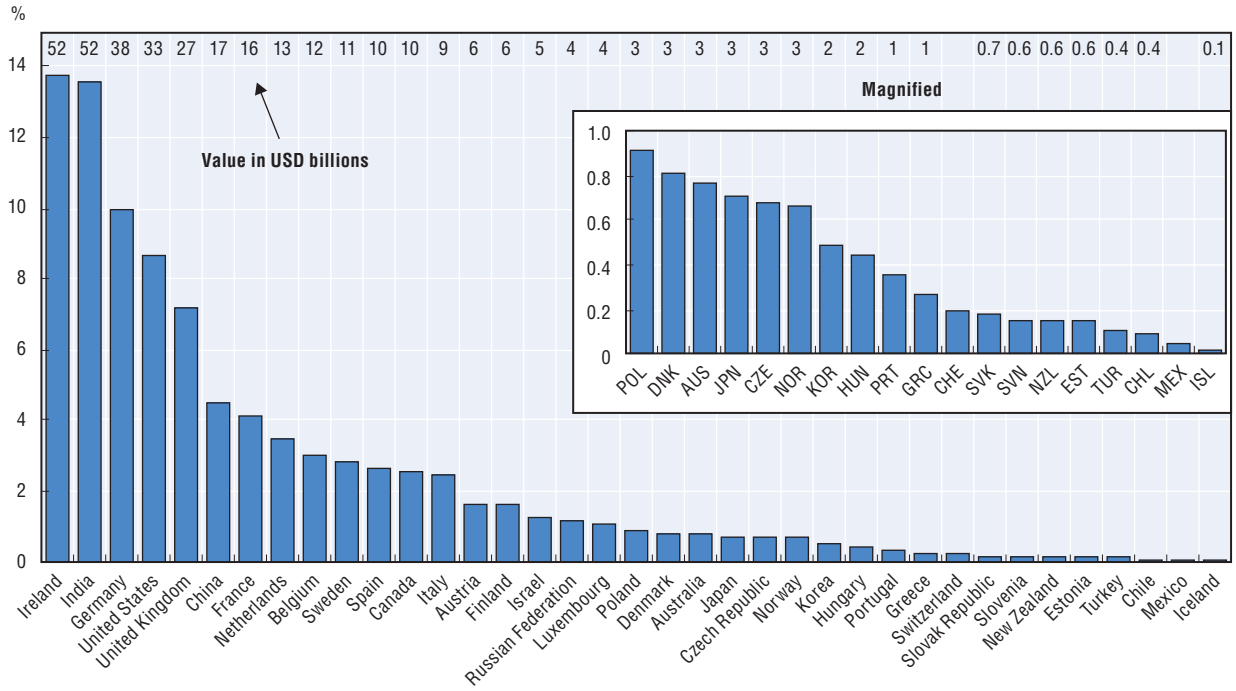
StatLink http://dx.doi.org/10.1787/888933224128

International trade in ICT services grew much faster than in ICT goods (30% per year). Between 2001 and 2013, it increased fourfold in current price dollar terms to almost USD 400 billion. In particular, the share of computer and information services almost doubled from 3.4% to 5.8% of world exports of services, while that of telecommunication services increased marginally. For the OECD area, the combined share of computer and information and communication services rose from 5.8% to 8.3% of total service exports (2001-13).

As with trade in ICT goods, a few economies account for a significant share in global exports of ICT services (Figure 1.6), with some major shifts in recent years. Ireland, which benefits from the presence of transnational companies, is the leading exporter of computer and information services, followed by India, which started from a very modest level. China is also becoming a major exporter of ICT services along with Germany, the United Kingdom and the United States. Together, these countries account for almost 60% of total exports of ICT services. The top exporters of telecommunications services include the United States, the largest European economies and the Netherlands.

Figure 1.6. **Exporters of ICT services, 2013**

Percentage shares of total world services exports and in USD billions



Notes: For Chile, Iceland and Israel, data refer to 2012. For Mexico and Switzerland, ICT services only include communications services.

Source: Based on UNCTAD, UNCTADstat, February 2015. http://unctadstat.unctad.org.

StatLink http://dx.doi.org/10.1787/888933224139

To a large extent, these trends are due to trade in intermediate inputs (i.e. goods and services used in production). The dramatic increase in ICT exports from China, for example, has been matched by a proportional increase in imports of ICT intermediate inputs – notably in its processing zones. Consequently, China's share of ICT goods and services valued added embodied in foreign final demand is significantly lower than its share of gross world exports. In 2011, US exports of ICT goods and services were higher than those of China in value added terms – driven partly by the high presence of US ICT services embodied in final demand products. Embodied ICT services also contributed to higher shares for India and the United Kingdom in value added terms (see Chapter 2, Figure 2.12).

Continued high R&D expenditures and a large number of ICT-related patents reflect the key role of the ICT sector in current innovation activities

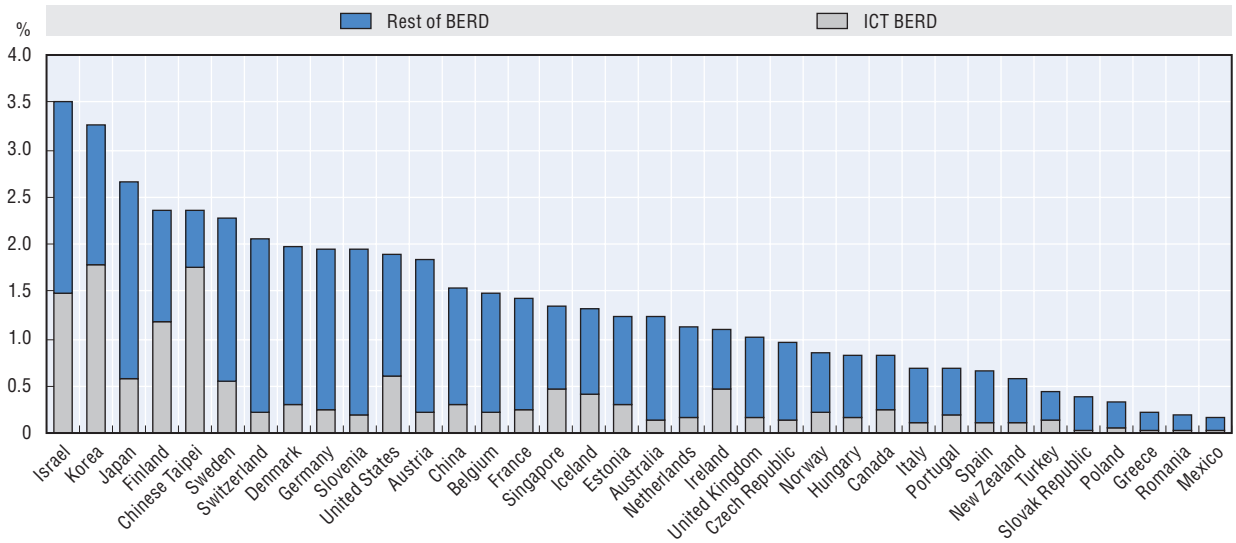
Another way to look at the future growth of the digital economy is to examine the role ICTs play in innovation activities. Two central indicators for measuring innovation are patents and research and development (R&D) expenditures.

Figure 1.7 provides an overview of ICT and total business enterprise expenditure on R&D (BERD). In 2013, total business enterprise expenditure amounted to 1.6 % of OECD GDP (OECD, 2015). Out of total BERD, business R&D performed by the ICT sector accounted for almost 33% or 0.5% of GDP. Large differences exist in R&D expenditures in the ICT sector across different countries. In Finland, Israel and Korea, ICT BERD accounts for over 40% of the total and represents between 1.2% and 1.8% of GDP.

ICT R&D expenditures in the OECD area tend to be more concentrated in ICT manufacturing (60% of ICT BERD) than in ICT services (see Chapter 2, Figure 2.13). In 2013, Chinese Taipei and Korea devoted over 70% and 50% of their total BERD to ICT manufacturing. Despite the drop in Nokia's activities, Finland continues to spend over 40% of its total BERD on ICT manufacturing, followed by Singapore, Japan, the United States and Sweden, all of which spent above 20% of total BERD.

Figure 1.7. **Business expenditure in R&D, 2013**

As a percentage of GDP



Notes: For the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Italy, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain Switzerland and the United Kingdom, data refer to 2012. For Australia, Austria, Belgium, Greece, Iceland, Ireland, Mexico, New Zealand, Singapore and the United States, data refer to 2011. The ICT sector is defined according to the OECD ICT sector definition based on ISIC Rev.4

Source: OECD ANBERD and RDS Databases, February 2015.

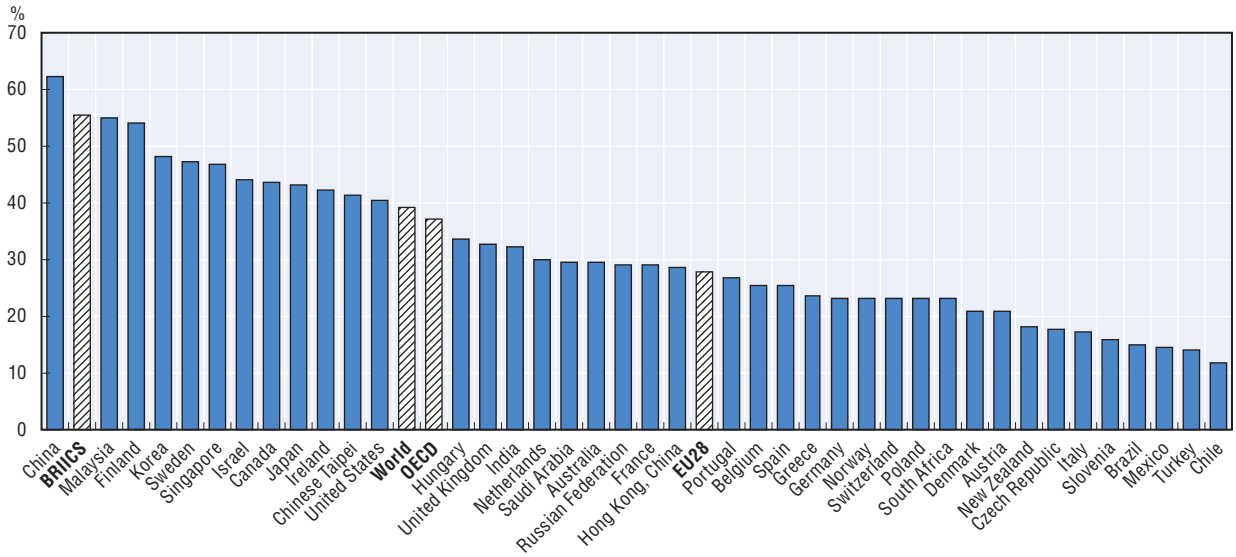
StatLink http://dx.doi.org/10.1787/888933224145

While R&D provides a measure of innovation input, patents, registered designs and trademarks capture innovation output. In 2010-12, more than half a million patent applications were filed worldwide under the Patent Cooperation Treaty (PCT). Patent applications in ICT technologies accounted for almost 40% of total applications (Figure 1.8), representing a return to almost the 2000-02 level. However, a closer look at OECD and non-

OECD economies shows that ICT-related patent applications dropped by 2.8% compared to 2000-02 in the OECD area, while applications by Brazil, Russia, India, Indonesia, China and South Africa (BRIICS) more than doubled, reaching 55%, largely as a result of increased patenting by China (see Chapter 2, Figure 2.15).

Figure 1.8. **ICT-related patents, 2010-12**

As percentage of total PCT patent applications



Notes: Data relate to patent applications filed under the Patent Co-operation Treaty (PCT). Patent counts are based on the priority date, the inventor's residence and fractional counts. ICT-related patents are defined using a selection of International Patent Classification (IPC) classes. Only economies that applied for more than 250 patents in 2010-12 are included. BRIICS refers to Brazil, the Russian Federation, India, Indonesia, China and South Africa.

Source: OECD, Patent Database, *www.oecd.org/sti/ipr-statistics*, January 2015.

StatLink *http://dx.doi.org/10.1787/888933224151*

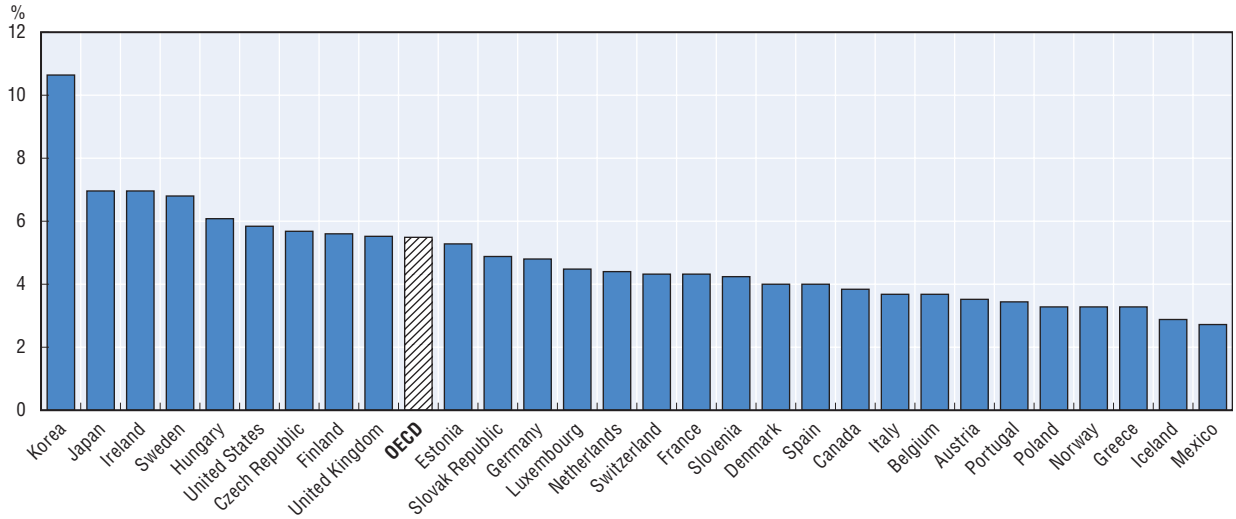
Although signs point to increased growth of the sector, the current share of ICTs in value added remains stable

While the above-mentioned developments suggest a positive future development for the ICT sector, the share of ICTs in OECD total value added has remained stable. In 2013, the ICT sector in the OECD area accounted for 5.5% of total value added (i.e. about USD 2.4 trillion). This share shows large variations across countries (Figure 1.9), ranging from 10.7% of value added in Korea to less than 3% in Iceland and Mexico (Figure 1.9). Ireland and Japan have the second largest share (7%), followed by Sweden and Hungary (over 6%).

Over two thirds of the ICT sector in the OECD is accounted for by IT and other information services (2% of total value added) and telecommunications (1.7%) (see Chapter 2, Figure 2.5). Computer, electronic and optical products and software publishing account for, respectively, 1.4% and 0.3% of total value added. The degree of specialisation, however, varies significantly among countries. Korea shows the strongest specialisation in computer, electronic and optical products (over 7% of total value added), Luxembourg in telecommunications (3%) and Ireland, Sweden and the United Kingdom specialise in IT and other information services (3%).

Figure 1.9. **Share of ICT sector in total value added, 2013**

As a percentage of total value added at current prices



Notes: The ICT sector is defined here as the sum of industries ISIC rev.4 26, 582, 61 and 62-63. For Germany, Iceland, Ireland, Japan, Mexico, Poland, Spain, Sweden, Switzerland and the United Kingdom, data refer to 2012. For Canada and Portugal, data refer to 2011. For Ireland and the United Kingdom, data refer to SNA 93 and were extracted in October 2014. For the rest of countries, data refer to SNA 2008. For Canada, Iceland, Ireland, Japan and Mexico, data for Software publishing are not available, and are therefore not included in the definition. The figure for Switzerland shows the ICT sector share as defined by the OECD (2011a). In this particular case, the share is not totally comparable with the rest of the countries.

Source: Based on OECD, National Accounts Database, ISIC Rev.4; Eurostat, National Accounts Statistics and national sources, April 2015.

StatLink http://dx.doi.org/10.1787/888933224163

While employment in the ICT sector has remained stable in the OECD area, demand for ICT specialists across all sectors has risen steadily

Employment in the ICT sector accounted for more than 14 million people, almost 3% of total employment in the OECD (see Chapter 2, Figure 2.6). This share remained relatively stable throughout the financial crisis. Shares in ICT employment range between over 4% in Ireland and Korea to less than 2% in Greece, Portugal and Mexico. IT and other information services together with telecommunications industry account for 80% of ICT employment in the OECD area.

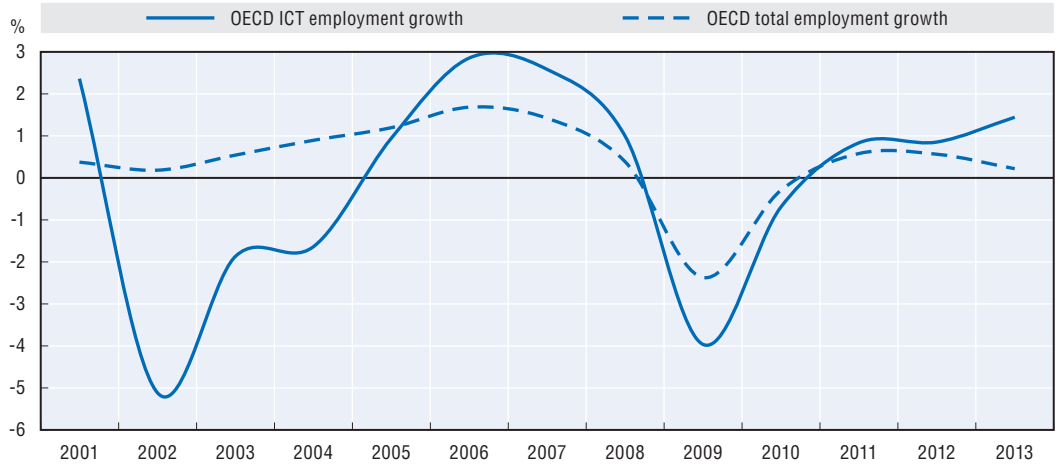
Overall, the contribution of the ICT sector to total employment growth has varied significantly over the past 15 years (Figure 1.10). In 2013, the ICT sector accounted for 22% of total employment growth, similar to its share just prior to the dot-com crisis.

Over 2001-13, the employment weight of ICTs decreased in countries with a large ICT sector and increased in countries with a smaller ICT sector. One likely explanation is that the crisis fostered rationalisation in large national ICT sectors and favoured ICT firms in countries with lower labour costs. Belgium and Hungary are the only exceptions to this general trend.

While employment within the ICT sector is stable, employment of ICT specialists across all sectors of the economy has risen, reaching at least 3% of total employment in most OECD countries (Figure 1.11). Finland, Sweden and Luxembourg employed the most ICT specialists in 2014 with shares of over 5%.

Figure 1.10. **ICT sector and total employment growth in the OECD area**

Year-on-year growth



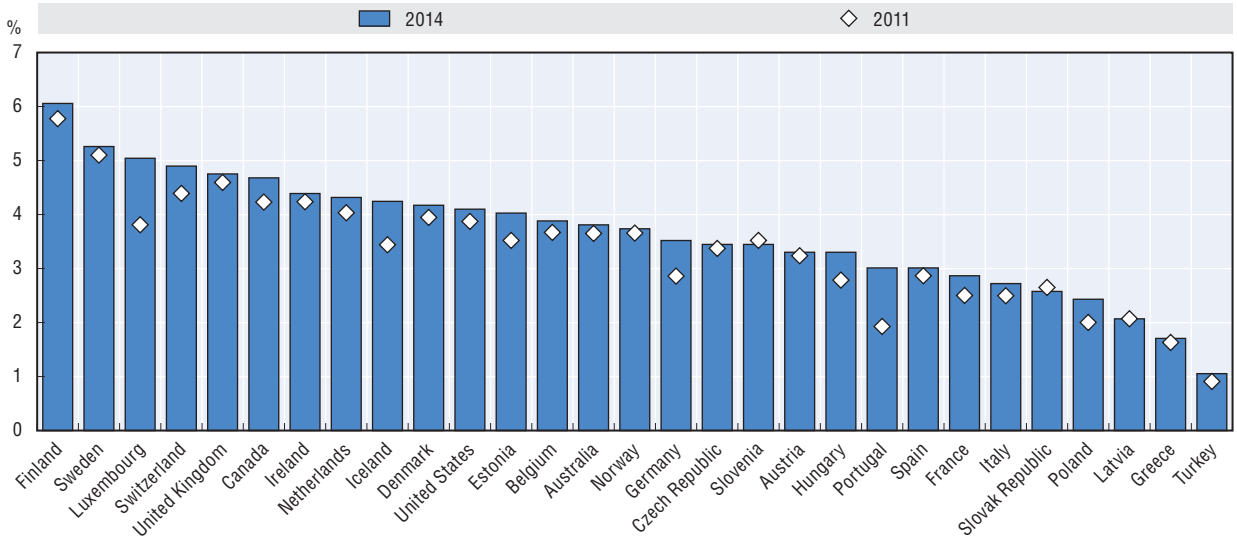
Notes: The aggregate for the OECD area includes 27 OECD countries for which data series were fully available. Data for 2013 are estimates.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4 and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224177

Figure 1.11. **Employment of ICT specialists across the economy**

As share of total employment



Source: Based on Australian, Canadian and European labour force surveys as well as United States Current Population Survey, April 2015.

StatLink http://dx.doi.org/10.1787/888933224189

A significant part of ICT value added and employment in OECD countries is accounted for by foreign affiliates (i.e. local firms owned or controlled by a foreign company) (see Chapter 2, Figure 2.9). Foreign affiliates contribute to a host country's international competitiveness by providing access to new markets and new technologies for domestic suppliers and buyers, generating knowledge spillovers for domestic firms, and investing a higher share of revenues in R&D.

Moving from the main developments in the ICT sector as a whole, the following paragraphs take a closer look at recent developments in communications markets including macro-trends, broadband penetration, prices and developments of Internet traffic. Developments in communications markets play an important role as good connectivity and affordable prices are necessary conditions for uptake of ICTs among businesses, citizens and governments.

Communications markets in the OECD area remained relatively stable in terms of revenues, investments and average penetration levels

Between 2012 and 2014, communication markets in the OECD area remained relatively stable in terms of overall subscriptions, penetration levels, revenues and investment. Overall telecommunication turnover in the OECD area reached USD 1.352 trillion, just below the 2011 level of USD 1.372 trillion, while investment stabilised at about 14.7% of total turnover.

The decrease in fixed telephone subscriptions was offset by growth in wireless broadband subscriptions, which increased by 14% per annum, a lower rate than in previous years. Mobile voice markets reached maturity in terms of penetration rates with 114 mobile subscriptions per 100 inhabitants, and growth in mobile communications is now focused on broadband services. Mobile broadband penetration reached 78.23 subscriptions per 100 inhabitants in the OECD area. Seven OECD countries now have over one subscription per inhabitant, highlighting the critical and growing importance of mobile technologies.

Wireless broadband subscriptions showed healthy growth, while fixed broadband subscriptions experienced high variation depending on the technology

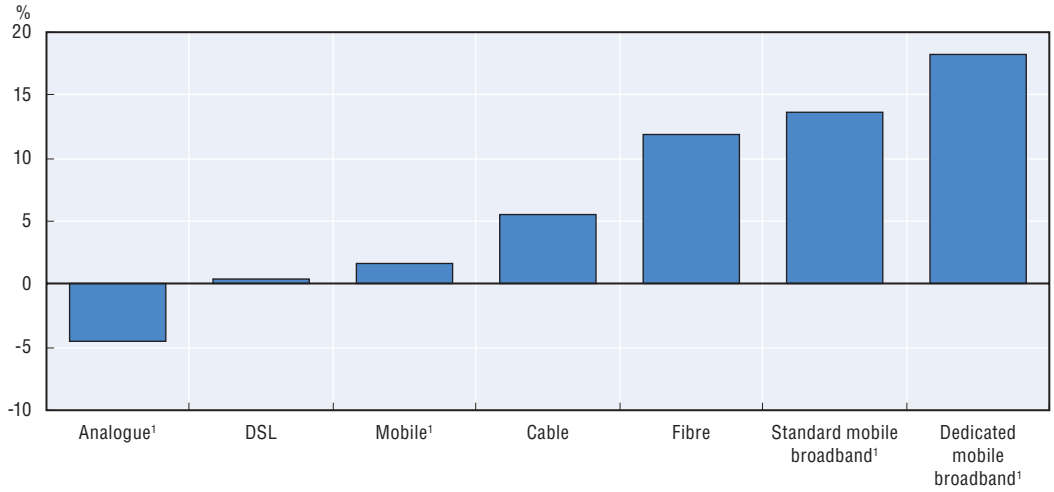
Growth rates in communication access paths between 2012 and 2014, broken down by technology, provide another perspective on the prevalence of mobile technologies (Figure 1.12). While wireless broadband subscriptions maintained a healthy growth of 18.14% (dedicated mobile broadband) and 13.61% (standard mobile broadband) per annum, fixed broadband subscriptions experienced very different growth rates. Fibre subscriptions showed a strong growth rate of 11.79% per annum, indicating that FTTH technology is gradually replacing DSL and cable broadband services. Not surprisingly, DSL subscriptions experienced a very low increase in relative terms (CAGR 0.4% in the same period). Cable grew at moderate rates (5.49% year on year), explained by the fact that DOCSIS 3.0 is more mature and provides higher speeds than deployed VDSL technologies.

Although some large OECD countries actively extend fibre connections, fibre subscriptions represent more than 10% of the total in only 14 OECD countries

On average, fixed broadband subscriptions amounted to 27 subscriptions per 100 inhabitants in the OECD area with Switzerland (47.3), the Netherlands (40.8) and Denmark (40.6) leading in terms of overall penetration (see Chapter 2, Figure 2.22). Some large OECD countries (Australia, Chile, Mexico, New Zealand and Spain) began to rapidly expand fibre penetration between 2012 and 2014 with the rate of deployment doubling each year. Overall, the transition from copper and cable to fibre is occurring at a gradual pace. At present, only 14 OECD countries have more than 10% of broadband subscriptions with fibre technology. Japan and Korea continue to lead the OECD by far with a fibre-to-the-home (FTTH) penetration rate of over 65%.

Figure 1.12. **Growth in communication access paths by technology**

As a percentage, June 2012 – June 2014



Notes: (*) For Analogue telephone lines and Mobile voice subscriptions, the growth rate is calculated from 2011 to 2013. Fibre includes FTTH/B/P and excludes FTTC. FTTC is included in DSL. Mobile accounts for all mobile subscriptions including voice only subscriptions and standard and dedicated mobile broadband subscriptions. Dedicated mobile broadband are data-only subscriptions. Standard mobile broadband are data and voice subscriptions.

StatLink http://dx.doi.org/10.1787/888933224199

A new OECD method allows measurement of broadband penetration by different speed tiers

The increased pervasiveness of the Internet in all sectors of the economy has underlined the importance of reporting broadband speeds. Accordingly, the OECD has adopted a set of harmonised speed tiers to report broadband speeds in a more detailed manner. The tiers break down subscriptions into those with advertised speeds higher than 1 Gbit/s, higher than 100 Mbit/s, higher than 25/30 Mbit/s, higher than 10 Mbit/s, higher than 1.5/2 Mbit/s and subscriptions not fulfilling these speed requirements but still qualifying as a broadband service (at least 256 Kbit/s of advertised download speed). For the first time, most OECD countries have used this breakdown to report broadband subscriptions (see Chapter 2, Figure 2.26).

The new method reveals a fixed broadband penetration rate of only 7.3 subscriptions per 100 inhabitants for speeds higher than 25/30 Mbit/s, indicating a need for further progress

The new measurement method enables analysis of broadband penetration by different speeds. While the average fixed broadband penetration for the OECD area amounts to 27 subscriptions per 100 inhabitants, the penetration for speeds higher than 10 Mbps amounts to 12.6 subscriptions per 100 inhabitants and 7.3 for speeds higher than 25/30 Mbit/s. These numbers indicate a need for further progress in the provision of high-speed connections, especially for applications where higher speeds are necessary such as medical imaging, office automation or effective use of cloud computing. In addition, actual broadband speeds are typically lower than advertised speeds (see OECD, 2014b).

In terms of mobile broadband speeds, network performance improved considerably due to LTE deployments between 2012 and 2014. According to Teligen/Strategy Analytics data from September 2014, 21 out of 34 OECD countries had at least one mobile operator

offering mobile broadband download speeds for laptops and tablets of 100 Mbit/s, in terms of theoretical advertised speeds.[41]

While prices for fixed-broadband connections showed little change, prices for mobile services have fallen markedly between 2012 and 2014

Affordability of broadband services is key to ICT adoption for all users, and for inclusive growth. Between 2012 and 2014, prices for fixed broadband showed little change. On average, countries with lower broadband speeds reported higher prices per Mbit/s. In contrast, Japan (USD 0.02), Sweden (USD 0.08) and France (USD 0.10) had the lowest prices per Mbit/s in 2014, in tandem with offers of high broadband speeds. Many countries have shown remarkable progress in bringing down entry prices per megabit per second. In 2012, three OECD countries had minimum prices of over USD 1, whereas in September 2014 the most expensive country was Greece with USD 0.74. Certain counties have considerably reduced their entry prices, such as Mexico (from USD 1.69 to USD 0.52) and Israel (from USD 0.77 to USD 0.32). Operators in those countries have also started offering higher speeds, usually through fibre networks, although these deployments may be restricted to the largest cities.

Prices for mobile services have fallen markedly between 2012 and 2014 for all OECD baskets. Prices for the 30 calls + 100 MB basket, for example, dropped by 10% from USD 19.74 to USD 17.72 per month and prices for the 100 calls plus 2 GB basket by 17% (see Chapter 2). Countries that experienced the largest price declines were Italy (52% on average across all baskets), New Zealand (46%) and Turkey (44%), while prices in Canada, France, Ireland, Slovak Republic, Switzerland and the United States remained relatively stable. Prices increased in Austria (36%) following a merger from four to three operators, and Greece (13%) over the two-year period.

Global Internet traffic continues to grow by 20% per year, albeit at a slower pace compared to previous years

Global Internet traffic continued to grow. According to Cisco's Visual Networking Index, Internet traffic grew by 20% CAGR in 2013. While this still represents double-digit growth, the growth rate has slowed down compared to 2012 (39%). This indicates that Internet adoption may be approaching saturation in areas where people have affordable access to networks, as over two thirds of the population in many OECD countries now use the Internet. For the first time, IPv6 usage is growing significantly, although from a very low base. Adoption has reached 30% in Belgium and over 10% in Germany, Norway, Luxembourg, Switzerland and the United States. However, the OECD average still only equalled 3.5% as of April 2014.

1.4 Uptake and use of ICTs across the digital economy

As the previous sections have shown, the public and private sectors have undertaken significant effort to expand existing broadband infrastructure. However, increased uptake on the demand side among businesses, households and the public sector is essential to benefit from these deployments. The uptake and adoption of ICTs depend on a multitude of factors, including the perceived value of using ICTs, the offer of digital applications and services, availability of the requisite skills and trust in the digital economy. The following paragraphs discuss usage across the economy and society, and present new business models and key issues in the area of trust.

While almost all businesses rely on ICTs, differences exist between countries and among large and small companies

Current adoption and usage rates show that almost all businesses in the OECD area rely on ICTs. In 2014, 95% of all enterprises with more than ten employees had a broadband connection. While close to 100% of large companies are connected to broadband, the experience for small firms is more varied. In Canada, Denmark, Finland, Korea, the Netherlands, Slovenia, Spain and Switzerland, almost all small firms had a broadband connection (98% and over). However, in Mexico, uptake was below 80% for small firms.

Statistics on the percentage of firms that have a website paint a similar picture. By 2014, more than three quarters of businesses (76%) had a web presence. In most OECD countries, 90% or more large enterprises had a website, while this was the case for only 69% of small businesses. Within the OECD area, web presence in SMEs ranges from 90% and above in Denmark, Finland and Switzerland to less than 50% in Latvia, Portugal and Mexico, indicating a significant divide in uptake between different OECD countries.

Participation in e-commerce is low and points to a significant divide between large companies and SMEs in the use of more sophisticated ICT services and applications

Analysis of Internet and ICT use beyond simple connectivity and web presence highlights significant potential to leverage ICTs for overall businesses processes. Participation in e-commerce, for example, is still relatively low in the OECD area (Figure 1.13). In 2013, only 21% of companies sold their products and services online, representing a small increase of 2 percentage points over 2009. There are considerable differences between OECD countries. In New Zealand, over 45% of companies engage in online sales, while the share is 10% or lower in Greece, Italy, Mexico and Turkey. There is also a significant gap between large and small companies. Participation in e-commerce for enterprises with 250 or more persons employed was 40% in 2013, but only 18.9% for small companies. The same picture is reflected in e-commerce sales as a percentage of turnover. On average, e-sales amounted to 17.1% of total turnover, however the share for large companies was 22.1% of turnover compared to 9% for small firms.

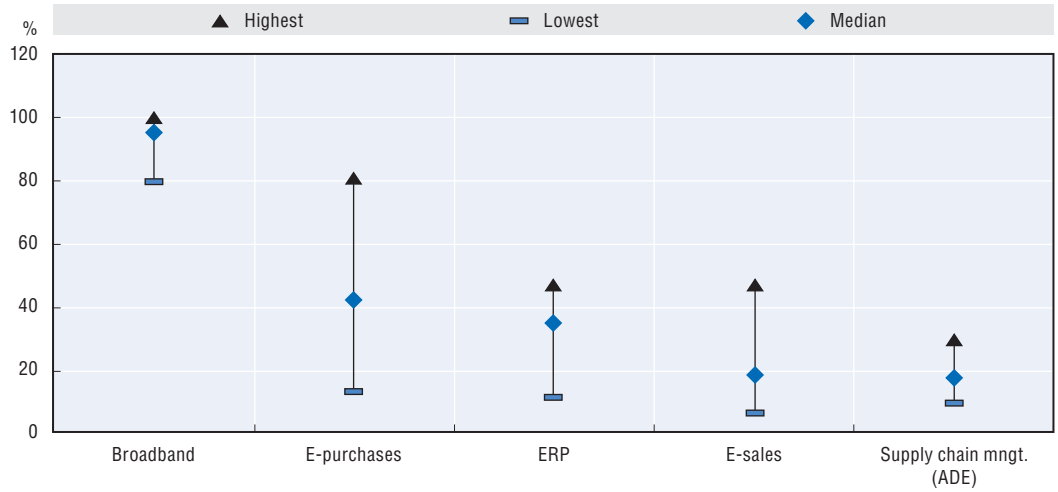
The modest uptake in e-commerce is paralleled by a relatively low adoption rate for supply chain management or enterprise resource planning (ERP) software applications to manage business information flows. One factor might be the changes in business organisation these processes necessitate. In 2014, on average, only 31% of companies used ERP applications, against less than 22% in 2010.

Further analysis shows that use of ERP applications is popular among large firms, with an adoption rate of more than 75% (Figure 1.14). These firms often need to manage more complex processes and can afford to invest in IT software. Conversely, ERP software was used by less than 25% of small firms, for which it has only recently become more affordable.

Differences in adoption rates of ERP software are also notable across countries. Adoption rates range between 44% and 92% for larger enterprises and between 7% and 41% for smaller ones, with Belgium, Austria, Sweden and Denmark leading, and Latvia, Iceland and the United Kingdom lagging for enterprises of all sizes (see Chapter 3, Figure 3.4).

Figure 1.13. **How enterprises make use of selected ICT applications, 2014**

Percentage of enterprises with ten or more persons employed



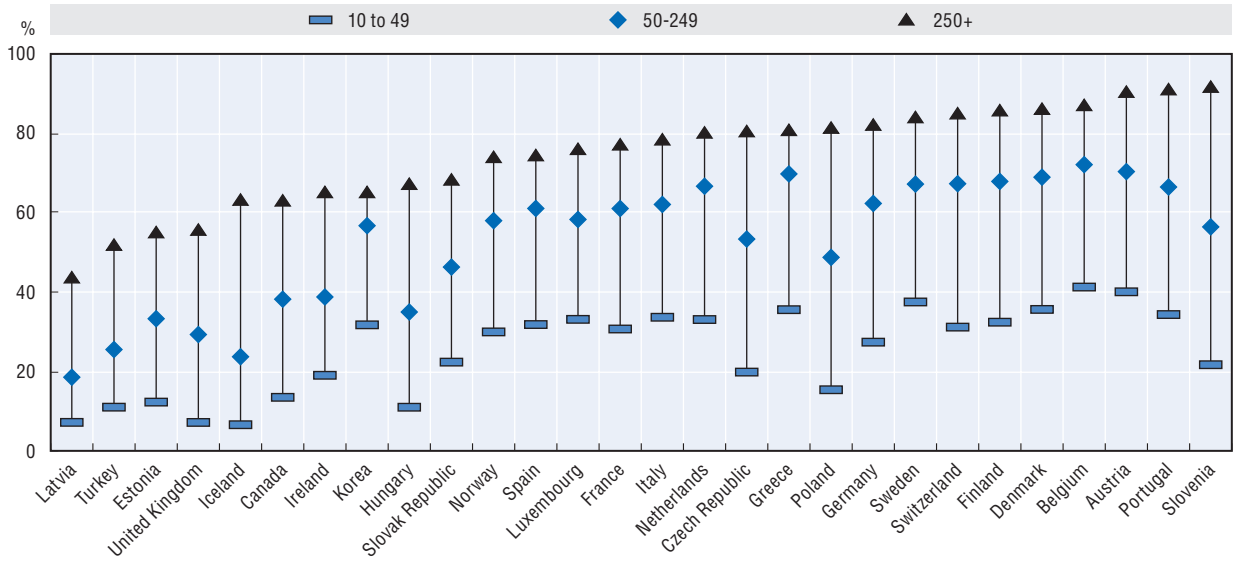
Notes: Supply chain management refers to the use of automated data exchange (ADE) applications. For countries in the European Statistical System, e-commerce variables (online purchases and online sales) refer to 2013. For Australia, Canada, Japan and Korea, data refer to 2013. For Mexico and New Zealand, data refer to 2012. For Switzerland, data refer to 2011.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224209

Figure 1.14. **Gaps in the use of enterprise resource planning software, 2014**

Percentage of enterprises in each employment size class



Notes: Unless otherwise stated, sector coverage consists of all activities in manufacturing and non-financial market services. Only enterprises with ten or more persons employed are considered. Size classes are defined as: small (from 10 to 49 persons employed), medium (50 to 249) and large (250 and above). For Canada, medium-sized enterprises have 50 to 299 employees. Large enterprises have 300 or more employees. For Korea, data refer to 2013. For Switzerland, data refer to 2011.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

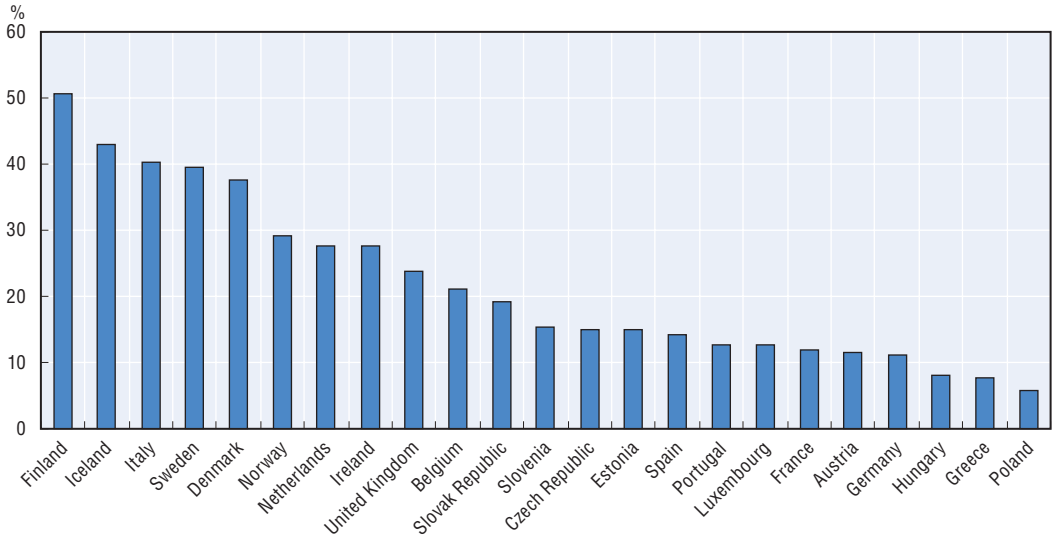
StatLink http://dx.doi.org/10.1787/888933224213

Diffusion of cloud computing among enterprises has accelerated over recent years, with higher uptake among large businesses compared to small businesses

Among the new uses of ICTs by firms, cloud computing deserves special attention. The cloud transforms computing into a service model that enables access to services, applications and computing power in a flexible, scalable and on-demand way (OECD, 2014c). Since cloud computing transforms computing into a service, firms can turn their capital expenditures into operating expenses.

Diffusion of different cloud computing applications and services among firms has accelerated in recent years. In 2014, 22% of companies relied on cloud computing services, with shares ranging from 50% in Finland down to 6% in Poland (Figure 1.15). In most countries, uptake is higher among large businesses (close to 40%) compared to small or medium-sized enterprises (around 21% and 27%, respectively). Only in Switzerland and the Slovak Republic are adoption rates higher for smaller companies than large ones. Businesses more frequently invest in cloud computing services with a high level of sophistication, such as finance/accounting software, CRM software and computing power, than less sophisticated services such as emails, office software or file storage (see Chapter 3, Figure 3.6).

Figure 1.15. **Use of cloud computing by enterprises, 2014**



Source: Eurostat, Information Society Statistics, January 2015.

StatLink http://dx.doi.org/10.1787/888933224224

Overall, businesses are increasingly adopting ICTs in their operations. However, there is room for progress, especially with regard to the use of more sophisticated ICT services and applications. In particular, small companies show low-uptake rates and are lagging behind. SMEs represent a large share of the economy in OECD countries; policy makers therefore have an important role to play in fostering their uptake of ICTs. To this end they need to carefully assess the barriers SMEs currently face with regard to adoption of ICTs, and promote uptake through measures such as raising awareness, promoting skills and tackling legal barriers that prevent small firms from purchasing and selling

online. In addition, the data indicate important differences in uptake rates across OECD countries. Since uptake of ICTs affects firm productivity, policy actions (or lack of) can have long-lasting implications for overall economic productivity. This implies a need for urgent policy actions, especially in countries with low uptake rates. The next section takes a closer look at uptake and use of ICTs among individuals.

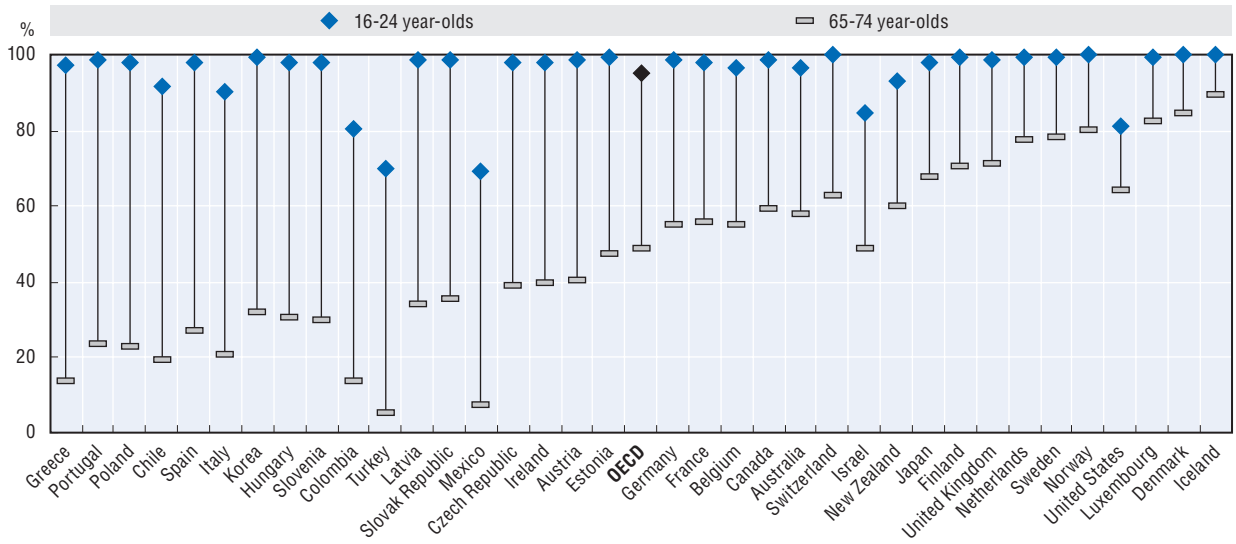
While almost all adults in the OECD area use the Internet, differences exist based on age and education

In 2014, diffusion of the Internet among adults in the OECD area was widespread (Figure 1.16) with 81% of the adult population accessing the Internet of which over 75% use it on a daily basis. More than 40% of adults used a mobile or smartphone to connect to the Internet in 2013.

However, gaps exist across different age groups and education levels. In most countries, uptake by young people is nearly universal, but there are wide differences for older generations. Over 95% of 16-24 year-olds in the OECD area used the Internet in 2014 against less than 49% among 65-74 year-olds. Usage rates for 65-74 year-olds with tertiary education are generally in line with those of the overall population, and in leading countries approach usage rates among 16-24 year-olds. However, differences between high and low educational attainments among 65-74 year-olds are particular large in Hungary, Poland and Spain (OECD, 2014a).

Figure 1.16. **Gaps in Internet usage by age, 2014**

As a percentage of population in each age group



Notes: Except otherwise stated, Internet users are defined for a recall period of 12 months. For Switzerland, the recall period is 6 months. For the United States, no time period is specified. For the United States, data refer to individuals aged 18 and above living in a house with Internet access, and to age intervals 18-34 instead of 16-24 and 65 and above instead of 65-74. Data are sourced from the US Census Bureau. For Australia, data refer to 2012/13 (fiscal year ending in June 2013) instead of 2013, and to individuals aged 65+ instead of 65-74. For Canada, Japan and New Zealand, data refer to 2012 instead of 2014. For Chile, Israel, the United States and Colombia, data refer to 2013 instead of 2014. For Israel, data refer to individuals aged 20-24 instead of 16-24. For Colombia, data refer to 12-24 year-olds instead of 16-24, and 55 year-olds and above instead of 65-74. For Japan, data refer to 15-28 year-olds instead of 16-24 and 60-69 year-olds instead of 65-74.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224237

Nearly all Internet users rely on the Web to send emails and read news

Basic use of the Internet is nearly ubiquitous in the OECD area. Over 2013-14, on average 87% of Internet users sent emails, 82% relied on the web to obtain information on goods and products, and 72% read news online (see Chapter 3, Figure 3.9). While 58% of Internet users ordered products online, only 21% sold products over the Internet. These activities showed little variation across all countries. However, use of the Internet for more sophisticated activities, such as e-government, e-commerce and online banking, showed larger cross-country variability. For example, more than four out of five Internet users in Finland engage in online banking, compared to less than one out of five in Greece.

More sophisticated Internet use, associated with higher levels of education, differs across OECD countries

More sophisticated Internet activities are associated with higher levels of education and more complex services infrastructures. The breadth of Internet activities carried out by users with tertiary education is, on average, 58% larger than for those with lower secondary education and below. Differences by level of education are particularly high for Belgium, Hungary, Ireland, Korea and Turkey.

In terms of e-commerce, about 50% of individuals in OECD countries bought products online in 2014, up from 31% in 2007. This trend is very likely to continue in the near future and has already disrupted traditional distribution channels for some categories of products, such as travel and holiday services. The rapid diffusion of smart mobile devices has resulted in a growing number of individuals buying products via their mobile device.

The share of online purchases varies widely across countries as well as across different product categories, with age, education, income and experience all playing a role in determining the uptake of e-commerce by individuals. For example, more than three quarters of adults buy online in Denmark, Norway and the United Kingdom, while only between 10% and 20% of adults do so in Chile and Turkey, and below 5% in Mexico and Colombia.

An increasing number of individuals use the Internet for education and continuous learning

Over the last few years, ICTs have contributed to a wider array of learning opportunities, with massive open online courses (MOOCs) becoming increasingly popular. In 2013, 7.8% of Internet users in the European Union followed an online course compared with 4.7% in 2007. This percentage varied from 16% in Finland to less than 3% in the Czech Republic (see Chapter 3, Figure 3.13).

The next section discusses the use of digital government services by businesses and households, as well as the use of ICTs by the public sector itself.

While use of e-government services is widespread across companies, only 35% of individuals use e-government services on average in the OECD area, with large differences across countries

e-Government services and applications are used by both companies and individuals. While use of e-government is frequent in OECD countries, the level of e-government engagement with people varies significantly depending on the country.

In 2013, the large majority of OECD enterprises (90%) interacted online with public authorities. Compared to 2010, the share of enterprises completing and submitting forms electronically increased by almost 20 percentage points in the Czech Republic and Italy, and by over 10 percentage points in Ireland, New Zealand and Norway.

Individuals use e-government services to a lesser extent. In 2013, 64% of individuals in the OECD area relied on e-government services for activities such as retrieving government information and downloading or filling and transmitting forms online. This share, however, remains quite dispersed across countries. In Iceland, 88% of individuals use e-government services, while less than 40% do so in Chile, Italy and Poland. Poor connectivity and provision of e-government services, as well as insufficient skills or other cultural factors, are often the root causes of low uptake rates. In addition, users in the EU area experienced problems with e-government services such as technical failures of websites (24% of all users in 2013) and outdated information (23% of users), factors that can also slow down the use of e-government services.

Governments are relying on digital technologies to move from a citizen-centred to a citizen-driven approach

Governments, on their side, aim to achieve public sector transformation through the use of ICTs to shift from a citizen-centred to a citizen-driven approach, implying that citizens and businesses determine their own needs and address them in partnership with public authorities (see Chapter 3, Box 3.1).

This shift is also reflected in government use of social media. The majority of governments around the world now draw on social media to communicate and engage with their citizens. As of November 2014, the office representing the top executive institution (head of state, head of government, or government as a whole) in 28 out of 34 OECD countries had a Twitter account and 21 had a Facebook account. This has enabled some governments to achieve significant popularity rates (Figure 1.17).

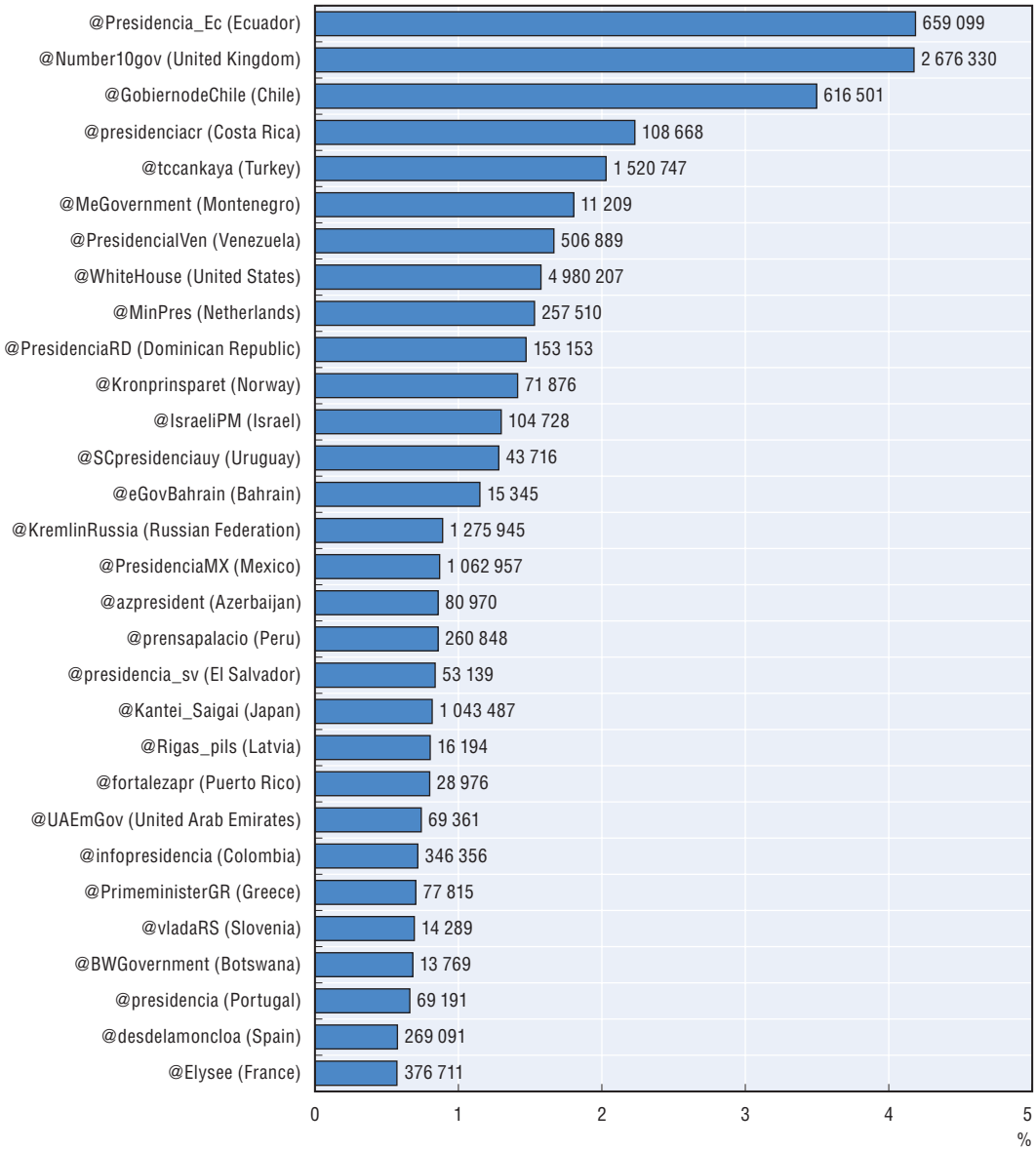
However, there is considerable uncertainty among institutions regarding how best to use social media outside of "corporate" communications (e.g. to improve public services or create trusted relationships with citizens). As a result, measurement is scarce and rarely targeted to relevant goals. Moreover, social media do not automatically "level the playing field" in the sense of empowering all societal groups equally, as level of education still determines the likeliness of using social media in many OECD countries (OECD, 2014d).

Governments are promoting open government data to increase public sector transparency and deliver societal and economic benefits

Another key area for governments is open government data (OGD), which has demonstrated significant potential to transform public services and is driving sectors to adopt a data-driven and inclusive approach. Many governments use OGD as an essential strategic enabler to increase public sector transparency and deliver societal and economic benefits. Reuse of government data enables entrepreneurs to create new types of commercial content and services, individuals to make more informed choices, and governments to work with citizens to create more liveable public spaces. However, many legal, institutional and policy-related issues still need to be addressed before governments and citizens can fully capture the value of data usage to transform operations, services and policy making.

Figure 1.17. **Top 30 central government Twitter accounts**

As a percentage of the domestic population and by number of followers



Notes: OECD calculations based on Twiplomacy data, June 2014 (Followers); World Bank (2013 population data). Accounts for head of state, head of government or government are given as a whole. Personal or political accounts are excluded. Only the account with the most followers per country is displayed. States with less than 500 000 inhabitants are not included.

Source: Androsoff and Mickoleit, 2015.

StatLink http://dx.doi.org/10.1787/888933224246

1.5 New and evolving business models

Increasing ICT uptake has been observed during recent years among businesses, governments and different groups of society. However, there is still huge potential for increased adoption and use of ICTs, especially in terms of more sophisticated ICT use across the economy and society. Tapping this potential will be crucial for further economic growth and social benefits. Several trends such as increased penetration of smartphones,

the surge in mobile social networking and heightened production of new data are touted to further spur uptake and drive the emergence of new businesses. These trends and emerging business models are discussed below.

Increasing penetration of smartphones, growing mobile social networking and the development of new data are driving the emergence of new business models

Increased smartphone penetration and intensity of use across society, the surge in mobile social networking and the development of new data are driving the emergence of new business models in the digital economy, and continue to radically transform established industries such as transportation, energy media delivery or banking.

Between 2012 and 2013, smartphone adoption in OECD countries grew by 30%, reaching a high of 73% in Korea and an average of almost 50% in 2013. Individuals use their smartphones for an increasing variety of activities with increasing intensity, including activities traditionally carried out on a computer, such as browsing the Internet, emailing or accessing a social network. More sophisticated activities, including online banking, mobile purchases and job search, are also experiencing fast growth. Many of these activities are carried out on dedicated mobile apps. Popular travel, mobility and retail apps have all made a recent appearance (TechCrunch, 2014), pointing to the growing effect of digital services delivered via mobile apps on traditional sectors.

Online social networking has largely gone mobile. In 2013, over 40% of individuals in OECD countries used their smartphones several times per day to access social networks. Several central elements of social networking, such as an online identity, sharing of content and frequent status updates, play an important role in preparing the grounds for new business models to flourish, notably those building on collective consumption in the sharing economy and exploring the possibilities of collaborative production.

Many mobile apps not only function with but also produce data, which can be used by entrepreneurs and businesses to offer innovative services. An important form of data produced on smartphones is geo-locational data. These are collected by and used in numerous mobile applications and services (mostly in real time) such as online maps. In 2013, 68% of smartphone users in the OECD looked up directions or used a map on their smartphone, up 18% from 2012 (Figure 1.18; Chapter 3, Figure 3.16). Beyond its use for online mobile maps, geo-locational real-time data enable new services in areas such as shared mobility and multichannel retailing.

These trends are influencing incumbent businesses in established markets and are enabling the emergence of new business models. The following sections shed some light on new business models in retail, banking, health and collective consumption.

Many firms are adopting multi-channel selling strategies and engaging in m-commerce

A growing number of individuals across the OECD purchase goods and services via their smartphones. The share of smartphone users who ordered a good or a service on their mobile device has grown from 24% in 2001 to 38% in 2013, and is likely to increase in coming years. Product information gathered on smartphones also influences purchasing decisions both online and offline. From the consumer perspective, m-commerce and mobile product information gathering translate largely into greater choice, convenience and reduced transaction costs, notably in product search.

Figure 1.18. **Smartphone use of selected geo-location services, 2013**

Notes: No data available for Chile, Estonia, Iceland, Luxembourg, Slovak Republic, Slovenia. The sample covers private smartphone users who use the Internet in general.

Source: Our Mobile Planet, 2013.

StatLink http://dx.doi.org/10.1787/888933224251

Firms are responding to these trends by combining bricks-and-mortar retailing and online presences. The effects of this multichannel selling are mixed, especially for SMEs, which rely increasingly on e-commerce intermediaries. On the one hand, these intermediaries allow for wider reach and facilitate online selling through the offer of various services along the selling chain. On the other hand, large intermediaries might also create new entry barriers for SMEs.

Uptake of e-commerce by SMEs has been moderate due to trade and regulatory barriers, as well as consumer mistrust, especially across borders

Overall uptake of e-commerce by SMEs has been moderate so far, especially across borders. Among other factors, consumer resistance to cross-border purchases, trade and regulatory barriers (e.g. high custom administration costs, high tariffs, inadequate property right protection) and lack of working capital to finance exports may explain this situation. Policy measures to reduce these barriers will benefit SMEs in particular, as they typically have only limited resources to address these barriers.

Retail banks are seeing demand shift to online and mobile banking and are starting to face competition from online banks and peer-to-peer platforms

Retail banks are facing continuing shifts in demand through online and mobile banking, as well as new competition from online peer-to-peer (P2P) lending platforms or, more recently, P2P currency exchange models. P2P platforms are still too small to significantly affect retail banks, but current trends suggest that they may have a disruptive potential on the banking sector.

More than half of Internet users in OECD countries use online banking, and mobile banking is catching up. In 2013, 60% of Internet users in OECD countries used online banking, up from 42% in 2011 and 31% in 2007 (OECD, 2012, 2014a). Uptake of mobile online

banking has also increased at a similar rate, from 35% of smartphone users in 2012 to 47% in 2013 (see Chapter 3, Figure 3.18).

The rise of online and mobile banking is changing market boundaries and the parameters for competition in traditional retail banking. In reaction to higher competition from online banks, offline banks can either specialise in specific place-based business (e.g. farmers), or step up their response to online competition, an option that involves significant costs. The expected trend points towards a reduction in local bank branches, with 20% of local branches estimated to disappear by 2020 in the United States, mostly to the detriment of smaller regional and community banks (PWC, 2014a).

P2P lending platforms tend to offer better returns than traditional banks and are mostly unregulated

New competition for retail banks also comes from P2P lending, which has blossomed thanks to low interest rates (*Economist*, 2014). P2P lending platforms match borrowers and lenders, mostly via online auctions, and offer often better returns than most banks. So far, P2P lending platforms are primarily targeting the consumer credit market. However, more recently, platforms like Funding Circle have started to focus on small business lending. P2P lending platforms have not yet come under serious economic stress. If their strong growth continues, and if they prove able to deal with economic uncertainties, they may become a potentially disruptive competitive force in consumer credit markets.

P2P lending has attracted little attention from regulators to date. The United Kingdom is among the few countries to have taken a pro-active stance on regulating P2P lending platforms. Important issues covered in the UK regulatory framework on crowdfunding over the Internet include minimum capital requirements, dispute resolution rules, client money protection rules, disclosure and reporting rules, as well as successor loan servicing arrangements.

The amount of digital content is growing, but there remains room for dematerialisation

Thanks to the growing availability of digital online content, consumption continues to rise. For example, Spotify, an online music streaming service, offers over 20 million tracks licensed globally, and adds on average over 20 000 songs per day.[42] The iTunes Store, available in 119 countries, offers a selection of over 26 million songs (Apple, 2013). However, despite the transformations experienced by major content markets, there remains room for dematerialisation, especially in the area of videos and books (Figure 1.19).

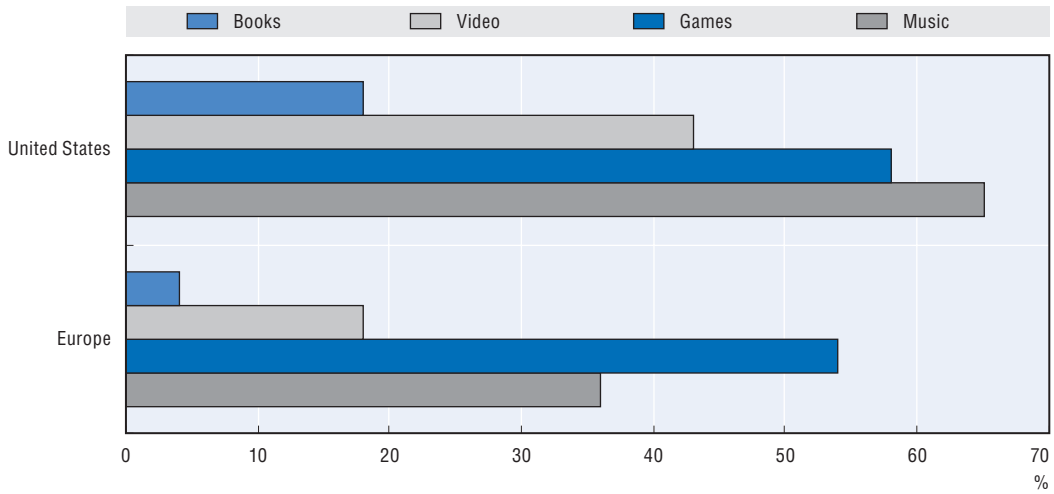
User-created content, notably images and video, continues to grow strongly. YouTube, for instance, reported in mid-2014 that users are uploading 100 hours of video to YouTube every minute.[43] Increasingly, digital content is being consumed and shared on mobile devices.

Television is undergoing significant transformation with delivery of audio-visual content over the Internet, and advertising revenues in digital content markets growing fast

Television services are also undergoing transformation with delivery over the Internet targeted to individuals and increased flexibility. Audio-visual content delivered over the Internet allows users to view films and programmes of their choice on any device, at any time. Netflix, for example, claims to offer over 10 000 movies and TV titles via its streaming-on-demand platform in the United States.[44] These offers are increasingly

being picked up on mobile devices. In November 2014, for the first time, Americans spent more time on mobile devices (177 minutes per day on average) than in front of a TV (168 minutes) (Flurry, 2014).

Figure 1.19. **Digital shares in content markets, US and EU, 2013**



Source: IDATE, 2014.

StatLink http://dx.doi.org/10.1787/888933224264

Advertising, a main revenue source in several digital content markets, is following suit. In 2013, revenues from online advertisement amounted to USD 117 billion and are expected to increase to over USD 190 billion by 2018, closing the gap with total TV advertisement revenues. Search accounts for the largest proportion of online advertising (USD 48 billion in 2013), followed by video and mobile advertisement with compound annual growth rates of 23.8% and 21.5% respectively (PwC, 2014b). Google currently dominates the market for online advertising, while Facebook and Google increasingly command the mobile segment (see Chapter 3, Figure 20), which may raise competition issues in the future.

Smartphone apps have enabled rapid development of the mobile health market and allowed for a higher degree of self-monitoring and wider collection of health data

The convergence between wireless communication technologies and healthcare devices, as well as increased use of smartphones for health monitoring, has started to reshape the health sector and open new markets with large growth potential.

Smartphones, in particular, offer the potential to broadly and cheaply diffuse more intensive self-monitoring, feedback, self-management and clinical support than has been possible previously. The data gathered can be leveraged to trigger highly personalised interventions and can be stored in large databases with the potential to boost healthcare research and innovation.

The market for mobile health and wellness apps (*mHealth*) has developed rapidly in recent years. The number of mHealth apps published on the two leading platforms, iOS and Android, has more than doubled in only 2.5 years to reach more than 100 000 apps (Q1 2014) (research2guidance, 2014). In 2012, 69% of US smartphone owners reported tracking at least one health indicator such as weight, diet or exercise (Fox and Duggan, 2013).

According to some estimates, the global mHealth market may reach USD 23 billion in 2017, with Europe accounting for USD 6.9 billion and Asia-Pacific for USD 6.8 billion, ahead of the North American market of USD 6.5 billion (GSMA and PwC, 2012). By 2017, mHealth could potentially save a total of EUR 99 billion in healthcare costs in the European Union. The largest savings would be in the areas of wellness/prevention (EUR 69 billion) and treatment/monitoring (EUR 32 billion), while increasing the wage bill for workers in mHealth by EUR 6.2 billion (GSMA, 2013).

Governments have a rising interest in electronic health records with many OECD countries having a national plan for their implementation

Increasing use of ICTs in healthcare has led to rapid growth in the amount of digitised data available. Over the past decade, in particular, there has been a rising interest in electronic health records (EHRs) in OECD countries. In 2011-12, most countries had a national plan or policy to implement EHRs (22 of 25 countries) and the majority had already begun to implement that plan (20 countries) (OECD, 2013b). EHR systems in some countries include data on key patient characteristics and health problems, as well as patient histories of encounters with the healthcare system and treatments received from a variety of healthcare providers (see Chapter 3, Figure 3.21). The greatest contribution of these systems as they develop is the potential for secondary analysis of data to monitor and conduct research, with a view to improving the health of the population and the quality, safety and efficiency of healthcare. The most commonly included secondary uses reported were public health and health system performance monitoring. Fourteen countries also indicated that they intended for physicians to be able to query data to support treatment decisions.

New businesses in the area of urban mobility and home sharing enable the shared consumption of private goods, which has raised new regulatory concerns

Another bundle of innovative business models has emerged over the past years under the heading of the "sharing economy". These models enable collective consumption of private durable goods by providing access to excess capacity of these goods.

Prominent sharing economy businesses are platforms that offer, for example, short-term rental of space, mostly homes. Although home exchanges are not new, the speed and scale at which platforms such as Airbnb have made commercial home sharing a common practice is unprecedented. The second market in which sharing economy business models have emerged at great speed is urban mobility. Shared mobility options range from the rental of private cars (Zipcar), rides (Uber, Lyft, blablacar) and parking spaces (justpark) to the rental of free floating (Car2go, DriveNow) and station-based cars (Autolib') and bikes (Velib'). These services are enjoying strong success among users, although their impact on urban mobility remains to be assessed (see also Chapter 3).

Factors that facilitated the emergence of these goods are, among others, increasingly ubiquitous mobile Internet penetration, the availability of real-time geo-locational data, social networks and the availability of online ratings, as well as constrained economic conditions which may have encouraged citizens to welcome additional opportunities to monetise assets, and consumers to welcome cheaper offers.

Many sharing economy businesses models currently rely on self-regulation, notably via ratings and reviews. While these reviews provide incentives for both sides to deliver on their promises, they suffer from several shortcomings, such as low response rates, incomplete information and misleading ratings.

While the sharing economy brings benefits to consumers such as a high variety of services and lower prices, its business model is not always consistent with existing regulations and laws, established at a time when the underlying technologies were unavailable. This situation has raised strong reactions from incumbent business associations, who regard it as unfair competition; from trade unions, who are concerned by the undefined status of the people working in these new businesses; and from policy makers, who want to ensure the protection of consumers and workers, to the point that these activities have been forbidden in some countries or cities.

The challenge for regulations and laws is to ensure effective protection of consumers and workers in this new economic environment, while fostering the potential benefits from the sharing economy. In addition, the changing business environment creates opportunities for strong co-operation across different ministries (e.g. ministries of transport, the economy and those concerned with ICT).

Crowdsourcing is used for multiple firm activities such as the creation of ideas, product development and marketing

While the sharing economy concerns "collective consumption", crowdsourcing and crowdfunding provide two interesting examples of "collaborative production". Both large companies and entrepreneurs make increasing use of these practices, for example, for capital peer-to-peer lending which could also be beneficial for SMEs.

Crowdsourcing can be applied to a large range of activities, the most common of which include idea creation, product design, problem solving, product development, marketing and advertising (Simula and Ahola, 2014). Large firms and organisations such as IBM, General Electric, NASA, DARPA or USAID tend to organise crowdsourcing within their internal networks. Smaller firms that have neither the scale nor the resources to undertake internal crowdsourcing address external communities, mostly via a crowdsourcing platform. Crowdsourcing is typically organised as a contest of competing people in which a prize rewards the winning solution. Platforms that enable online collaboration, such as Wikipedia, or co-creation, such as Quirky, are still rare.

Crowdsourcing for product development is not a widely spread practice, but some firms are using it intensively and with success (Figure 1.20). The most common approach elicits customer involvement and feedback through social media (see Chapter 3, Figure 3.22). In the EU28 countries, almost 10% of enterprises are currently involving customers in the development or innovation of goods and services. Another good example is the Chinese smartphone producer Xiaomi, which releases a new version of its MIUI software once per week, based on customer feedback. Customers make suggestions and vote on modifications via Weibo, the Chinese equivalent of Twitter (*The Economist*, 2013).

To date, crowdsourcing in OECD countries is not regulated. However, issues such employment regulation (e.g. rules for employing and remunerating people online), as well as issues related to intellectual property will need to be addressed in the future.

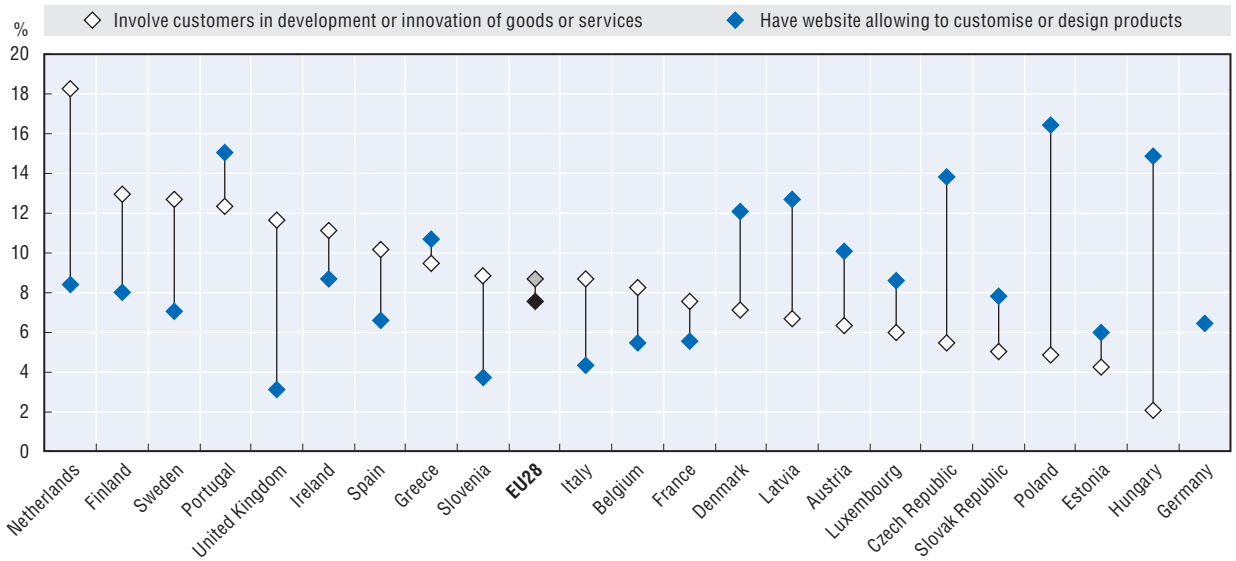
Crowd-funding provides additional sources for early stage funding of start-ups, but a clearer regulatory framework is needed to foster its potential and minimise risks

The term *crowdfunding* is used for different types of platforms, enabling lending (P2P), donations or reward-based funding, and equity crowdfunding (investment). The crowdfunding market has grown strongly over the past years, driven mainly by non-equity

crowdfunding. Crowdfunding is most developed in the United States and Europe, which accounted for 60% and 35%, respectively, of the market in 2012 (Massolution, 2013).

Non-equity crowdfunding (donation and reward-based) platforms create opportunities for innovators while creating little risks for backers, which have no financial interests attached to their contribution, but rather care for the (future) product (Belleflamme and Lambert, 2014).

Figure 1.20. **Customer involvement in product development, 2013**



Note: Unless otherwise stated, sector coverage consists of all activities in manufacturing and non-financial market services. Only enterprises with ten or more persons employed are considered.

Source: Eurostat, Information Society Statistics, January 2015.

StatLink http://dx.doi.org/10.1787/888933224270

Opportunities created by equity crowdfunding platforms for both entrepreneurs and investors should be examined together with risks. Given the potential to provide additional resources for early stage funding of start-ups, a clear regulatory framework is necessary to minimise risks and foster the potential of crowdfunding (Wilson and Testoni, 2014). Few countries have addressed these challenges so far. In particular, in Europe, the second largest crowdfunding market, a variety of national regulations remain to be addressed. The United States has adopted a comprehensive legal framework for crowdfunding, through the Jumpstart Our Business Startups (JOBS) Act, which is currently being implemented.

1.6 The Internet of Things

While use of the Internet as a digital platform has enabled the creation of the sharing economy, the ability to connect any smart device or object is enabling the "Internet of Things". It will have a profound impact on multiple sectors of the economy, including industry automation, energy provision and transportation (see Chapter 6).

In the coming years, billions of devices will be connected to the Internet. While the vision of smart, communicating objects has been around for decades, the smartphone revolution has made it possible. Smartphones and tablets provide an easy, ever-present interface through which people can interact with connected devices and objects. In

addition, the scale of demand for smartphones has led to a dramatic decline in costs for the various components of connected devices, such as screens, sensors, processors and network interfaces.

The present report uses a broad definition of the Internet of Things (IoT), encompassing all devices and objects whose state can be read or altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, all of which are often considered to form part of the "traditional Internet". However, as these devices are integral to operating, reading and analysing the state of IoT devices, they are included here.

The Internet of Things consists of a series of components of equal importance – machine-to-machine communication, cloud computing, big data analysis, and sensors and actuators. Their combination, however, engenders machine learning, remote control, and eventually autonomous machines and systems, which will learn to adapt and optimise themselves.

There have been numerous predictions about the size of the Internet of Things. The most widely cited is that of Ericsson, which stated in 2010 that there would be 50 billion connected devices by 2020. Prior to this, Intel estimated in 2009 that 5 billion devices were already connected to the Internet and predicted that this number would rise to 15 billion by 2015. In 2012, the OECD produced its own estimates of IoT usage in people's residences, to verify some of the claims. Today, in OECD countries, an average family of four with two teenagers has ten Internet connected devices in and around their home. Estimates indicate that this figure could rise to 50 by 2022. As a result, the number of connected devices in OECD countries would increase from over 1 billion today to 14 billion by 2022. Actual measurements of the number of devices connected to the Internet have proven harder to obtain, with countries only now starting to collect some data.

Governments have recognised the potential benefits of the Internet of Things and introduced regulations in areas such as numbering policies and spectrum policy

A number of governments have introduced regulations that depend on the Internet of Things to achieve policy goals. For example, the Internet of Things enables governments to manage public spaces in more efficient, more effective or different ways. Remotely monitoring traffic lights or dykes allows governments to optimise traffic flow or to better understand flooding risks. It also allows governments to achieve policy goals in new ways. For example, reducing congestion using road pricing, calculated on time of day and distance travelled, is possible via GPS and mobile communication, but more difficult to achieve through conventional means. Similarly, smart energy meters lead to more decentralised energy markets and higher consumer awareness of energy use. Analysts and governments have high expectations of eHealth devices which will allow remote monitoring of patients at home or work. However, only a few such devices are available on the market – a situation that appears to be due not to a lack of research or government commitment, but rather to difficulties in implementation.

The potential benefits of the Internet of Things feature in a growing number of public policies, either as a means to achieve goals or an area targeted for research. There is no consistent approach among governments, but some examples can be provided. In particular, some countries have begun to assess whether current policies are aligned

with the perceived future. Ofcom in the United Kingdom, for example, has initiated a consultation on the implications of the Internet of Things for spectrum and numbering policy (Ofcom, 2014). The Netherlands, the first country to liberalise access to IMSI numbers for SIM cards, is consulting on further policies regarding signalling point codes needed for routing traffic in mobile networks.

Governments still need to address multiple issues such as trust and naming and numbering or standardisation

The evolution of the Internet of Things will require substantial efforts on the part of governments to re-evaluate and review a significant number of policies. These could include the regulations surrounding naming and numbering, particularly with regard to numbers used in mobile networks, where further liberalisation and access for private networks could bring great economic benefits. Policies surrounding the use of "national" numbers on an international scale will also need discussion. Spectrum is another key area, as the extent needed for the Internet of Things is as yet unclear. Globally harmonised ranges would be best, but may be unattainable. Standards are also a challenge, as the Internet of Things encompasses technical levels through to business processes, as well as political decisions. As a result, existing applicable standards are fragmented. Lastly, privacy, security, liability, consumer rights and reliability are all affected by the pervasiveness and longevity of the Internet of Things.

As the Internet of Things becomes pervasive, it will touch much of government policy. Policy makers should therefore focus not just on the potential benefits, but also work to identify where data and functionality offered by the Internet of Things could be leveraged and combined with other data elsewhere.

In order to ensure that the Internet of Things works to the benefit of people, some have argued that it should be thought of as the "Internet of Trust", as trust will be fundamental to enhancing user experience and addressing key legal challenges such as user privacy. Another pertinent factor is legal frameworks. As Capgemini noted, the "IoT is global [but] the law is not" (2014). The OECD has typically considered security, privacy and consumer protection as key elements for building trust in new technologies such as the Internet of Things (OECD, 2005c).

1.7 Trust, competition and network neutrality

To maximise the potential of the digital economy for productivity, innovation, inclusive growth and jobs, governments need to work in multiple policy areas. They must, for example, engage in further and renewed efforts to protect competition, lower entry barriers in communications and content markets, strengthen regulatory coherence, improve skills, assign spectrum in an efficient manner and establish trust at the infrastructure and applications layers. Policy implications derived from new developments in the digital economy are discussed throughout all the chapters of this report. The following paragraphs focus on three policy issues: trust, competition and net neutrality.

Digital trust is elevated in profile and importance

The opportunities of the digital economy will not be realised in the absence of trust. Trust is a powerful tool in complex environments for reducing uncertainties and enabling reliance on others. It underpins business, institutional and personal relationships and is particularly important in a global online environment. In 2014, in an OECD survey on

31 possible priority areas for the digital economy, governments identified security as the second highest priority area and privacy as the third, with only broadband coming higher (OECD, 2014a).

Although the disclosures in 2013 by Edward Snowden have no doubt elevated the visibility of security and privacy, the increasing prominence of these issues is the result of a transformation in the way data are generated, shared and analysed, and the corresponding benefits that these developments have brought in terms of innovation, growth and well-being. It is also the result of the horizontal nature of security and privacy issues and the increasing recognition that they need to be considered within the broader economic and social landscape, encompassing trade, competition, education and health, to name but a few.

User privacy and security concerns are growing

Growing trust concerns were highlighted in 2014 by at least three surveys of Internet users in the United States and Europe. These suggest that 64% of respondents are more concerned about privacy than they were a year ago (CIGI, 2014), while 91% agree that they have lost control of their personal information and data (Pew, 2014). Top concerns include the misuse of personal data and the security of online payments (EC, 2015). In 2014 and 2015, security breaches in companies from North America to Asia affected tens of millions of individuals and had a significant economic impact, with one breach reportedly leaving the company with charges of USD 162 million (Lunden, 2015). However, the damage to the firm's reputation, relationships in the industry and impact on employees may be longer-lasting and hard to measure. Such data security breaches are not limited to the private sector; many involve personal data, and as such also represent a privacy problem. There is thus a growing need for better metrics and evidence to inform policy makers.

Businesses invest more to restore trust

The perception that user trust is at stake persists and has been reflected in recent business practices to protect privacy and secure services.

Demand for security expertise continues to grow steadily and is accelerating for privacy

Locating available professionals with the required skills to help organisations manage digital risks to security and privacy remains a challenge. For example, the International Information Systems Security Certification Consortium (ISC)[2] noted a fourfold increase over a decade of certified individuals worldwide as of the end of 2013, but evidence from Japan (National Information Security Center), the United Kingdom (National Audit Office) and the United States (Bureau of Labour statistics) suggests that the current skills shortage confronting organisations in both the public and private sectors is expected to become more severe over the next decade. As a result, the UK Cabinet Office, Department for Business Innovation and Skills, National Cyber Security Programme and GCHQ have partnered to lead and support activities to increase cybersecurity skills at all levels of education.

Privacy professionals are in steady demand, prompted in part by the existence of a statutory basis in a number of countries, such as Canada, New Zealand, the United States, Germany and other EU countries. This development has been encouraged and supported by professional associations. For example, the steep growth in membership of the International Association of Privacy Professionals (IAPP) suggests broad market recognition for sound data governance practices (see Chapter 5, Figure 5.2). In its *Fortune 1000 Privacy Program Benchmarking Study*, the IAPP noted that while budgets vary widely across

Fortune 1000 companies, the average privacy budget is USD 2.4 million, 80% of which is spent internally on areas ranging from developing policies, training and certification to audits and data inventories.

Under the 2013 revisions to the OECD Privacy Guidelines, accountable organisations need to put in place multifaceted privacy management programmes, and be ready to demonstrate them on request from a privacy enforcement authority (OECD, 2013c, para. 15). As a result, the increase in privacy budgets and the number of privacy professionals is accompanied by an increased focus on training, education and certification activities. Looking ahead, with the growth of data-driven innovation and data analytics, data ethics is becoming a key element in protecting privacy (OECD, 2015a, forthcoming). Companies will need to adjust their perception of privacy from that of a compliance matter to be addressed by legal departments or a technical issue to be handled by IT departments, and instead implement ethical review processes and ensure that privacy-literate employees are designated throughout the organisation to identify potential issues.

Transparency reporting is increasing

Improved transparency is a long-standing OECD objective dating back to the original 1980 Privacy Guidelines, and was reaffirmed in the 2011 OECD Recommendation on Principles for Internet Policy Making (IPPs). Concerns about government access requests – particularly to data entrusted to providers of cloud computing services – predate the revelations by Edward Snowden in 2013 and are not limited to intelligence gathering. But those revelations have brought into sharper focus the need for transparency. Today, Internet and communications businesses are under increasing pressure to be open about the manner in which they address government access requests. One response has been the publication of transparency reports; since Google issued the first transparency report in 2009 the number has grown with over 30 companies now issuing public reports.

While governments have begun to acknowledge the need to improve transparency and are taking steps in that direction, more work is needed to increase public awareness about how governments access and use commercial data. Transparency reports are an important step forward in this regard, but their quality and comparability needs to be improved.

Governments adopt comprehensive National Cybersecurity Strategies

Cybersecurity has become a national policy priority addressed in an increasingly integrated manner, encompassing economic, educational, legal, technical and sovereignty-related issues. Today, many OECD countries have a national cybersecurity strategy: Australia (2009), Austria (2013), Belgium (2013), Estonia (2014), Hungary (2013), Italy (2013), Japan (2013), Norway (2012), Switzerland (2012), the Netherlands (2013) and Turkey (2013). Many non-OECD members have also recently adopted or revised their national cybersecurity strategies: India (2013), Kenya (2013), Latvia (2014), Qatar (2014), Russia (2013), Singapore (2013), South Africa (2013), Trinidad and Tobago (2012) and Uganda (2013). In 2014, the Chinese government organised a high-level working group on cybersecurity and Internet management, chaired by the country's president, with no less than six agencies and ministries providing input into cybersecurity policies. The group aims to improve co-operation among different agencies and ministries, while raising the profile of cybersecurity among leaders (Segal, 2014).

One notable trend is the increased role played by international and regional organisations in the development, implementation and evaluation of national cybersecurity strategies in Africa, Europe and the United States. For OECD countries, the forthcoming revised 2002

Security Guidelines call for national strategies to pursue the following complementary objectives: (i) create the conditions for all stakeholders to manage digital security risk to economic and social activities and foster trust and confidence in the digital environment; (ii) safeguard national and international security, and (iii) preserve human rights. Looking ahead, an important objective is to support SMEs and individuals to better manage digital security risks to their own activities.

In contrast, government responses to privacy risks are largely legal in nature

Governments have not begun to develop national privacy strategies to address privacy issues in a coordinated, holistic manner, as recommended in the OECD Privacy Guidelines. Such an approach would enable stakeholders to clarify the depth of protection to be afforded to individuals and the limitations society would be willing to accept to serve collective public interests. Instead, despite increased attention devoted to privacy risks, including at the political level, legislation remains a key response.

Almost all OECD countries (aside from Chile and Turkey) have privacy legislation. In 2014, reforms took place in Australia to enhance the powers of the Office of the Australian Information Commissioner and in Japan to establish the first independent data protection authority for government-issued identification numbers. Japan is also reviewing its Personal Data Protection Law to ensure its suitability for a world of "personal data utilisation". Proposed privacy legislation in the United States, however, remains a work in progress. Outside the OECD, China amended its consumer rights law to add provisions on the protection of personal information. Brazil recognised fundamental rights regarding personal data in the "Marco Civil da Internet". South Africa adopted a Protection of Personal Information Act in November 2013 and established an information regulator. Singapore's new law governing the collection and use of personal data by private sector organisations came into force in July 2014.

In terms of international developments, negotiations are still underway to complete a major overhaul of Europe's data protection framework. The Council of Europe is updating its primary data protection instrument, Convention 108. The Organization of American States is also working on a model law on personal data protection. Meanwhile, Asia-Pacific Economic Co-operation (APEC) has begun a review of its 2004 APEC Privacy Framework, with a view to possibly drawing on elements from the 2013 update to the OECD Privacy Guidelines.

Co-operation for privacy enforcement and security responses is growing

Since the adoption of an OECD recommendation in 2007, co-operation among privacy enforcement authorities has improved. In particular, the International Conference of Data Protection and Privacy Commissioners took steps to operationalise good practices from the Recommendation. The Global Privacy Enforcement Network (GPEN), composed of 51 data protection authorities across 39 jurisdictions, has conducted a cross-border survey of disclosure practices regarding the use of personal data by mobile apps, with a view to increasing public and commercial awareness of data protection rights and responsibilities, as well as to identify specific issues for future enforcement actions and initiatives. With respect to cybersecurity risk management, statistics from the Forum of Incident Response and Security Teams (FIRST) reveal a steady increase in interaction, information sharing, collaboration and co-operation among Computer Security Incident Response Teams (CSIRT), which should lead to improved incident response and better cybersecurity risk management.

Technology responses: Encryption and DNSSEC

On the technology front, Apple, Google and other companies have increased the default use of encryption in response to cyber-security and privacy risks. The popular messaging tool, WhatsApp, also announced its own end-to-end encryption. Apple has begun to explicitly market its privacy practices at the CEO level, emphasising security and privacy as fundamental design elements in Apple products and services. Such developments offer encouragement to policy makers who have long hoped that businesses would treat privacy protection as a business differentiator.

Another effort to reduce the risk of breach of confidentiality (data snooping) and various forms of deceptive attacks launched against Internet users via the Domain Name System (DNS) is the promotion of a security technology called Domain Name System Security Extensions (DNSSEC). The risk is that hostile attacks could replace a genuine DNS response with a crafted response, thereby misdirecting a user's traffic to unintended locations. Internet users are placed in the position of being forced to trust the responses they receive from their queries, yet having no certain means to assure themselves they are not being misled by a malicious third party. The response to this vulnerability is to add digital signatures to the DNS resource records. This enables them to confirm that the received DNS information is genuine. The widespread adoption of DNSSEC can significantly improve the robustness and reliability of the Internet. Successful experiences in Sweden also suggest that co-ordinated efforts by key stakeholders can have a positive impact on the adoption rate of this promising technology, while the Internet Corporation for Assigned Names and Numbers (ICANN) has determined that all new generic top-level domains (gTLDs) must support DNSSEC from inception.

There is a need to develop a security and privacy evidence base

The growing profile of privacy and security issues has not been matched by an equivalent acceleration in the development of metrics and other evidence needed by policy makers to evaluate the size and nature of the problem, and address the challenges. Many CSIRTs generate statistics on the number of incidents handled, and also collect data or potentially have access to data that could be used to generate statistics on other relevant phenomena. The OECD is currently working with the incident response community to develop guidance to help improve the quality and international comparability of statistics produced by CSIRTs (see OECD, 2015a, forthcoming). A number of other developments related to privacy and security risks are covered in Chapter 4, including the possible growth of cybersecurity risk insurance markets and the increasing role of the courts.

Competition policy issues have grown in importance both on the supply and demand sides

Several trends in the digital economy such as industry consolidation in the telecommunications sector; convergence between broadcasting, fixed and mobile networks; and the emerging field of zero-rating have the potential to affect competition. In addition, some observers argue that the sharing economy might also create additional competition issues, since different rules may apply to individuals offering private services and industries offering professional services (Chapter 4). The following section discusses competition issues arising from convergence and industry consolidation. Zero-rating is

discussed in the section on net neutrality, while potential emergent competition policy issues linked to the sharing economy and collective consumption are highlighted in Chapter 3.

Recent years have seen a trend towards industry consolidation, especially in mobile communications

Consolidation in the communications and media industry is not a new phenomenon, but has increased in recent years, especially in mobile markets. Since 2010, 19 mobile mergers took place in OECD countries compared to fewer new entries for the same period (Chapter 4, Tables 4.5 and 4.6). Consolidation between fixed and mobile operators is another trend mirroring fixed-mobile convergence, discussed below.

In most countries, infrastructure competition has emerged between traditional public switched telephone networks (which later evolved to DSL) and cable networks (upgraded to provide Internet access services). There is, however, very limited geographical competition between the same networks in the same area. In some of these markets there may be additional players due to new private sector entry or municipal networks. Some observers also point to the potential for competition from mobile operators. While mobile networks certainly provide strong competition for traditional services, such as telephony, they are still regarded as being largely complementary to fixed networks. The degree of competition in many markets thus depends on the number of ISPs in an area.

Policy makers have addressed competition issues in fixed markets through measures such as unbundling and functional or structural separation.

Policy makers have addressed challenges to competition in fixed markets through the use of regulatory tools such as unbundling of local facilities, or measures such as functional or structural separation. In some cases, countries have opted for public investment in networks, usually linked with open access requirements.

For mobile markets, policy makers may need to influence the number of players

In mobile markets, all OECD countries have at least three mobile network operators (MNOs) and the majority have four. In addition, Mobile Virtual Network Operators (MVNOs) exert competitive pressure on established providers. However, a recent spate of mergers has raised concerns over the level of effective competition. For this reason, the OECD examined the implications of an increase or decrease in the number of players in mobile markets (OECD, 2014e). While it would be preferable for market forces to determine the number of players, the scarcity of spectrum resources and the need for significant network deployment investments suggest that policy makers may have to take a stance and determine, or at least influence, the number of players in mobile markets.

Recent years have witnessed the growing use of network sharing between MNOs in OECD countries. This can decrease costs to a single operator of network deployment and extend coverage to locations especially in rural areas which might otherwise be underserved. However, network sharing can affect competition through unilateral effects, potential co-ordination and information sharing. For example, in a market with four MNOs, two sharing agreements may facilitate co-ordination and effectively result in a wholesale duopoly. Telecom regulators and competition authorities need to be vigilant, monitor sharing agreements and assess whether MVNOs exert sufficient pressure on MNOs.

There is a need to monitor the effects of convergence and ensure technological neutral regulation

Competition in communication markets is also affected by increasing convergence. During recent years, trends in convergence have been observed mainly between fixed and mobile networks (i.e. joint provision of fixed and mobile communication services), and between telecommunications and television service offers, with market players tending to offer triple-play services (voice, video and broadband). More recently, convergence between telecommunications offers and over-the-top (OTT) services from application-based companies (e.g. Facebook, Netflix, Spotify) have begun to pose new challenges to current regulatory frameworks.

Convergence, whether between fixed and mobile, telecoms and broadcasting or telecoms and OTT, inevitably leads to service bundles. These enable consumers to benefit from integrated offers, but may lead to the exclusion of other operators unable to offer the full range of services. This situation calls for telecom regulators and competition authorities to advance regulatory reform, with a view to applying the same rules if similar services are being provided, thus guaranteeing technological neutrality. Since the principle of technological neutrality would suggest that similar services should operate under the same rules and conditions, its implementation poses significant challenges to most current regulatory frameworks, as the Internet and traditional television broadcasting services stem from radically different environments and OTT services are typically not included. In cases where bundling incorporates goods that have an important level of market power (e.g. premium television content) and bundles could become a serious source of competition concern, regulators have applied ex-ante regulation. For example, in the United Kingdom, the Office of Communications (Ofcom) imposed a wholesale obligation on the leading pay television provider, Sky, to offer its wholesale sports channels at regulated prices to third-party providers.

Network neutrality is gaining momentum

Network neutrality – or the issue around treating Internet traffic equally versus prioritising traffic – is complex and potentially involves two main aspects. One is the ability of users to access content and services, which could be affected by differentiation through pricing, quality of service or blocking of access (e.g. blocking VoIP services). The second concerns the commercial arrangements that enable traffic exchange between networks (i.e. peering and transit). Both issues relate to the relationship between users and their Internet service provider (ISP), whom they pay for access to the Internet, as well as to the terms and conditions by which networks agree to exchange traffic.

The network neutrality debate is becoming increasingly heated in Europe and elsewhere. In the United States, most policy discussions on network neutrality have so far focused on last-mile issues (e.g. the FCC's 2014 Open Internet Notice of Proposed Rule Making).

Network neutrality in Internet access service: Countries take different policy approaches

If ISPs change access terms to some content, services or networks, including quality, this might create different limitations for users of the network, and affect the capacity of users on other networks to communicate with them. Any unreasonable limitation of such

communication could lead to different quality levels for alternative network paths, not all of which treat traffic in the same manner. Apart from a potential "fragmentation" effect, limitations on access could affect the Internet as a platform for innovation.

There is no unified approach towards network neutrality, and policy frameworks vary from country to country. A number of OECD countries have introduced legislation to ensure network neutrality and have prohibited blocking and unreasonable discrimination of services. In 2010, Chile was the first OECD country to legislate in favour of network neutrality, followed by the Netherlands (2011) and Slovenia (2012). Brazil's Congress passed the bill "Marco Civil da Internet" (Internet's Civil Framework Act), which makes network neutrality the rule on the Internet, even though the implementing regulations still need to be developed by Presidential Decree. For its part, Italy is following a similar process with a public consultation launched in October 2014.

Other countries established provisions on network neutrality jointly with the industry, such as the Norwegian model of co-regulation, or Korea's "Guidelines on Net Neutrality and Internet Traffic Management", published in December 2011. The United Kingdom favours self-regulation, relying on transparency and competition to provide consumers with sufficient information to make informed decisions. In Canada, the Canadian Radio-television and Telecommunications Commission (CRTC) released a network neutrality framework to guide the telecommunications industry in the use of acceptable traffic management practices.

While most European countries have not, at least officially, adopted a formal position on network neutrality, the European Commission has voiced on many occasions its support for this principle, linking it to the ability for users to "access and distribute information or run applications and services of their choice". Moreover, the European Parliament adopted its position on the proposal on 3 April 2014 and the Council gave a negotiation mandate to the Latvian Presidency on 4 March 2015. Dialogues between the institutions started in March 2015. In the United States, the FCC released on 12 March 2015, the Order "Protecting and Promoting the Open Internet", which established three "bright line" rules applicable to both fixed and mobile broadband Internet access service, prohibiting blocking, throttling and paid prioritisation (FCC, 2015).

Network neutrality and traffic exchange between networks: Efficient traffic exchange markets have developed in competitive markets without the need for regulation

The Internet's model for traffic exchange works extremely well and has been a major ingredient in enabling it to scale so rapidly and pervasively. At its heart, every user of the Internet pays for his or her own access. In turn, their ISP undertakes to provide connectivity to the rest of the Internet either through peering (direct interconnection) or transit. The purchase of transit enables an ISP to reach all networks around the world. Peering enables two ISPs to directly exchange traffic, bypassing the transit providers. The use of peering allows ISPs to reduce their costs, as they do not need to purchase transit for that traffic. To save costs, ISPs establish or make use of Internet Exchange Points (IXPs), where they can peer with multiple networks at the same time. Meanwhile, the purchase of transit enables them to economically reach networks where they do not have facilities.

A recent survey found that 99.5% of peering agreements are realised on a handshake basis, with no written contract and no exchange of payment (Weller and Woodcock, 2013). Moreover, multilateral agreements exist on many IXPs, enabling hundreds of networks

to exchange traffic for free with any network that joins the agreement. Parties to these agreements include Internet backbone, access and content distribution networks, as well as universities, non-governmental organisations, branches of government, businesses and enterprises. Under the current voluntary system, operators invest in and expand their network to reach new peers, and co-operate with other networks to establish new IXPs in areas where there are none, because they save on transit costs.

The Internet model of traffic exchange operates in a highly competitive environment, largely without regulation or central organisation, and has enabled the development of an efficient market for connectivity based on voluntary contractual agreements. It has produced lower prices, promoted efficiency and innovation, and attracted the necessary investment to keep pace with demand. Nonetheless, where commercial negotiations do take place and in the absence of sufficient competition, one player may leverage their position to extract higher rents from others. In such instances, ISPs have the option to bypass each other. This is a key reason for the success of the Internet in competitive markets.

In the absence of sufficient retail competition a key issue is whether consumers are receiving the service they pay for. Resolving this question can be a challenge given that the Internet is a network of networks with each network responsible for delivering connectivity and traffic to its own customers. Nevertheless, computer scientists are developing tools to help inform stakeholders about issues such as the existence of online congestion. The preliminary report of a joint project undertaken in 2014 by the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory and the Centre for Applied Internet Data Analysis (CAIDA/UCSD) did not reveal widespread congestion among ISPs in the United States. Similar projects in other parts of the world would contribute greatly to informing policy makers and regulators.

Could zero-rating be considered a violation of net neutrality?

One emerging practice that features high in net neutrality discussions is zero-rating. The ICT industry applies the term zero-rating when some of the traffic sent and received by consumers over the Internet is unmetered.

Zero-rating can take a number of forms. For example, zero rating can be applied by ISPs to their own content or to that of pre-selected partners such as video or music services. When customers access this content, it does not count against the data cap of their broadband plans. Alternatively, if the customer of another ISP accesses that content over the Internet, they would pay a subscription charge to the service and their ISP would count these data against their allowance.

Another example of zero-rating involves a large difference in price between on-net and off-net traffic (i.e. either traffic supplied by the ISP itself or its unpaid peers, or content obtained via an IP transit network). These kinds of arrangements tend to be popular in countries that have broadband offers with low bit caps in monthly allocations. In Australia, lower bit caps due to high IP transit rates resulted in the use of zero-rating as a competitive tool. Smaller ISPs and content providers, such as radio stations, directly exchanged traffic and ISPs passed on the lower costs to their customers through zero-rating. This enabled consumers with low bit caps to stream audio from these stations – an option that would not have been attractive at metered pricing. Had regulation required these ISPs to treat this

traffic like that of any other content provider not directly interconnecting with them, it would have distorted the incentives for peering and transit.

An additional form of zero-rating occurs in developing countries where the practice is increasing. Popular Internet services, such as Facebook, WhatsApp, Twitter, Wikipedia and Google, have been partnering with telecommunication operators to offer zero-rated access to these services. However, it should be noted that these products do not provide access to the Internet, but only to a limited number of sites. The goal is to use these sites as a teaser to encourage wider Internet use among consumers. This approach can also help achieve social objectives by including unmetered access to websites such as Wikipedia or health and government information.

To date, regulators have taken different positions on zero rating. In Canada, Chile, Norway, the Netherlands and Slovenia, regulators have made explicit statements against zero-rating as anti-competitive or contravening national net neutrality regulation. In other countries the practice exists among various operators in different forms and regulators have not taken action.

While zero-rating can clearly be pro-competitive and may have beneficial aspects for economic and social development, regulators need to be vigilant. Previous experiences in OECD countries have shown that zero-rating becomes less of an issue with increased competition and higher or unlimited data allowances. Indeed, it can be a tool to increase competition. Prohibiting zero-rating may have implications for a market where there is lower competition for transit and may reduce the effectiveness of peering. Nevertheless, in any market with limited competition for access, zero-rating can affect competition among content providers. For example, any situation where a dominant content provider is zero-rated and its competitors are not (and the provider's position enables them to opt for paid-peering rather than peering) may impede new or innovative firms from entering the market. Likewise, a situation where an ISP offers a high-volume service while setting a low data cap could also stifle competition.

1.8 Internet governance and policy outlook

The digital economy has far-reaching impacts across sectors. Accordingly, stakeholders are paying increasing attention to the issue of Internet governance at national and international levels, with many governments ranking the issue high on agendas (e.g. see OECD, 2011). In 2014, the international summit NETmundial in São Paulo produced a global multi-stakeholder statement of generally accepted principles and a further roadmap for Internet governance (NETmundial, 2014).

A number of distinct but interrelated processes could further shape the Internet governance landscape over the next two years. Firstly, the Internet community is developing a proposal to transition oversight of the Internet's technical resources from the United States government to the global multi-stakeholder community. The private, non-profit Internet Corporation for Assigned Names and Numbers (ICANN) has convened this process at the request of the United States. Secondly, developments in the network neutrality discussion are expected with a number of states, such as Brazil, the European Union and the United States, to review or develop net neutrality regulation and discuss ways to deal with zero-rating in this context. Lastly, the United Nations is due to publish the Sustainable Developments Goals as part of the post-2015 development agenda. These are likely to make

reference to ICTs and their role in promoting development, which has focused interest on the potential economic and social benefits of an open Internet.

The IANA stewardship transition

Internet governance is – as the Internet itself – spread out, with a number of different organisations handling different aspects. Coordination of the domain name system and Internet addressing has been handled largely by the private, non-profit Internet Corporation for Assigned Names and Numbers (ICANN), since its creation in 1998.

ICANN coordinates bottom-up policy development processes by stakeholders of the domain name system. ICANN also performs the narrower set of technical functions known as the Internet Assigned Numbers Authority (IANA) functions under contract with the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) since 2000.

Under its role as the "IANA functions operator", ICANN allocates blocks of IP addresses and network numbers to Regional Internet Number Registries (RIRs) that serve different geographical regions. ICANN also administers protocol parameter registries that involves maintaining many of the codes and numbers used in Internet protocols. And importantly, ICANN performs certain administrative duties associated with the root zone file and root zone WHOIS, which includes reviewing change requests from top-level domain name operators. ICANN also provides "other services" related to the administration of the .int and .arpa top level domains.

In March 2014, NTIA asked ICANN to convene a multi-stakeholder process to develop a proposal to transition the US stewardship role over the IANA functions to the global multistakeholder community. Prior to this transition, NTIA specified that the proposal must adhere to specific conditions. Namely, the proposal must:

- Support and enhance the bottom-up, multistakeholder model;
- Maintain the security, stability, and resiliency of the domain name system;
- Meet the needs and expectations of the global customers and partners of the IANA services;
- Maintain the openness of the Internet.

NTIA also stated that it would not accept a proposal that replaces its role with a government-led or an inter-governmental organization solution.

In response to this task, stakeholders organized two parallel processes. The first focuses on the specifics of the IANA functions and developing a transition proposal and the second focuses on enhancing ICANN accountability to the global community of Internet stakeholders. For the first track, an IANA Stewardship Transition Coordination Group (ICG) was established in July 2014. The ICG called for the three communities of interest aligned to the three primary IANA functions – domain names, numbering resources, and protocol parameters – to each develop a proposal related to that function.

The Internet Engineering Task Force (IETF) for the protocol parameters function and the Regional Internet Registries (RIRs) for the Internet numbers related function submitted their proposals to the ICG in January 2015. An ICANN Cross Community Working Group (CWG-Stewardship) on naming related functions was at the time of writing continuing to develop their proposal. Once the naming proposal is finalized, the ICG will review

and compile them into one consolidated transition proposal. Once fully vetted by the broader community, the ICG will submit a final proposal to ICANN who will then transmit it to NTIA.

The second process is addressing how to enhance ICANN's accountability to the global Internet community in the absence of the contractual relationship with the US National Telecommunications and Information Administration (NTIA). An ICANN Cross Community Working Group (CCWG-Accountability) was formed to look at ICANN accountability enhancements and established two work streams: 1) identify accountability measures that need to be in place before the transition, and 2) address accountability measures that should be adopted and implemented by ICANN in the longer term. Once the CCWG-Accountability has completed its work stream 1 output, ICANN will transmit it to NTIA.

NTIA has not set a deadline for this transition. While the base period of the IANA functions contract expires in September 2015, NTIA has the flexibility to extend the contract if the community needs more time.

Renewal of the IGF mandate and the Sustainable Development Goals

In December 2015, the mandate of the Internet Governance Forum (IGF) will come up for renewal. In the same month, the high-level meeting for the overall review by the General Assembly of the implementation of the outcomes of the World Summit on the Information Society (WSIS) will take place. The WSIS conferences in 2003 and 2005 and their outcomes played a key role in increasing the visibility of Internet governance on the international agenda. The forthcoming high-level meeting will review progress toward objectives established in the outcome documents, in line with UN General Assembly resolutions 60/252 and 68/302. September 2015 will also see the launch of the post-2015 UN development agenda with a new set of targets designed to replace and build on the Millennium Development Goals (MDGs). The Internet and ICTs appear in the MDGs only in the context of a "global partnership for development", as a sub-target of Goal 8.[45] The new targets, the Sustainable Development Goals (SDGs), place a stronger emphasis on increased access to ICTs as a means to create an inclusive and global digital economy (UN, 2014). According to the draft document, Goal 9c underlines the need to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020".[46] Despite their inclusion in the SDGs, however, some experts in the Internet governance and development community believe that ICTs should be developed as a crosscutting, horizontal goal. The present formulation focuses primarily on access to ICTs, rather than on the economic and social benefits achievable through the adoption and use of ICTs. These issues are likely to be discussed during the upcoming Internet Governance Forum (IGF) to be held in November in Brazil which, for the first time, aims at producing a declaration

The openness of the Internet

Another issue gaining attention in the area of governance and policy is preservation of the open Internet. Internet openness can be viewed as a spectrum, ranging from completely open to completely closed. From a policy perspective, neither extreme is optimal. On the one hand, boundaries and limitations may be required for economic or social purposes;

on the other, closed systems are economically and socially costly because they reduce opportunities for trade gains, and social and civic inclusiveness, exchange and enrichment. The objective for governments is to ascertain the optimal position on the Internet openness spectrum. Assessing the full social implications of imposing limits may well be complex and requires careful examination of the dynamics at play – and the potential consequences. In addition, national choices have international ramifications, as restrictions on one national system may decrease the opportunities available to other countries to reap benefits from trade and knowledge flows.

The 2008 OECD Ministerial Meeting on the Future of the Internet Economy and the 2011 OECD Recommendation of the Council on Principles for Internet Policy Making (IPPs) highlighted the link between a distributed interconnected architecture designed to be open "by default" and the Internet's key role in catalysing economic growth and social well-being. Indeed, the digital economy has benefitted from numerous innovations resulting from businesses, citizens and governments serendipitously innovating and developing applications and service across this open platform. But in recent years, a number of policy and governance trends have arisen that may impact, directly or indirectly, the economic and social benefits delivered by the open and decentralised nature of the Internet and by the free flow of trans-border data. Such trends include data and content localisation requirements and new challenges in the area of net neutrality.

Ongoing OECD work aims to categorise different dimensions of the open Internet and to analyse the effects of an open Internet and the risks and consequences of fragmentation. The ultimate goal is to provide a framework accompanied by analysis and evidence that allows policy makers to make more informed decisions. The framework will have to acknowledge the balance between harnessing the Internet for economic growth and permitting sources of friction that address public policy goals. It must also recognise that this balance can differ between countries driven by different societal values.

The third OECD Digital Economy Ministerial Meeting

The benefits of and risks to an open Internet will be addressed at the forthcoming third OECD Ministerial Meeting on "The Digital Economy: Innovation, Growth and Social Prosperity" in 2016. Ministers and other high-level representatives of the global Internet community will take a holistic look at recent developments in the digital economy and discuss ways to maximise the economic and social benefits while mitigating risks. Discussions will be structured around four main themes:

- *The open Internet as a platform for growth* will analyse the benefits of openness and the concomitant risks and consequences of fragmentation, as well as innovations on the demand side enabled by ICTs and the conception of the Internet as an open platform.
- *Building global connectivity* will focus on issues related to the convergence of networks and services and the Internet of Things (Chapter 6).
- *Trust* will address the importance of consumer trust for market growth and explore digital risk management.
- *Jobs and skills* will focus on ways for policy to promote labour market transformation and for digital skills to maximise the benefits of the digital economy.

Box 1.3. **Brazil: Internet governance and policy outlook**

Promoting multistakeholderism in policy making

The Internet's complexity, global reach and constant evolution require timely, scalable and innovation-enabling policies. As the Internet becomes more critical to economies and societies and affects an increasing number of interests, the decision making process around legal and political frameworks becomes more complex, and sometimes, contentious. Experience has shown that multi-stakeholder processes can provide the flexibility and global scalability required to address Internet policy challenges.

The Brazilian experience in promoting a multi-stakeholder approach to Internet policy making has received international acclaim and inspired the organisation of the 2014 NETMundial conference in São Paulo to discuss principles and a roadmap for Internet governance. Brazil's success in implementing a participative and cross-sectoral framework for Internet policy making is the result of an innovative framework embodied by the Internet Steering Committee (CGI.br).

The CGI.br is responsible for establishing strategic directives related to the use and development of the Internet in Brazil, as well as guidelines for the implementation of Domain Name registration, allocation of IP (Internet Protocol) and administration of the Top Level Domain (TLD) ".br". The CGI.br follows a multi-stakeholder model and consists of 21 members, including nine representatives from federal government, four from the business sector, four from civil society, three from the scientific and technical community, and a renowned Internet expert.

Typically, this steering committee meets once per month and publishes its agendas and minutes online. A group of multi-sectoral consulting chambers support the steering committee by discussing specific topics in depth, such as changes to the technical structure of port 25 which resulted in a drop in online spam.

The Internet Steering Committee's decisions are supported and executed by the Centre for Information and Coordination (NIC.br), established in 2005 as a non-profit organization. NIC.br has a mandate to register and maintain .br domain names, respond to and treat security incidents, promote studies, measure indicators, and recommend procedures and standards, among other operational assignments. CGI.br and ANATEL also counsel the President of the Republic on implementing exceptions to the network neutrality principle.

Marco Civil

The Brazilian Internet Bill of Rights (Bill of Law no. 12.965/2014), or "Marco Civil" in Portuguese, consolidates rights, duties and principles for the use and development of the Internet in Brazil. Its importance lies not only in its principles, but also in the manner in which its was drafted. The law was a joint initiative of the Ministry of Justice in partnership with the Centre for Technology and Society at the Getulio Vargas Foundation (FGV). It was based on an open and collaborative consultation process, implemented at an unprecedented scale across the country.

The first phase of the consultation registered more than 800 proposals, comments and messages of support from various sectors of Brazilian society concerning key topics for debate about Internet use. The second phase saw the formulation and submission of a draft bill for comments and public debate.

The initiative gained national and international attention for its multi-stakeholder approach and for the development of a regulatory framework defining key principles for a user-centric open Internet. Public consultation is currently underway on further regulations for certain provisions of the law. The main issues under discussion relate to network neutrality, protection of personal data and data retention requirements for providers.

Notes

1. See, for example, the OECD Principles of Internet Policy Making (OECD, 2011) and the NetMundial Multistakeholder Statement (NETmundial, 2014).
2. These include: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States (OECD countries), and Egypt, Latvia, Lithuania and Russian Federation (non-OECD countries).
3. These include: Australia, Belgium, Canada, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Turkey and the United Kingdom (OECD countries), and Egypt, Latvia and Lithuania (non-OECD countries).
4. See *www.evm.dk/~/media/files/2014/web-185953-indhold-v-kstrapport-for-digitaliering.ashx*.
5. See *www.digitale-agenda.de/DA/Navigation/DE/Home/home.html*.
6. See *www.agid.gov.it/sites/default/files/documenti_indirizzo/strategia_italiana_agenda_digitale_0.pdf*.
7. See *http://embamex.sre.gob.mx/italia/images/pdf/national%20digital%20strategy.pdf*.
8. See *www.bilgitoplumu.gov.tr/en/2014-2018-information-society-strategy/*.
9. See *http://apo.org.au/research/advancing-australia-digital-economy-update-national-digital-economy-strategy*.
10. See *www.france-universite-numerique.fr/IMG/pdf/feuille_de_route_du_gouvernement_sur_le_numerique.pdf*.
11. See *http://japan.kantei.go.jp/policy/it/index_e.html*.
12. See *www.gov.uk/government/publications/information-economy-strategy*.
13. In 2012, the Digital Agenda for Europe underwent a review that identified areas where more focused action is needed to create growth and jobs in Europe. As a result of the review it added 31 actions.
14. See *www.bmg.gv.at/home/Schwerpunkte/E_Health_Elga/E_Health_in_Oesterreich/*.
15. See *www.efit21.at/en/about-efit21*.
16. See *www.sozialministerium.at/cms/site/attachments/7/7/8/CH2477/CMS1332494355998/nap_behinderung-web_2013-01-30_eng.pdf*.
17. See *www.regeringen.se/sb/d/108/a/181801*.
18. See *www.government.se/sb/d/574/a/134980*.
19. See *www.regeringen.se/sb/d/15700/a/206004*.
20. See *www.government.se/sb/d/574/a/152926*.
21. See *www.government.se/download/70f489cb.pdf?major=1&minor=181914&cn=attachmentPublDuplicator_0_attachment*.
22. See *www.regeringen.se/sb/d/2498*.
23. See *www.government.se/sb/d/2025/a/202558*.
24. See *www.ic.gc.ca/eic/site/028.nsf/eng/home*.
25. This investment comes on top of CAD 14 billion already allocated over the next ten years for a new Building Canada Fund, to which broadband and connectivity projects are eligible. The Building Canada Fund consists of a National Infrastructure Component (CAD 4 billion), which will support projects of national significance, and Provincial-Territorial Infrastructure Component (PTIC) (CAD 10 billion) for projects of national, local or regional significance.
26. See *www.mpo.cz/zprava149132.html*.
27. See *www.portugaldigital.pt*.
28. See *www.gouvernement.lu/4103941/dossier-de-presse-digital-letzebuerg-20141017.pdf*.
29. See *www.fcc.gov/national-broadband-plan*.
30. See *www.regjeringen.no/nb/dep/kmd/dok/regpubl/stmeld/2012-2013/meld-st-23-20122013-2.html?id=728993*.

31. See *www.msip.go.kr/cms/www/open/go30/info/info_1/info_11/__icsFiles/afieldfile/2014/11/24/%EC%A0%9C5%EC%B0%A8%EA%B5%AD%EA%B0%80%EC%A0%95%EB%B3%B4%ED%99%94%EA%B8%B0%EB%B3%B8%EA%B3%84%ED%9A%8D%282013~2017%29.pdf*.
32. See *www.mg.gov.pl/node/20481*.
33. See *http://ec.europa.eu/digital-agenda/en/our-goals/pillar-ii-interoperability-standards*.
34. See *www.mcit.gov.eg/Upcont/Documents/MCITstrategy2013_en.pdf*.
35. See *www.nih.gov.hu/download.php?docID=25413*.
36. See *http://e-estonia.com/nordicday/digitalagendas/*.
37. See *www.mizs.gov.si/si/medijsko_sredisce/novica/article//8881/a6a53e02d821d14c3dbcc42bea5b9b35*.
38. *www.dcenr.gov.ie/NR/rdonlyres/54AF1E6E-1A0D-413F-8CEB-2442C03E09BD/0/NationalDigitalStrategyforIreland.pdf*.
39. See *www.agendadigital.gob.es/Paginas/Index.aspx*.
40. The definition of Telework in this Goal includes Telework of a formal, scheduled, contracted nature.
41. These speeds are reached under very specific conditions, in particular with regards to the number of users in a cell, distance to a tower and so forth.
42. For more information, see *http://press.spotify.com/fr/information/*.
43. For more information, see *www.youtube.com/yt/press/statistics.html*.
44. See OECD based on Instantwatcher (*http://instantwatcher.com/titles/all*).
45. Target 8F states: "in cooperation with the private sector, make available the benefits of new technologies, especially information and communication technologies".
46. In addition, ICTs are mentioned briefly in Target 5b, on enhancing the use of enabling technologies, in particular ICT, to promote women's empowerment (goal 5 "Achieve gender equality and empower all women and girls").

References

Androsoff, R. and A. Mickoleit (2015), "Measuring government impact in a social media world", *OECD Insights* blog, 18 February 2015, *http://oecdinsights.org/2015/02/18/measuring-government-impact-in-a-social-media-world* (accessed 15 April 2015).

Apple (2013), "iTunes store sets new record with 25 billion songs sold", *Apple Press Info*, 6 February 2013, Cupertino, *www.apple.com/pr/library/2013/02/06iTunes-Store-Sets-New-Record-with-25-Billion-Songs-Sold.html* (accessed 15 April 2015).

Belleflamme, P. and T. Lambert (2014), "Crowdfunding: some empirical findings and microeconomic underpinnings", prepared for a special issue of the *Revue Bancaire et Financière*, July 2014.

Brazil (2010), Decreto N° 7.175 de 12 de Maio de 2010, *Presidência da República*, *www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7175.htm* (accessed 29 April 2015).

Capgemini (2014), "Internet of Things = Internet of trust", *Capping IT Off* blog, 19 September 2014, *www.capgemini.com/blog/capping-it-off/2014/09/internet-of-things-internet-of-trust*.

CIGI (2014), *CIGI-Ipsos Global Survey on Internet Security and Trust*, Centre for International Governance Innovation, Waterloo, ON, *www.cigionline.org/internet-survey* (accessed 15 April 2015).

EC (2015), *Special Eurobarometer 423: Cyber Security Report*, European Commission, Brussels, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf*.

EC (2010), *A Digital Agenda for Europe*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010)245 final, European Commission, Brussels, *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN* (accessed 21 November 2014).

Economist (2014), "Banking without banks", *The Economist*, 1 March 2014, *www.economist.com/news/finance-and-economics/21597932-offering-both-borrowers-and-lenders-better-deal-websites-put-two*, (accessed 22 October 2014).

Economist (2013), "Taking a bite out of Apple", *The Economist*, 12 September 2013, *www.economist.com/news/business/21586344-xiaomi-often-described-chinas-answer-apple-actually-quite-different-taking-bite-out*, (accessed 14 October 2014).

FCC (2015), *Report and Order on Remand, Declaratory Ruling, and Order, in the Matter of Protecting and Promoting the Open Internet*, 12 March 2015, Federal Communications Commission, Washington DC, *http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0403/FCC-15-24A1.pdf*.

Flurry (2014), "Mobile to television", *Flurry Insights*, *www.flurry.com/blog/flurry-insights/mobile-television-we-interrupt-broadcast-again#.VG-PgPnF9HX* (accessed 21 November 2014).

Fox, S. and M. Duggan (2013), "Tracking for health", *Pew Research Center*, 28 January 2013, Pew Research Center, Washington DC, *www.pewinternet.org/2013/01/28/tracking-for-health/*.

GSMA (2013), *Socio-economic Impact of mHealth: An Assessment Report for the European Union*, London, Groupe Speciale Mobile Association and PricewaterhouseCoopers, *www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic_impact-of-mHealth_EU_14062013V2.pdf*.

GSMA and PwC (2012), *Touching Lives through Mobile Health: Assessment of the Global Market Opportunity*, London, Groupe Speciale Mobile Association and PricewaterhouseCoopers, *www.gsma.com/connectedliving/gsma-pwc-report-touching-lives-through-mobile-health-assessment-of-the-global-market-opportunity/* (accessed 21 November 2014).

IAPP (2014), "Benchmarking privacy management and investments of the Fortune 1000", *International Association of Privacy Professionals* (IAPP) website, *https://privacyassociation.org/resources/article/benchmarking-privacy-management-and-investments-of-the-fortune-1000-2/* (accessed 15 April 2015).

IDATE (2014), *Digiworld Yearbook 2014*, IDATE, Montpellier, France.

Lunden, I. (2015), "Target Says credit card data breach cost it $162M in 2013-14", *TechCrunch*, 25 February 2015, *http://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/* (accessed 15 April 2015).

Massolution (2013), *2013CF: The Crowdfunding Industry Report*, Massolution, Los Angeles, CA, *www.crowdsourcing.org/editorial/2013cf-the-crowdfunding-industry-report/25107* (accessed 13 April 2015).

NETmundial (2014), *NETmundial Multistakeholder Statement*, *http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf* (accessed 4 April 2015).

OECD (2015a), *Data Driven Innovation for Growth and Well-Being*, OECD Publishing, Paris, forthcoming.

OECD (2015b), *Improving the International Comparability of Statistics Produced by Computer Security Incident Response Team*, OECD Publishing, Paris, forthcoming.

OECD (2015c), *Trust in a Data-Driven Economy: Data and Analytics: Prospects for Growth and Well-being*, OECD, Paris.

OECD (2014a), *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris.

OECD (2014b), "Access network speed tests", *OECD Digital Economy Papers*, No. 237, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5jz2m5mr66f5-en*.

OECD (2014c), "Cloud computing: The concept, impacts and the role of government policy", *OECD Digital Economy Papers*, No. 240, OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/5jxzf4lcc7f5-en*.

OECD (2014d), "Government use of social media. A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Maker", *OECD Public Governance Working Papers No. 26*, OECD, Paris, *http://dx.doi.org/10.1787/5jxrcmghmk0s-en*.

OECD (2014e), "Wireless market structures and network sharing", *OECD Digital Economy Papers*, No. 243, OECD Publishing, Paris, DOI: 10.1787/20716826.

OECD (2014f), *Recommendation of the Council on Digital Government Strategies*, OECD Publishing, Paris, *www.oecd.org/gov/public-innovation/recommendation-on-digital-government-strategies.htm*.

OECD (2013a), *The Internet Economy on the Rise: Progress Since the Seoul Declaration*, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/9789264201545-en* (accessed 13 April 2015).

OECD (2013b), *Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges*, OECD Health Policy Studies, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/9789264193505-en*.

OECD (2013c), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, *http://oe.cd/privacy*.

OECD (2012), *OECD Internet Economy Outlook 2012*, OECD Publishing, Paris, *www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm*.

OECD (2011), *Recommendation on Principles for Internet Policy Making*, OECD, Paris, *www.oecd.org/sti/ieconomy/49258588.pdf*.

OECD (2008), *Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information*, OECD Publishing, Paris, *www.oecd.org/sti/oecdrecommendationonpublicsectorinformationpsi.htm*.

Ofcom (2014), *Promoting Investment and Innovation in the Internet of Things*, Ofcom, London, *http://stakeholders.ofcom.org.uk/consultations/iot/* (accessed 15 April 2015).

Our Mobile Planet (2013), *Our Mobile Planet – Full Data Sets and Country Reports*, Google, Mountain View, CA, *http://think.withgoogle.com/mobileplanet/en-gb/downloads/* (accessed 13 April 2015).

Pew Research Center (2014), *Few Feel that the Government or Advertisers can be Trusted*, Pew Research Center, Washington DC, *www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/* (accessed 13 April 2015).

PricewaterhouseCoopers (2015), MoneyTree Survey Report, February, London Pwc.

PwC (2014a), *Retail Banking 2020: Evolution or Revolution?* PricewaterhouseCoopers, London, *www.pwc.com/et_EE/EE/publications/assets/pub/pwc-retail-banking-2020-evolution-or-revolution.pdf*.

PwC (2014b), *Internet Advertising – Key Insights at a Glance*, PricewaterhouseCoopers, London, *www.pwc.com/gx/en/global-entertainment-media-outlook/segment-insights/internet-advertising.jhtml* (accessed 20 November 2014).

research2guidance (2014), *mHealth App Developer Economics 2014: The State of the Art of mHealth App Publishing*, research2guidance, Berlin, *http://research2guidance.com/r2g/research2guidance-mHealth-App-Developer-Economics-2014.pdf*.

Segal, A. (2014), "China's new small leading group on cybersecurity and Internet management", *Forbes*, 27 February 2014, *www.forbes.com/sites/adamsegal/2014/02/27/chinas-new-small-leading-group-on-cybersecurity-and-internet-management/* (accessed 15 April 2015).

Simula, H. and T. Ahola (2014), "A network perspective on idea and innovation crowdsourcing in industrial firms, *Industrial Marketing Management*, No. 43, pp. 400-408, *http://dx.doi.org/10.1016/j.indmarman.2013.12.008*.

TechCrunch (2014), "Travel, retail and media are 3 industries taking over the App Store", *TechCrunch*, 18 October 2014, *http://techcrunch.com/2014/10/18/travel-retail-and-media-are-3-industries-taking-over-the-app-store/* (accessed 22 October 2014).

UN (2014), *Open Working Proposal for Sustainable Development Goals*, Full report of the Open Working Group of the General Assembly on Sustainable Development Goals, document A/68/970, United Nations, New York, *https://sustainabledevelopment.un.org/content/documents/1579SDGs%20Proposal.pdf*.

Weller, D. and B. Woodcock (2013), "Internet traffic exchange: Market developments and policy challenges", *OECD Digital Economy Papers*, No. 207, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5k918gpt130q-en*

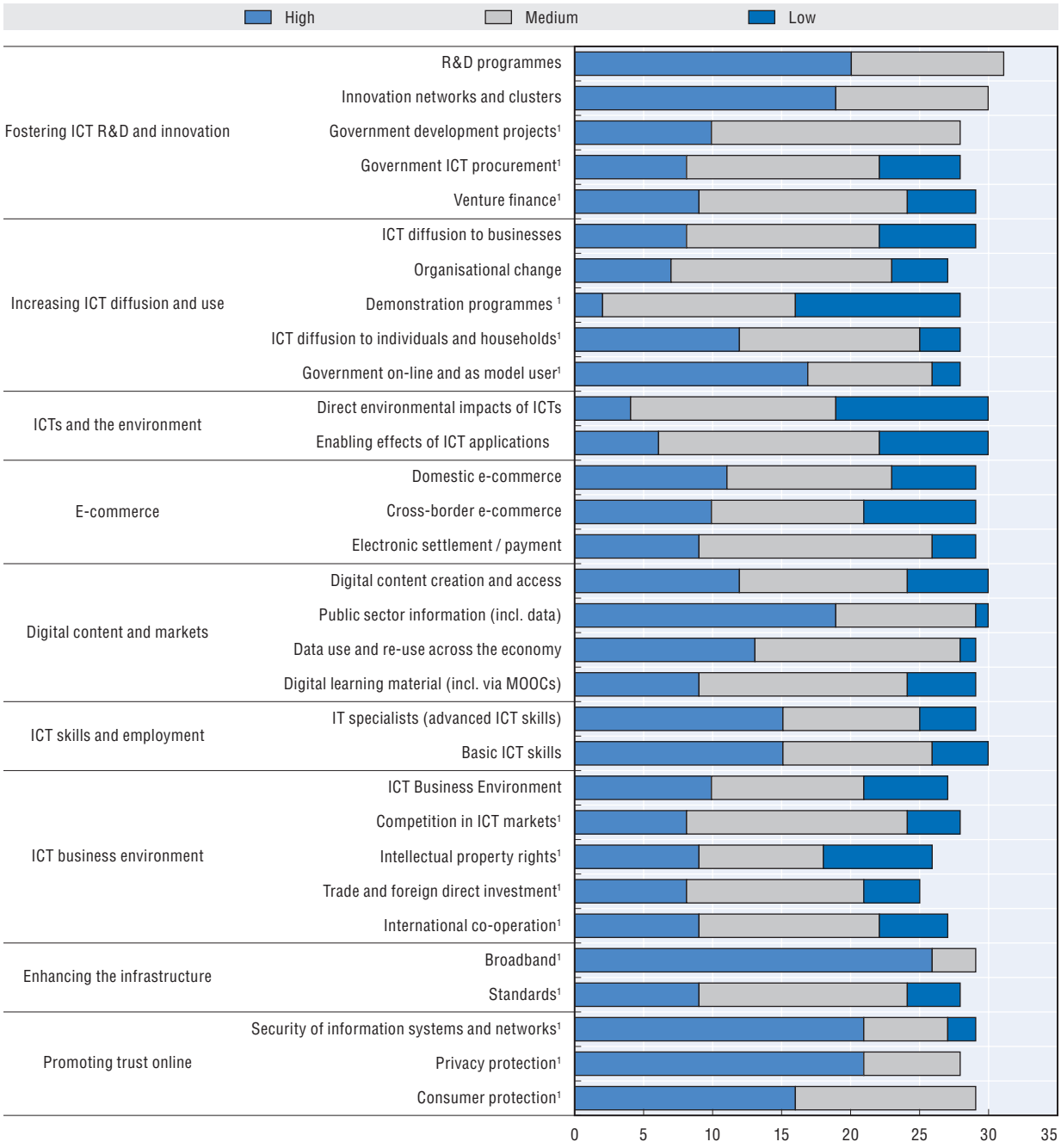
Wilson, K. and M. Testoni (2014), "Improving the role of equity crowdfunding in Europe's capital markets", *Bruegel Policy Contribution Issue*, 2014/09.

WSTS (World Semiconductor Trade Statistics) (2015), *WSTS Historical Billings Report*, *www.wsts.org/Teaser-Left/Historical-Billings-Report*.

Annex

Figure A.1. **Current ICT policy priorities, 2014**

Number of responses



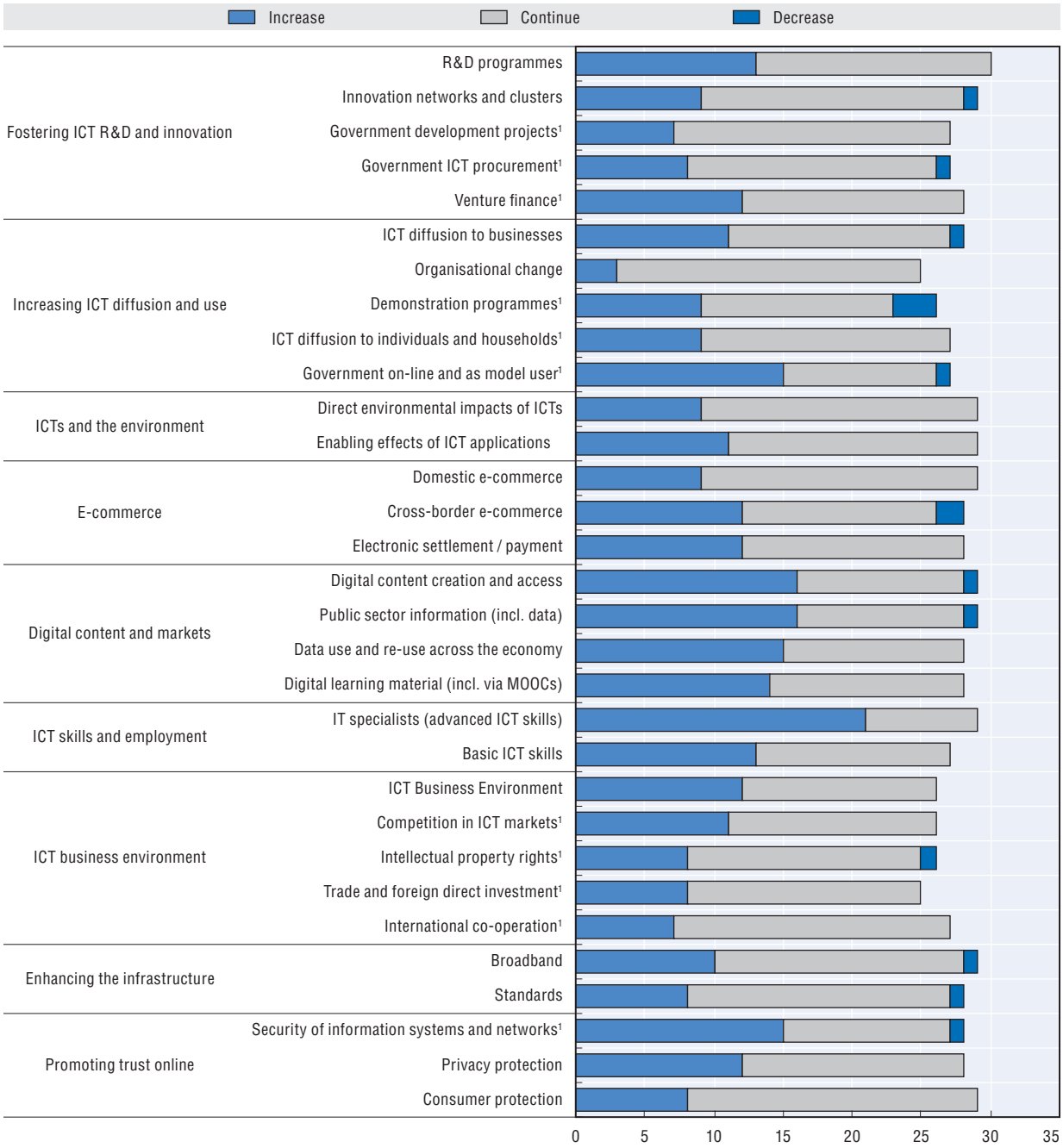
Note: *These policy areas are not covered in the 2014 policy questionnaire. They are retained here because (i) they are included in national strategies for the digital economy, and (ii) some of the policy areas are being addressed by other committees conducting related surveys (e.g. the Public Governance Committee on e-government and government ICT procurement).

Source: Based on 31 detailed responses (including 25 OECD countries) to the OECD DEO Policy Questionnaire 2014 on current and future policy priorities, sent on June 2014.

StatLink http://dx.doi.org/10.1787/888933224286

Figure A.2. **Evolution of ICT policy priorities**

Number of responses



Note: *These policy areas are not covered in the 2014 policy questionnaire. They are retained here because (i) they are included in national strategies for the digital economy, and (ii) some of the policy areas are being addressed by other committees conducting related surveys (e.g. the Public Governance Committee on e-government and government ICT procurement).

Source: Based on 31 detailed responses (including 25 OECD countries) to the OECD DEO Policy Questionnaire 2014 on current and future policy priorities, sent on June 2014.

StatLink http://dx.doi.org/10.1787/888933224297

© OECD 2015

Chapter 2

The foundations of the digital economy

The Internet, broadband networks, mobile applications, IT services and hardware constitute the foundations of the digital economy. This chapter examines recent trends and structural features of the ICT sector, telecommunication markets, and broadband infrastructures and services. By looking at growth in value added and employment, changes in international trade, R&D expenditures, innovation activities and communication revenue, penetration, network size, broadband speeds and prices, and IPv6 indicators, the chapter highlights the fundamental role of information and communication industries as a driver of growth and innovation in the digital economy.

2.1 The ICT sector

Recent developments

The ICT sector proved relatively resilient to the 2007-09 global economic crisis, but still had not fully recovered by 2014. Output growth in ICT-producing industries was sluggish from late 2010 onwards in most countries, especially for those impacted more severely by the crisis (Figure 2.1a). The same trend was observed in computer-related services and telecommunication services, although the effects of the crisis were milder in both sectors (Figure 2.1b and 2.1c).

Growth rates in semiconductors – an industry where cyclical fluctuations appear ahead of other ICT industries – increased in the first half of 2014, but started to decrease thereafter (Figure 2.2). This trend is forecast to continue in 2015-16. Venture capital investment, a market indicator of upcoming business opportunities, presents a more positive outlook. Venture capital investment in the United States reached almost USD 15 billion in Q4 2014, its highest level since the dot-com bubble (Figure 2.3). The share of US venture capital devoted to ICT industries increased from about 48% to 67% between 2011 and 2014. In the same year, ICT services alone accounted for over 40% of total US venture capital investment.

Value added and employment in the ICT sector

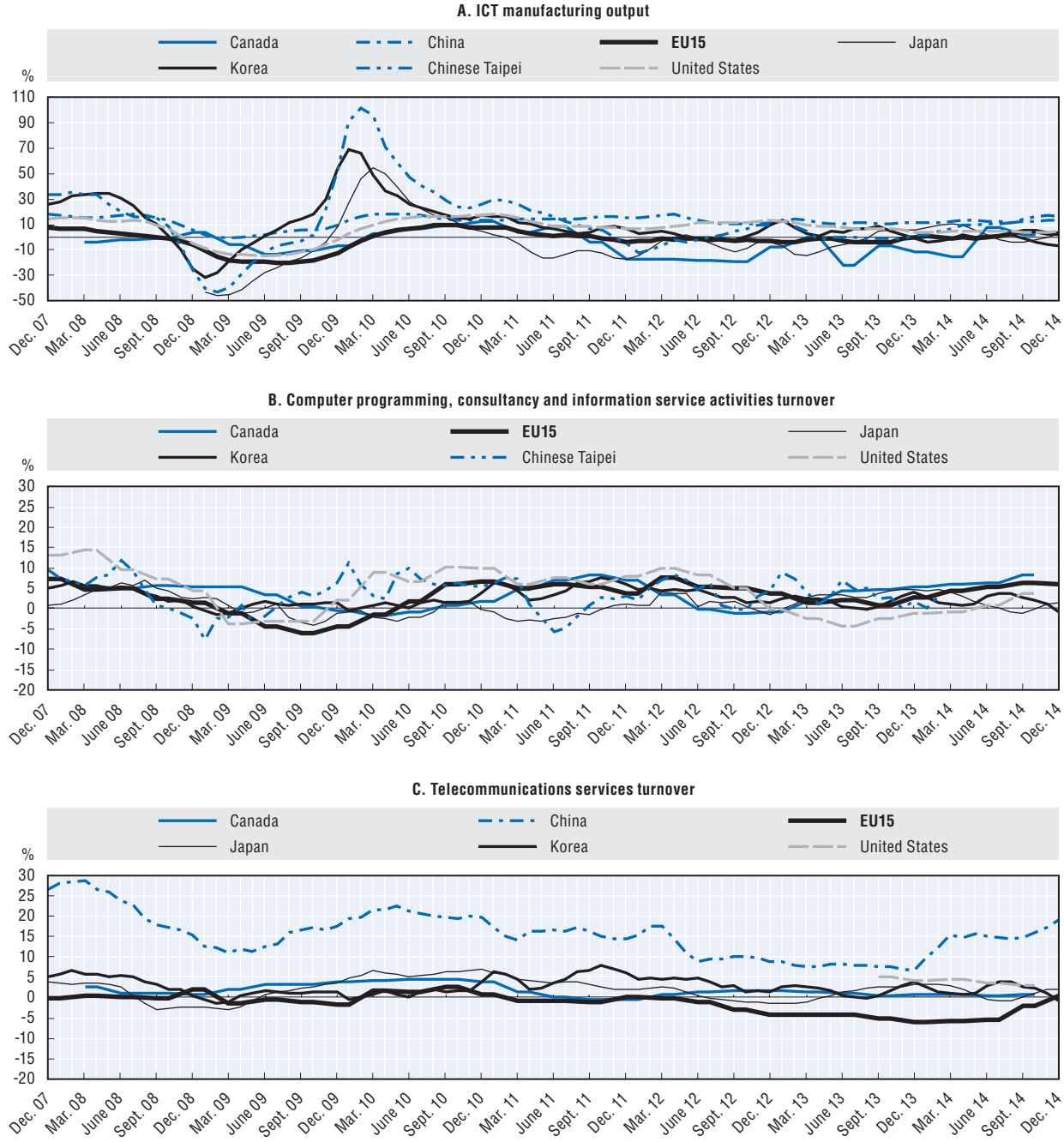
In 2013, the ICT sector in the OECD accounted for 5.5% of total value added, equivalent to about USD 2.4 trillion (Figure 2.4). This share shows large variations across countries, ranging from 10.7% of value added in Korea to less than 3% in Iceland and Mexico. Ireland and Japan have the second largest share (7%), followed by Sweden and Hungary (over 6%).

Over two thirds of the ICT sector in the OECD is accounted for by IT and other information services (2% of total value added) and telecommunications (1.7%). Computer, electronic and optical products and software publishing account for, respectively, 1.4% and 0.3% of total value added. The degree of specialisation, however, varies significantly among countries. Korea shows the strongest specialisation in computer, electronic and optical products (over 7% of total value added), Luxembourg in telecommunications (3%) and Ireland, Sweden and the United Kingdom specialise in IT and other information services (3%).

The share of ICT goods and services in OECD total value added remained stable between 2007 and 2013 (Figure 2.5). In certain countries, however, this share decreased in the years following the crisis: Finland (-4.9 percentage points), France (-0.8) Mexico (-0.7), the Netherlands (-0.5), Denmark, Germany and Italy (-0.4). In some cases, the relative decrease in the ICT sector began before the crisis, following the dot-com bubble: Ireland (-2.1 percentage points), Luxembourg (-1.6), Austria (-0.8) and France (-0.4). Over the whole period (2001-13), the share of ICT increased in the Czech Republic (1.2), Estonia and Slovenia (0.9).

Figure 2.1. **Growth of the ICT sector, December 2007 – December 2014**

Year-on-year percentage change, three-month moving average



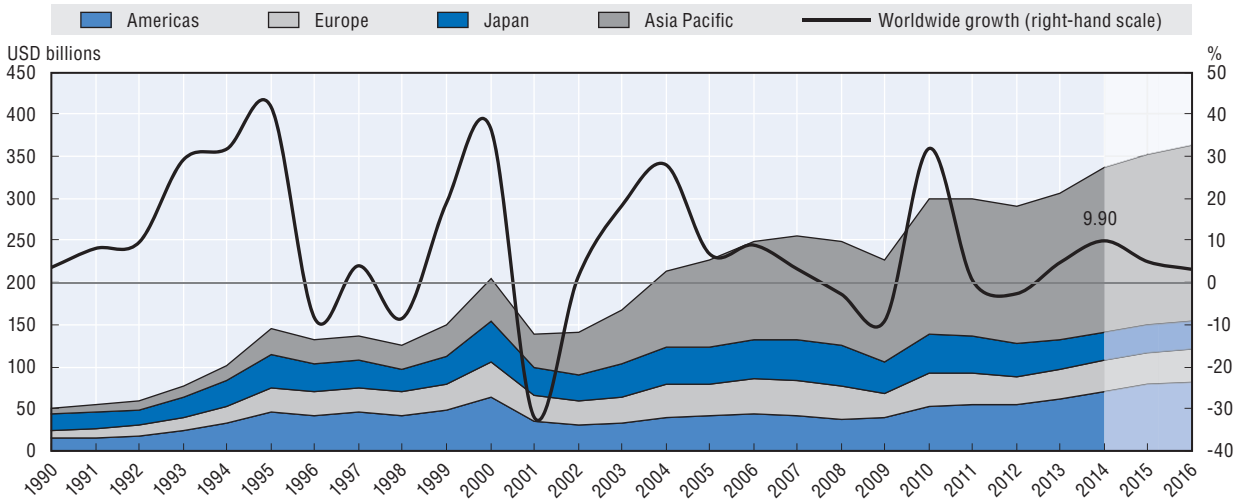
Notes: Data are seasonally adjusted. The EU15 comprise the following 15 countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom. For Canada and Chinese Taipei, data correspond to Computer Systems Design and Data processing services. For Korea, data refer to the aggregate for Information services.

Sources: Based on data from national statistical offices, short-term indicators and Eurostat Short-term business statistics database, May 2015.

StatLink http://dx.doi.org/10.1787/888933224306

Figure 2.2. **Worldwide semiconductor market by region, 1990-2016**

Annual sales, USD billion, current prices and year on year growth



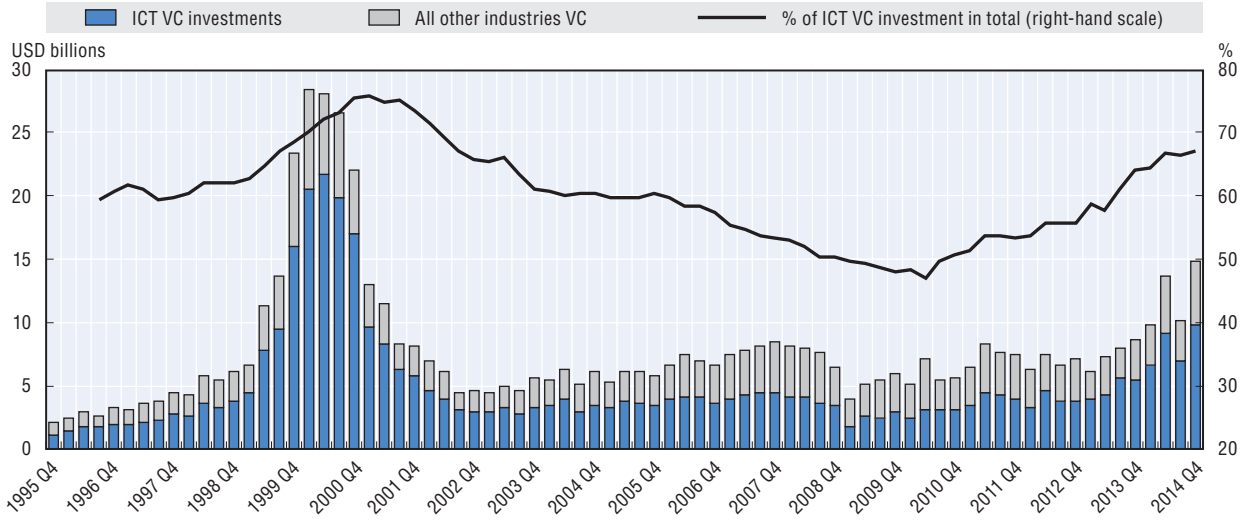
Note: 2015 and 2016 data are forecasts.

Source: Based on World Semiconductor Trade Statistics (WSTS), February 2015.

StatLink http://dx.doi.org/10.1787/888933224336

Figure 2.3. **Quarterly venture capital investments and trends of ICT VC shares in the United States, Q4 1995- Q4 2014**

USD billions and year-on-year growth, 4Q moving average



Notes: The aggregate ICT is defined here as the sum of software, IT services and telecommunications, semiconductors, computers and peripherals, networking equipment, electronics and instrumentation, and media and entertainment industries (comprising consumer electronics such as TV/stereos/games). The share of ICT of the total is expressed as a 4Q moving average.

Source: Based on PricewaterhouseCoopers/National Venture Capital Association MoneyTree™ Report, which draws on Thomson Reuters data, February 2015.

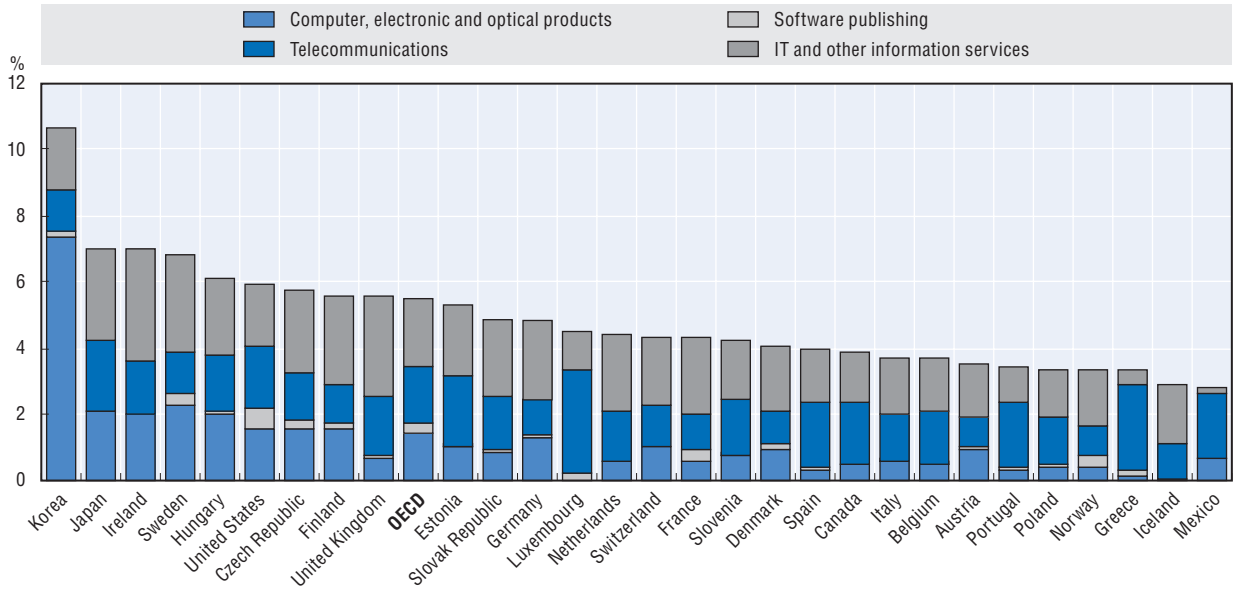
StatLink http://dx.doi.org/10.1787/888933224347

Computer and electronics manufacturing and, to a lesser extent, telecommunication services lost weight as a result of a combination of factors, including delocalisation of production to non-OECD economies, a decrease in unit prices and a less than proportional increase in final demand (OECD, 2014a). Between 2001 and 2013, the share of ICT

manufacturing activities dropped from 1.7% to 1.4% of total value added. This share grew only in Korea and a few countries in Eastern Europe, which benefited from offshoring, but fell steeply in Finland and Ireland. The share of telecommunication services also decreased from 2% to 1.7% with respect to 2001, and even further with regard to the 2003-04 peak, as a result of a steep fall in prices.

Figure 2.4. **Value added of ICT sector and sub-sectors, 2013**

As a percentage of total value added at current prices



Notes: The ICT sector is defined here as the sum of industries ISIC rev.4 26, 582, 61 and 62-63. For Germany, Iceland, Ireland, Japan, Mexico, Poland, Spain, Sweden, Switzerland and the United Kingdom, data refer to 2012. For Canada and Portugal, data refer to 2011. For Ireland and the United Kingdom, data refer to SNA 93 and were extracted in October 2014. For the rest of countries, data refer to SNA 2008. For Canada, Iceland, Ireland, Japan and Mexico, data for Software publishing are not available, and are therefore not included in the definition. The figure for Switzerland shows the ICT sector share as defined by the OECD (2011a). In this particular case, the share is not totally comparable with the rest of the countries.

Source: Based on OECD, National Accounts Database; Eurostat, National Accounts Statistics and national sources, April 2015.

StatLink http://dx.doi.org/10.1787/888933224356

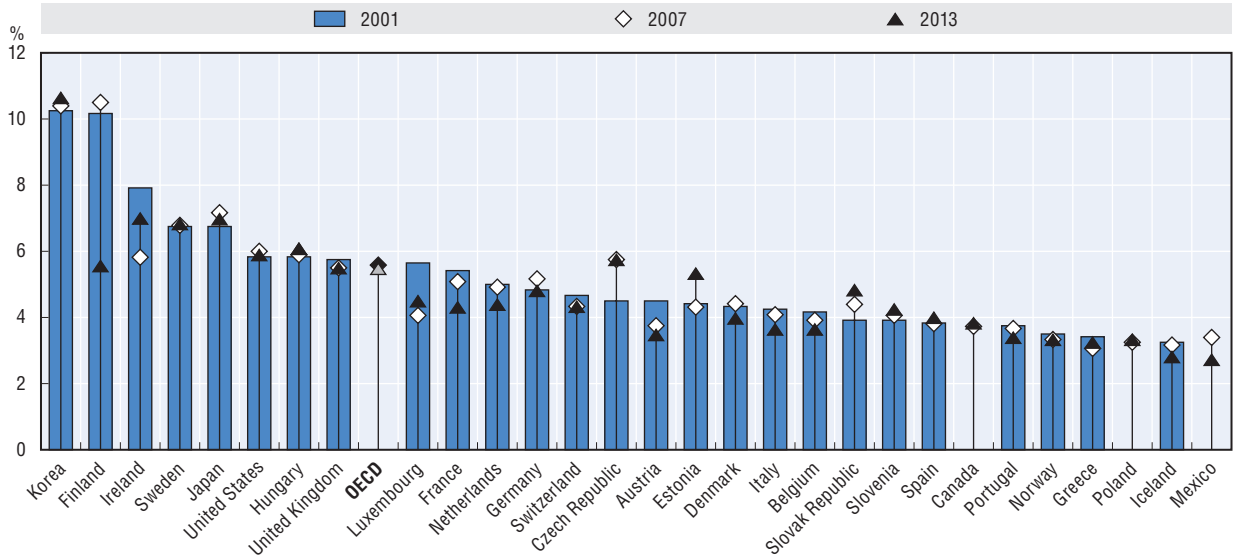
Over the same period, the share of software publishing in total value added remained at 0.3% while the share of IT services rose in all reporting economies, from 1.8% to 2%, largely offsetting losses in the other ICT sectors. In the Czech Republic, Estonia, Finland, Hungary, the Slovak Republic and Slovenia, the share of IT services in total value added increased by about 1 percentage point or more. Even in larger economies such as Germany, Japan, Spain, the United Kingdom and the United States, the share of IT services rose by about 0.5 percentage points. Despite the increasing importance of IT services, country differences in the overall share of the ICT sector remain driven mainly by the relative importance of ICT manufacturing industries and, to a small extent, software publishing activities.

In 2013, employment in the ICT sector accounted for more than 14 million people, almost 3% of total employment in the OECD (Figure 2.6). This share ranges between over 4% in Ireland and Korea to less than 2% in Greece, Portugal and Mexico. IT and other information services together with the telecommunications industry account for 80% of ICT employment in the OECD area. Over 2001-13, the employment weight of ICT decreased

in countries with a large ICT sector and increased in countries with a smaller ICT sector. One likely explanation is that the crisis fostered rationalisation in large national ICT sectors and favoured ICT firms in countries with lower labour costs. Belgium and Hungary are the only exceptions to this general trend (Figure 2.7).

Figure 2.5. **Evolution of ICT sector value added, 2001, 2007 and 2013**

Shares of total value added



Note: The ICT sector is defined here as the sum of industries ISIC rev.4 26, 582, 61 and 62-63. For Germany, Iceland, Ireland, Japan, Mexico, Poland, Spain, Sweden, Switzerland and the United Kingdom, data refer to 2012. For Canada and Portugal, data refer to 2011. For Ireland and the United Kingdom, data refer to SNA 93 and were extracted in October 2014. For the rest of countries, data refer to SNA 2008. For Canada, Iceland, Ireland, Japan and Mexico, data for Software publishing are not available, and are therefore not included in the definition. The figure for Switzerland shows the ICT sector share as defined by the OECD (2011a). In this particular case, the share is not totally comparable with the rest of the countries. For Mexico, data refer to 2003 instead of 2001.

Source: Based on OECD, National Accounts Database, ISIC Rev.4; Eurostat, National Accounts Statistics and national sources, April 2015.

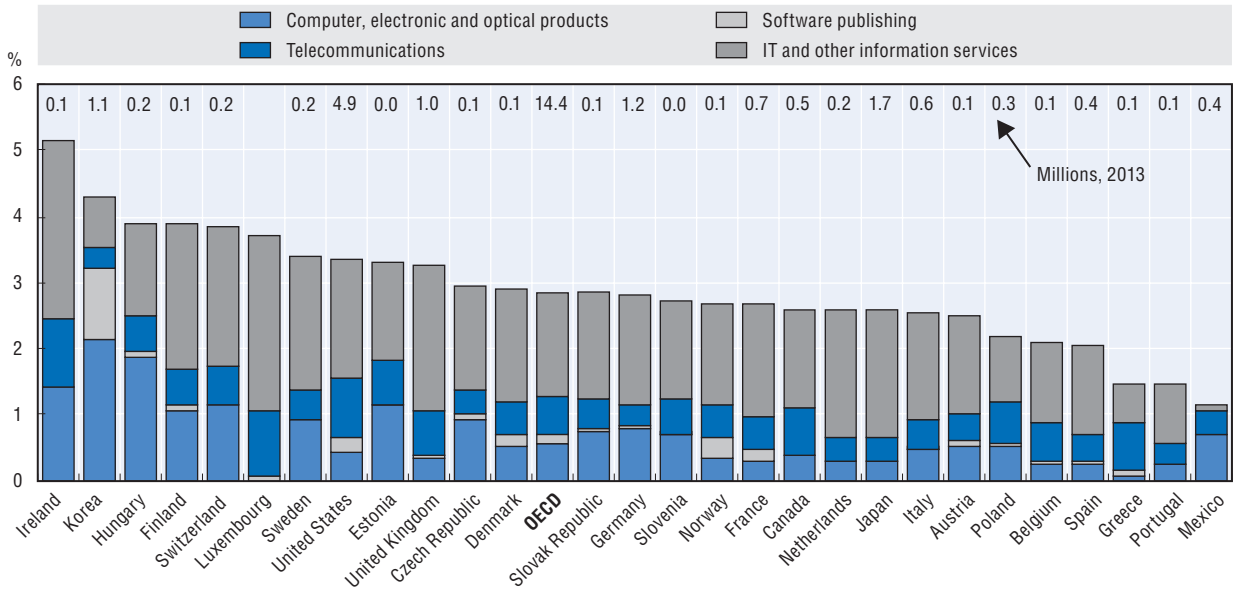
StatLink *http://dx.doi.org/10.1787/888933224366*

Some ICT activities are carried out in sectors other than the ICT sector. Accordingly, data on ICT specialists complement those on ICT-related employment. ICT specialists engaged in developing, maintaining or operating ICT systems, or for whom ICTs are the main part of their job (OECD, 2005; 2012a; 2013), accounted on average for 3.6% of OECD total employment in 2014 (Figure 2.8). In the few countries where data are available over several years, the share of ICT specialists has increased at a moderate rate – from about 4% to 4.7% in Canada, from 3.2% to 4% in the United States and from 3.6% to 3.8% in Australia over 2003-14.

A significant part of ICT value added and employment in OECD countries is accounted for by foreign affiliates (i.e. local firms owned or controlled by a foreign company). In 2013, the share of ICT value added produced by foreign affiliates was as high as 80% in Estonia, above 75% in Hungary, 65% in the Slovak Republic, and about 60% in the Czech Republic and Poland. ICT employment matches this trend, although the employment shares tend to be lower due to higher productivity of foreign affiliates relative to domestic firms (Figure 2.9).

Figure 2.6. **Employment in the ICT sector and sub-sectors, 2013**

As a percentage of total employment



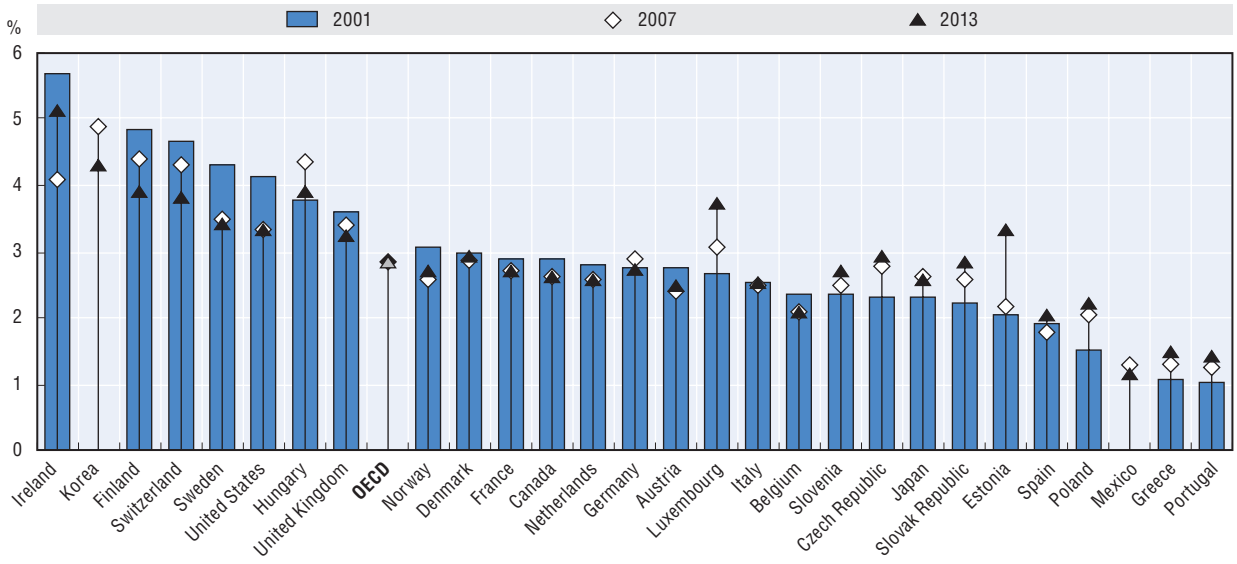
Notes: The ICT sector is defined here as the sum of industries ISIC rev.4 26, 582, 61 and 62-63. For France, Germany, Ireland, Japan, Spain and Switzerland, data refer to 2012. For Mexico, Portugal and Sweden, data refer to 2011. For Ireland, Mexico, Portugal and Sweden, data refer to SNA 93 and were extracted in October 2014. For Canada, Ireland, Japan, Mexico, the Netherlands, Portugal and Sweden, data for Software publishing are not available, and are therefore not included in the definition. The figure for Switzerland shows the ICT sector share as defined by the OECD (2011a). In this particular case, the share is not totally comparable with the rest of the countries.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4; Eurostat, National Accounts Statistics and national sources, April 2015.

StatLink http://dx.doi.org/10.1787/888933224376

Figure 2.7. **Evolution of ICT sector employment, 2001, 2007 and 2013**

As a percentage of total employment



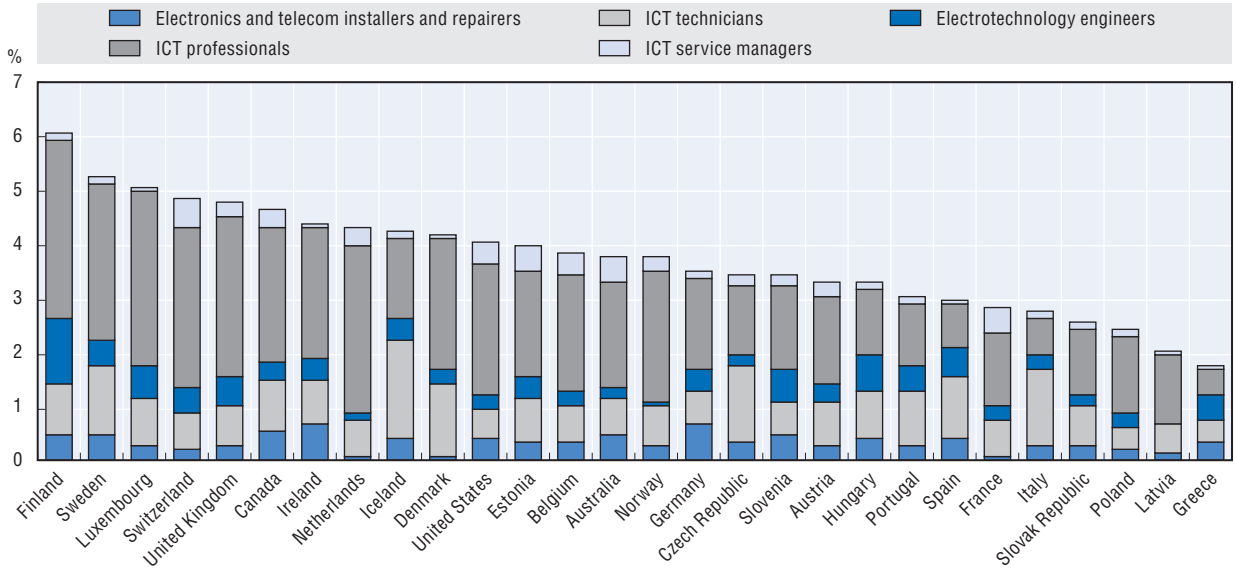
Notes: The ICT sector is defined here as the sum of industries ISIC rev.4 26, 582, 61 and 62-63. For France, Germany, Ireland, Japan, Spain and Switzerland, data refer to 2012. For Mexico, Portugal and Sweden, data refer to 2011. For Ireland, Mexico, Portugal and Sweden, data refer to SNA 93 and were extracted in October 2014. For Canada, Ireland, Japan, Mexico, the Netherlands, Portugal and Sweden, data for Software publishing are not available, and are therefore not included in the definition. The figure for Switzerland shows the ICT sector share as defined by the OECD (2011a). In this particular case, the share is not totally comparable with the rest of the countries.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4; Eurostat, National Accounts Statistics and national sources, April 2015.

StatLink http://dx.doi.org/10.1787/888933224381

Figure 2.8. **ICT specialists in OECD countries, 2014**

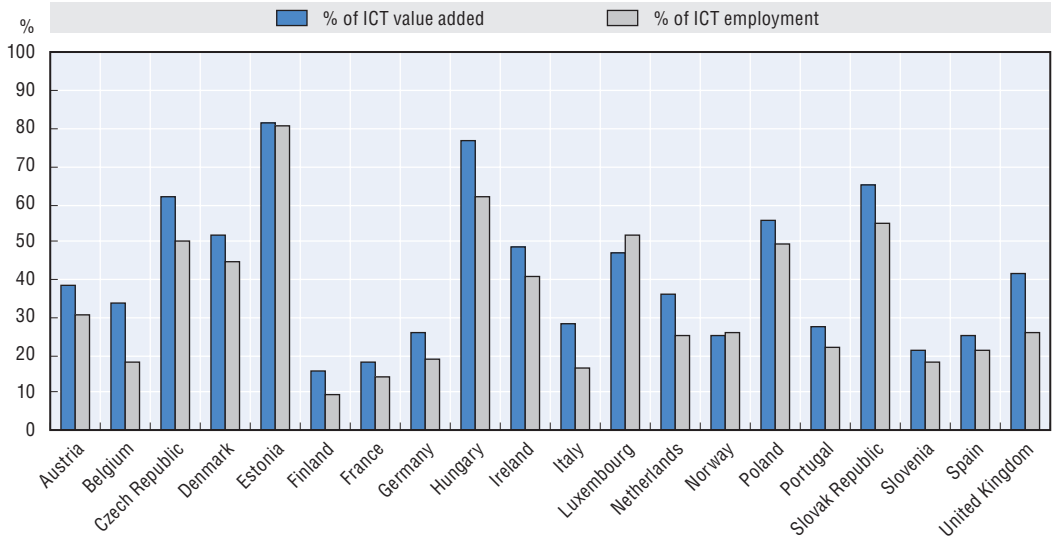
As a share of total employment, by category



Sources: Based on Australian, Canadian and European labour force surveys, as well as United States Current Population Survey, April 2015.

StatLink http://dx.doi.org/10.1787/888933224392

Figure 2.9. **Share of national value added and employment accounted by foreign affiliates in the ICT sector, 2013**



Notes: The ICT sector here is a proxy for the sum of industries ISIC rev.4 26, 61 and 62-63. Data refer to 2013 or latest available year.

Sources: Based on OECD National Accounts Database, ISIC Rev.4 and OECD Activity of Multinational Enterprises Database, April 2015.

StatLink http://dx.doi.org/10.1787/888933224409

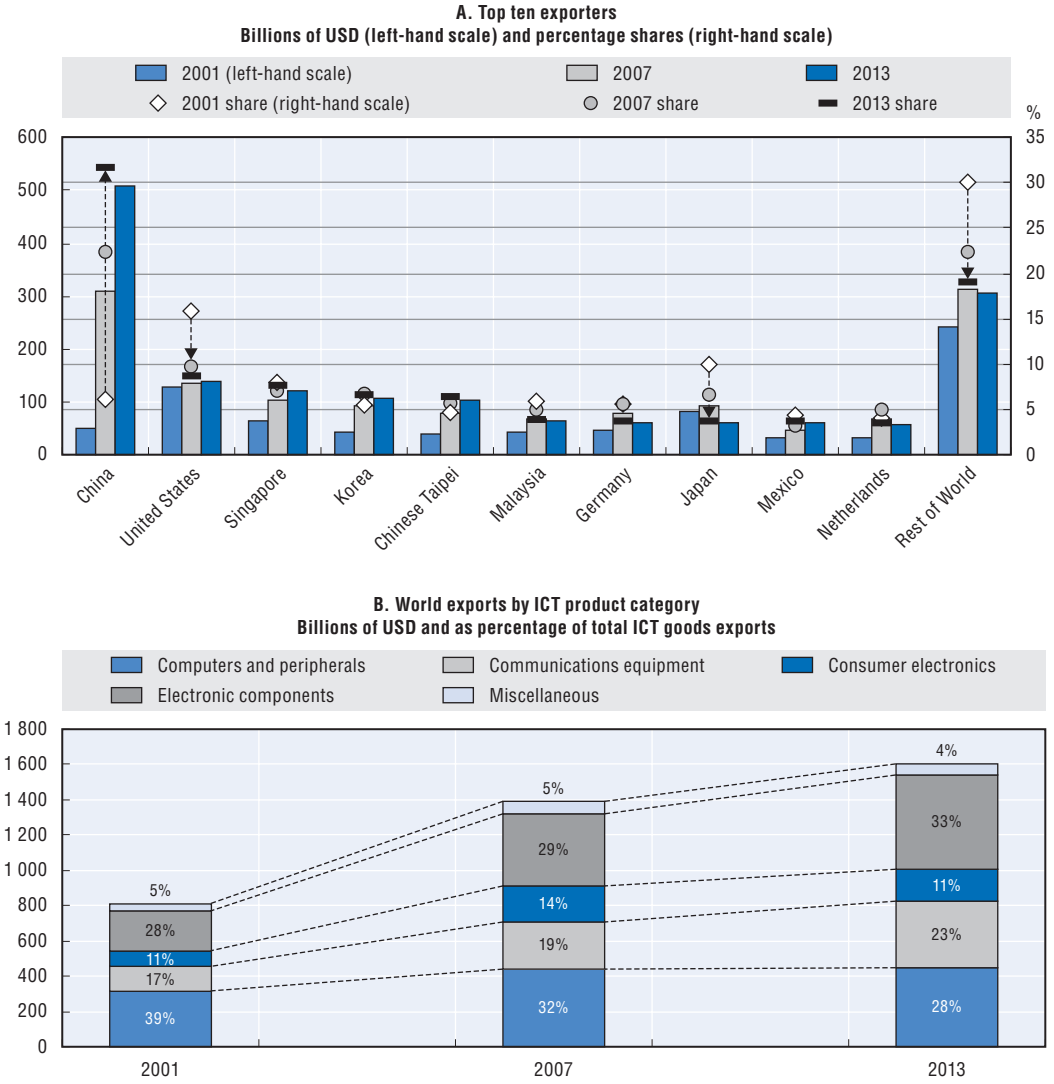
International trade in ICT goods and services

Trade data show continued growth in global ICT goods exports. Production and export of ICT goods are increasingly concentrated in a few economies (Figure 2.10a). The shares of Japan and the United States in world exports of ICT goods halved from 2001 to 2013, due

in part to offshoring of production, while China's grew from 6.1% to almost 32%, with a tenfold increase in dollar terms. Having a closer look at OECD countries, Korea is the only economy to increase its share of the world market for ICT goods over the same period, while Mexico increased its share from 2007 to 2013 and benefited from the relocation of international (not only US) activities linked to NAFTA.

Between 2001 and 2013, world exports of manufactured ICT goods grew by 6% per year, reaching over USD 1.6 trillion. However, the share of computers and peripherals in total ICT world exports decreased by 11 percentage points (Figure 2.10b), partly due to widespread falls in unit prices and inelastic final demand. Such decreases reflect a major shift in world trade patterns towards communication equipment and electronic components.

Figure 2.10. **World exports of ICT goods, 2001, 2007 and 2013**



Note: World exports are estimated based on the 103 BTDIxE declaring countries, which reported ICT exports in all three years. World exports exclude re-imports for China and re-exports for Hong Kong China. China's ICT exports are adjusted for re-imports.

Source: OECD, Bilateral Trade Database by Industry and End-use category (BTDIxE), *http://oe.cd/btd*, February 2015.

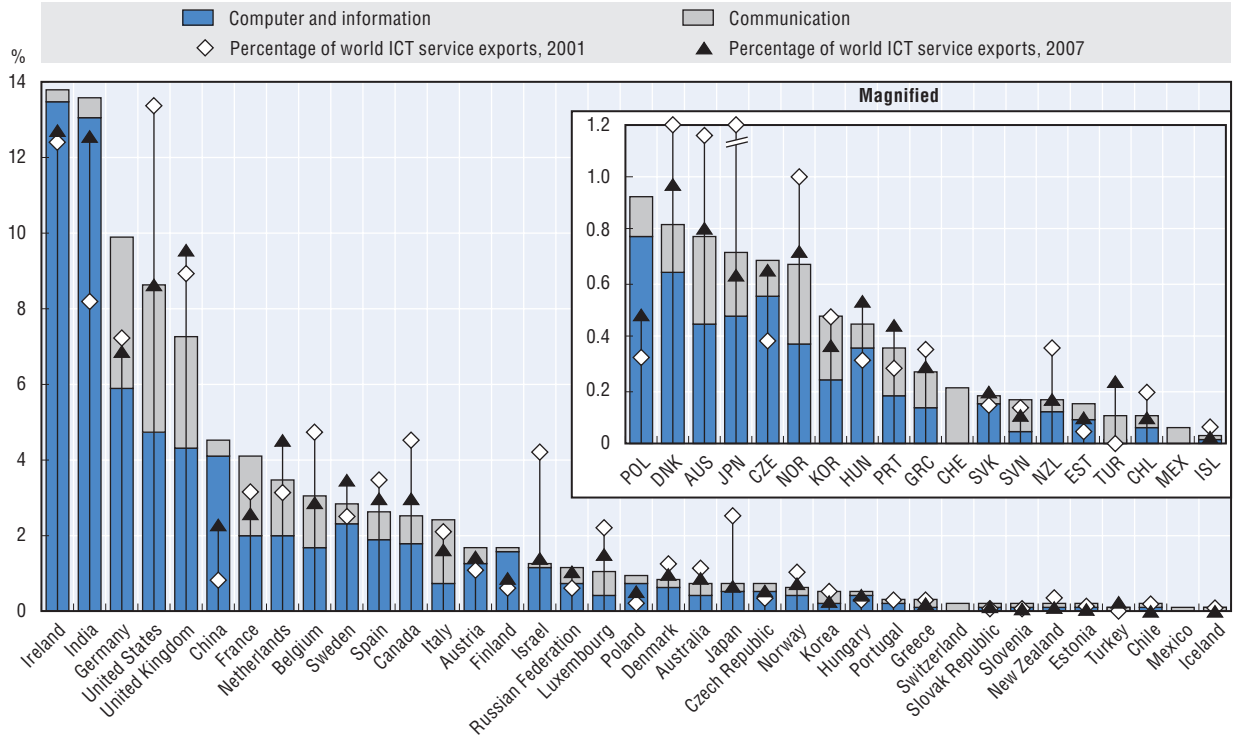
StatLink *http://dx.doi.org/10.1787/888933224410*

International trade in ICT services grew much faster than that of ICT goods, increasing fourfold in current price dollar terms to almost USD 400 billion between 2001 and 2013. In particular, the share of Computer and Information services almost doubled from 3.4% to 5.8% of world exports of services, while that of Telecommunication services increased marginally. For the OECD, the combined share of Computer and Information and Communication services rose from 5.8% to 8.3% of total service exports. However, the change in classification in 2007 renders interpretation of detailed trends and changes in trade difficult for that year.

As with trade in ICT goods, a few economies account for a significant share in global exports of ICT services, with some major shifts in recent years. Ireland is the leading exporter of computer and information services, followed by India, which started from a very modest level. China is also becoming a major exporter of ICT services along with Germany, the United Kingdom and the United States. Together, these countries account for more than 60% of total exports of ICT services. The top exporters of telecommunications services include the United States, the largest European economies and the Netherlands (Figure 2.11).

Figure 2.11. **OECD and major exporters of ICT services, 2001, 2007 and 2013**

Percentage shares of total world exports



Notes: For Denmark, data refer to 2004 instead of 2001. For Chile, Iceland and Israel, data refer to 2012. For Luxembourg, data refer to 2002 instead of 2001. For Mexico and Switzerland, exports of computer and information services are not included.

Source: Based on UNCTAD, UNCTADstat, February 2015. *http://unctadstat.unctad.org*.

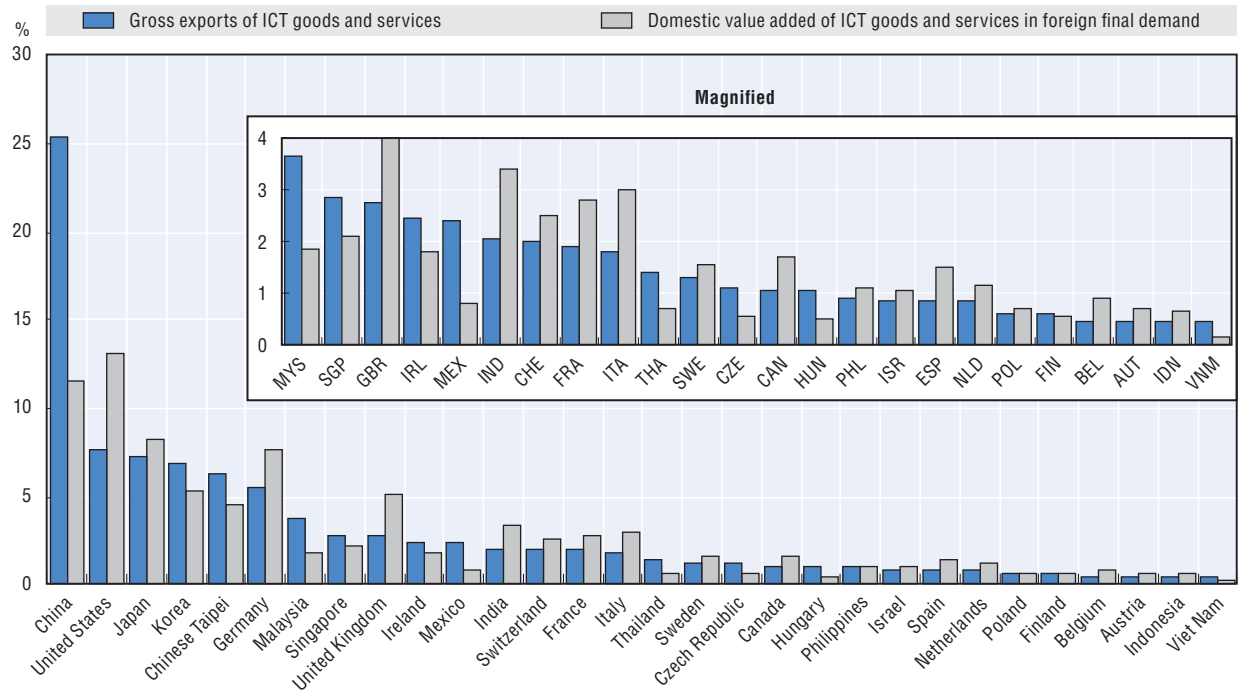
StatLink *http://dx.doi.org/10.1787/888933224437*

To a large extent, these trends are due to increasing trade in intermediate inputs (i.e. goods and services used in production). The dramatic increase in ICT exports from China, for example, has been matched by a proportional increase in imports of ICT intermediate inputs – notably in its processing zones. Consequently, China's share of ICT

goods and services valued added embodied in foreign final demand is significantly lower than its share of gross world exports. In 2011, US exports of ICT goods and services were higher than China's in value added terms – partly driven by the high presence of US ICT services embodied in final demand products. Embodied ICT services also contributed to higher shares for India and the United Kingdom in value added terms (Figure 2.12).

Figure 2.12. **Trade in ICT goods and services – gross exports and value added, 2011**

Percentage shares of the world total



Source: OECD, Inter-Country Input-Output (ICIO) Database, May 2015.

StatLink http://dx.doi.org/10.1787/888933224445

Innovation in the ICT sector

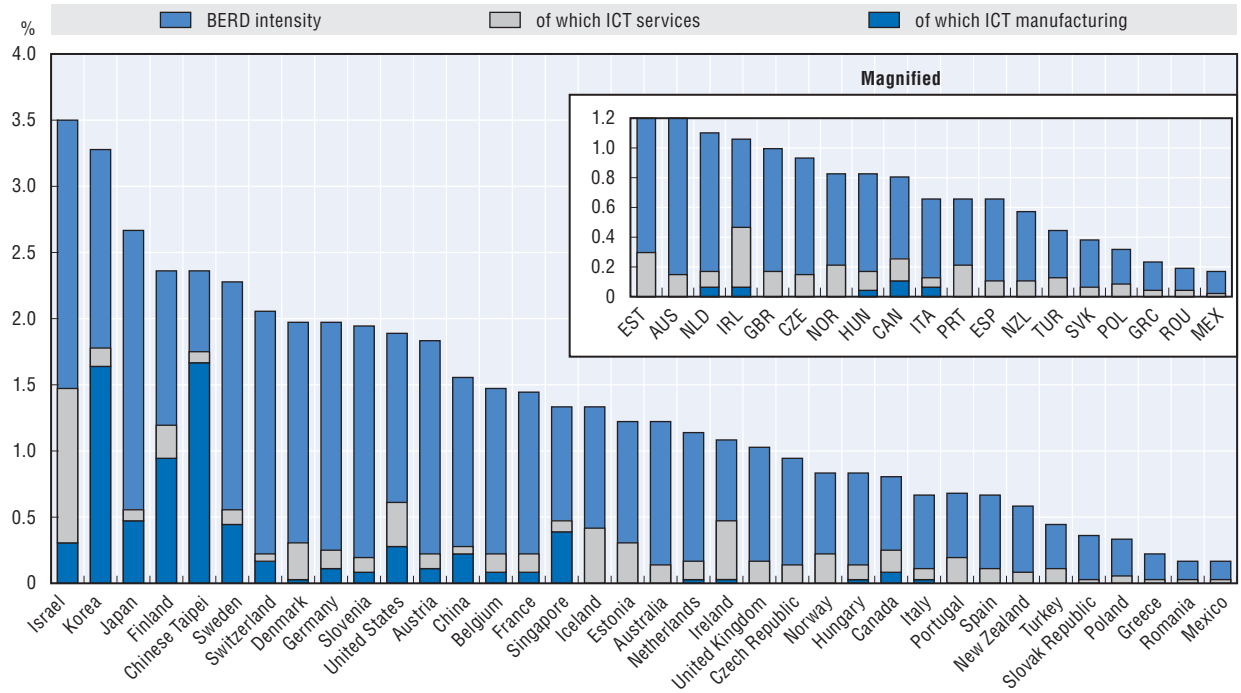
ICTs play a key role in today's innovation activities. Enterprises in the ICT sector are leading across all types of innovation activities, while innovators are often intensive users of ICTs.

In most OECD countries, the ICT sector accounts for the largest share of business expenditures on research and development (BERD), amounting to almost 33% of total BERD and 0.5% of GDP in most countries (Figure 2.13). In 2013, ICT BERD relative to GDP was highest in Chinese Taipei (1.77%), Korea (1.75%), Israel (1.5%) and Finland (1.2%), followed by the United States, Japan and Sweden (about 0.6%).

In general, ICT R&D expenditures tend to be concentrated in the ICT manufacturing sector, which accounts for over 60% of ICT BERD in the OECD. In 2013, Chinese Taipei and Korea devoted over 70% and 50% of their total BERD to ICT manufacturing. Despite the drop in Nokia's activities, Finland continues to spend over 40% of its total BERD on ICT manufacturing, followed by Singapore, Japan, the United States and Sweden, which all spent above 20% of total BERD. In Israel, China, Canada, Germany, Italy and France, the share of ICT BERD is between 10% and 20% of the total.

Figure 2.13. **ICT and total business expenditure in R&D intensities, 2013**

As a percentage of GDP



Notes: The ICT sector is defined as the sum of "ICT manufacturing" and "ICT services", which comprises "ICT trade industries", "Software publishing", "Telecommunications" and "IT and other information services", defined according to the OECD ICT sector definition based on ISIC Rev.4. When detailed data were not available, divisions 26 and 58 were used as a proxy for ICT manufacturing and Software publishing industries respectively. For the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Italy, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Switzerland and the United Kingdom, data refer to 2012. For Australia, Austria, Belgium, Greece, Iceland, Ireland, Mexico, New Zealand, Singapore and the United States, data refer to 2011.

Sources: OECD ANBERD and RDS Databases, February 2015.

StatLink http://dx.doi.org/10.1787/888933224458

Telecommunication services account for a lower share of R&D in most countries except Portugal, Denmark and Ireland. R&D expenditure on publishing and audio-visual activities, which includes some software development, is also substantial in Ireland (Figure 2.14).

Lower R&D expenditures in other countries reflect their specialisation in activities with low technological intensity (e.g. in Italy and Spain), or at the lower end of the value chain (e.g. Czech Republic, Estonia and Hungary).

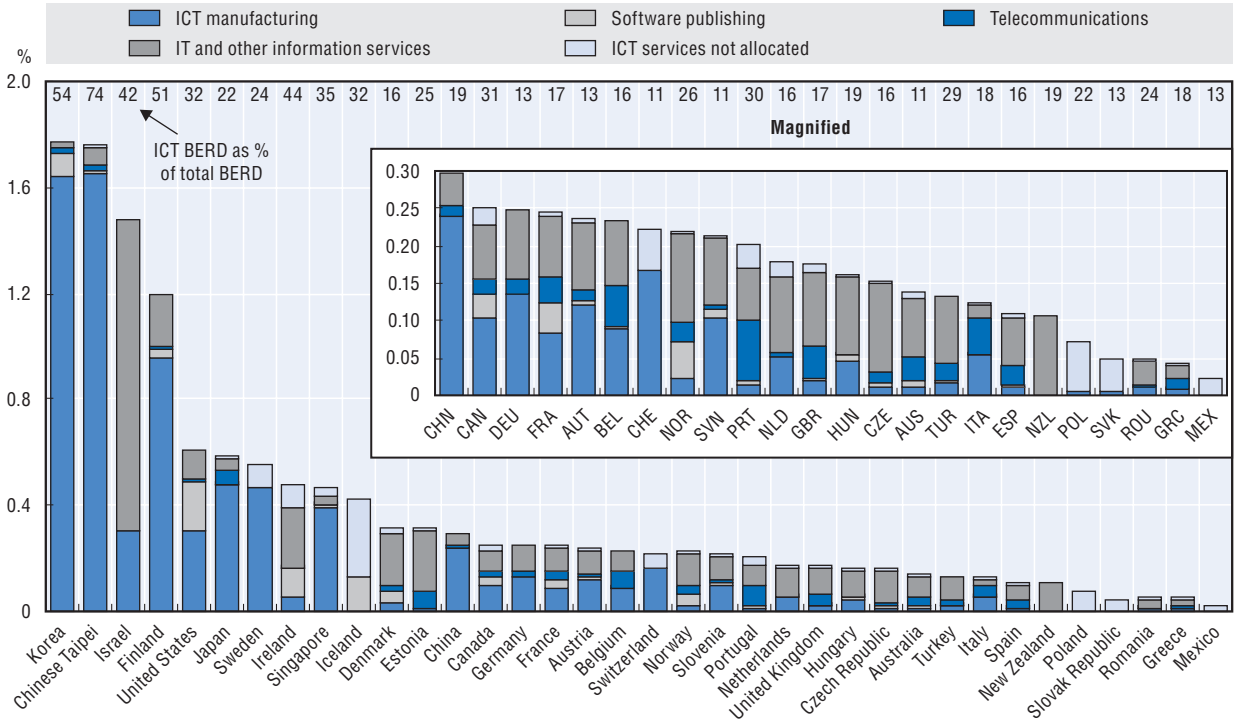
BERD intensity in information and communication services is also growing in many countries, but generally ranges from 2-3% to 5-6% of value added. In 2011, this share was above 6% in Denmark, followed by the United States and Portugal, as opposed to Hungary and Italy, which ranked below 2% (OECD, 2014a).

The level of BERD intensity in information and communication services (which is much lower than in ICT manufacturing) can be partly explained by the weight of network infrastructure on value added in telecommunication services, and the difficulties encountered in unbundling R&D and software development in IT services.

While R&D provides a measure of innovation input, patents, registered designs and trademarks capture innovation output. In 2010-12, more than half a million patent applications were filed worldwide under the Patent Cooperation Treaty (PCT). Patent

Figure 2.14. **Business R&D expenditures in the ICT sector, 2013**

As a percentage of GDP and of total business expenditure in R&D



Note: For the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Italy, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Switzerland and the United Kingdom, data refer to 2012. For Australia, Austria, Belgium, Greece, Iceland, Ireland, Mexico, New Zealand, Singapore and the United States, data refer to 2011. "ICT services not allocated" refers to ICT trade industries and other ICT industries within Divisions 61-63 that cannot be separated.

Sources: OECD ANBERD and RDS Databases, February 2015.

StatLink http://dx.doi.org/10.1787/888933224461

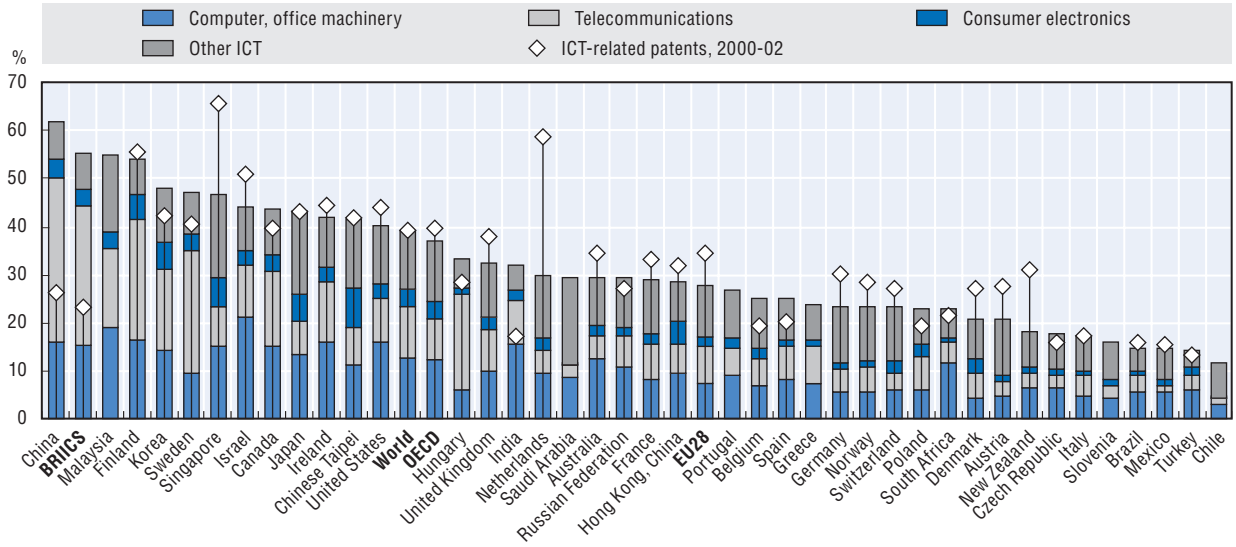
applications in ICT technologies accounted for almost 40% of total applications, representing a return to almost the 2000-02 level. In OECD countries ICT-related patents accounted for 37% of all applications (a decrease of 2.8 percentage points from 2000-02), while applications by BRIICS more than doubled reaching 55%, largely as a result of increased patenting by China (Figure 2.15).

About one quarter of ICT-related patents relate to one or more other technological fields. The top 25 technological fields associated with ICTs in patent applications include closely related technologies such as electrical machinery (14% of all ICT patents), as well as distant technological fields that rely heavily on ICTs, such as medical technology (9%) and biotechnology (7%) (see Figure 2.16).

Innovation activities in ICTs are increasingly undertaken through international networks. ICT-related patent applications are filed by co-inventors based in Canada, France, Germany, Switzerland, the United Kingdom and the United States, as well as China, India, Israel and Japan (Figure 2.17). Co-authored scientific publications in ICT-related fields show even denser and more diffused networks of international researchers (Figure 2.18).

Figure 2.15. **Specialisation in ICT-related patents, 2000-02 and 2010-12**

As a percentage of total PCT patent applications



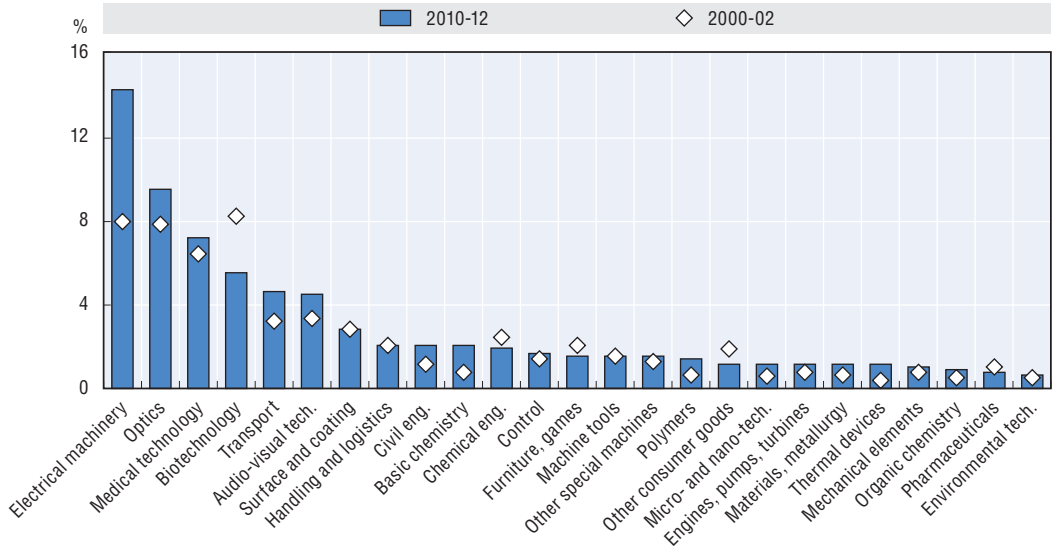
Note: Data relate to patent applications filed under the Patent Co-operation Treaty (PCT). Patent counts are based on the priority date, the inventor's residence and fractional counts. ICT-related patents are defined using a selection of International Patent Classification (IPC) classes. Only economies that applied for more than 250 patents in 2010-12 are included. BRIICS refers to Brazil, the Russian Federation, India, Indonesia, China and South Africa.

Source: OECD, Patent Database, *www.oecd.org/sti/ipr-statistics*, January 2015.

StatLink *http://dx.doi.org/10.1787/888933224476*

Figure 2.16. **Top 25 combinations between ICTs and other technologies in patent applications, 2000-02 and 2010-12**

As a percentage of all ICT-related applications also belonging to other technological fields



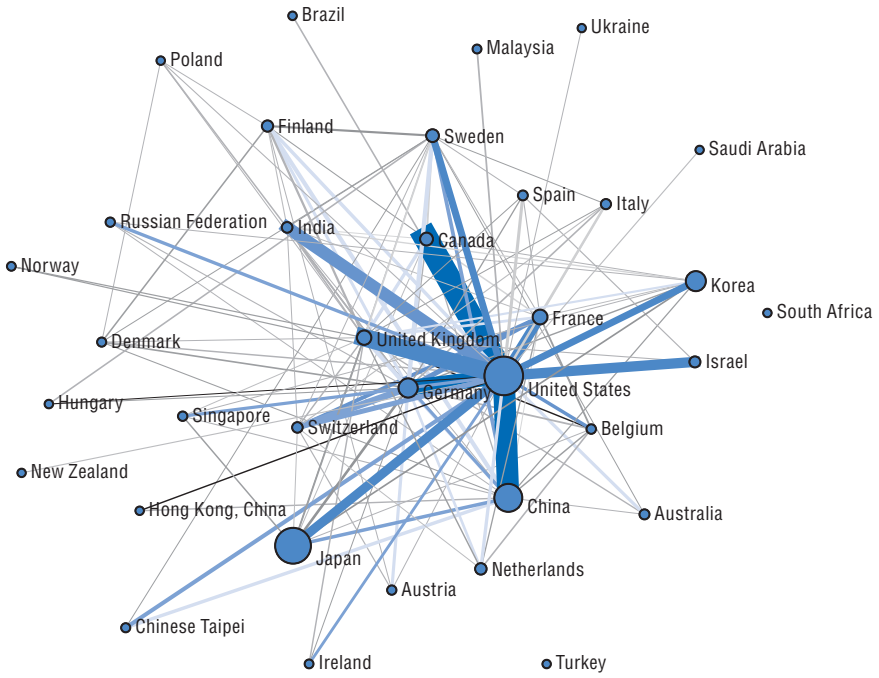
Notes: Data relate to patent applications filed under the Patent Co-operation Treaty (PCT). Patent counts are based on the priority date. ICT-related patents are defined using a selection of International Patent Classification (IPC) classes. Additional IPC codes listed in ICT-related patent documents have been classified according to the IPC-Technology Concordance proposed by Schmoch (2008), revised in January 2013, available at *www.wipo.int/ipstats/en/statistics/technology_concordance.html*. Control refers to the field that covers elements for controlling and regulating electrical and non-electrical systems and referring test arrangements, traffic control or signalling systems etc.

Source: OECD, Patent Database, February 2015.

StatLink *http://dx.doi.org/10.1787/888933224483*

Figure 2.17. **International cooperation networks in ICT-related patents, 2010-12**

Whole counts of internationally co-invented patents



Notes: The data refer to counts of patent applications filed under the Patent Co-operation Treaty (PCT) to protect ICT-related inventions, with at least one co-inventor located in a different country, by priority date, using whole counts. ICT-related patents are defined using a selection of International Patent Classification (IPC) classes.

Source: OECD, Patent Database, February 2015.

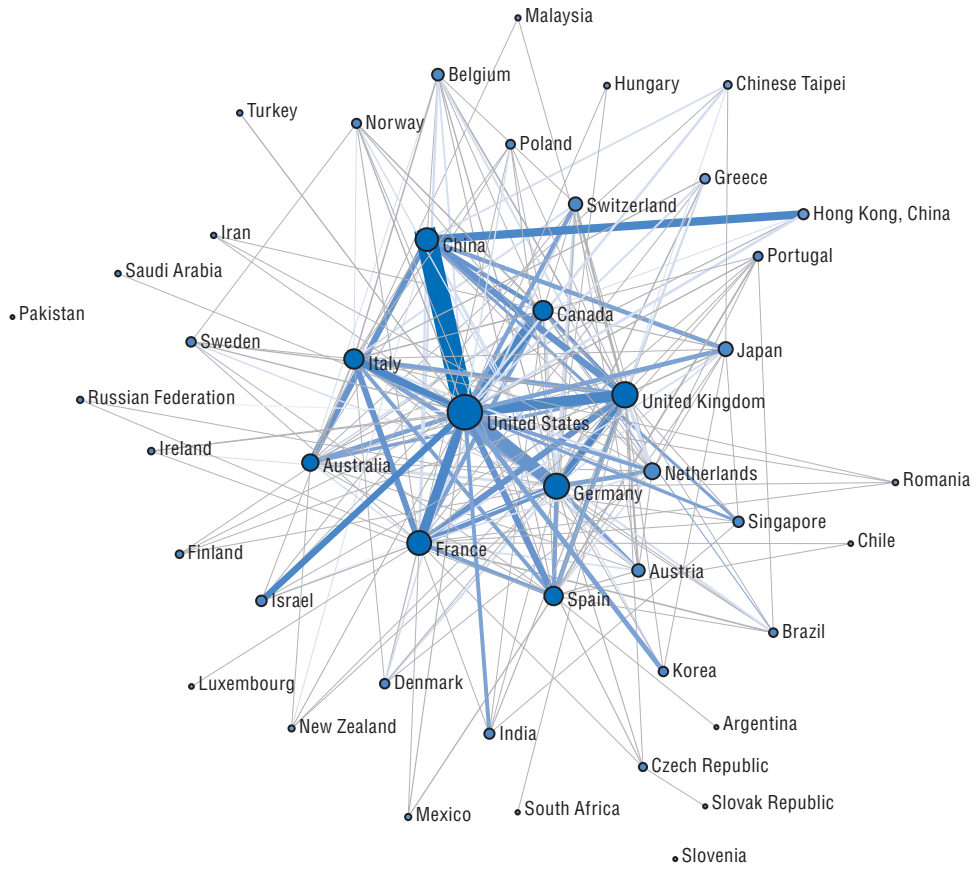
Registered designs can be used to proxy innovation in relation to the aesthetic feature of products. They can also provide information about product differentiation and customisation and, more generally, about the role played by design to shape competition in the marketplace. In 2010-13, registered designs in ICT and audio-visual devices[1] accounted for 8.5% of European Registered Community Designs (RCD), representing a 1-percentage point increase over 2005-08 (Figure 2.19). Across all economies, about 60% of registered ICT and audio-visual-related designs refer to data-processing and recording equipment, followed by communication and audio-visual devices.

The United States and Korea are the most active economies in ICT and audio-visual-related RCD (both gaining shares with respect to 2005-08), followed by Germany and Japan (both losing shares) with the other large European economies tailing behind. China doubled its share but remains a minor player with regard to designs registered in Europe.

The United States scores high in data-processing equipment and Korea in communication equipment, while France and Japan lead in the design of audio-visual devices. Design related to ICT and audio-visual products represents almost 60% of Korean total RCD. Other economies specialising in this field are Canada, Chinese Taipei, Japan and the United States.

Figure 2.18. **International cooperation networks in ICT-related science fields, 2011-12**

Whole counts of internationally co-authored documents



Notes: Data extraction is based on Elsevier's All Science and Journal Classification codes 17 (all subjects), 1903, 2614 and 2718. Bubble sizes are proportional to the number of scientific collaborations in a given year. The thickness of the lines (edges) between countries represents the intensity of collaboration (number of co-authored documents between each pair). The result has been visualised using the Kamada-Kawai (Kamada and Kawai, 1989) force algorithm, and implemented using the Sci2 tool (Sci2 Team, 2009).

Source: Based on Scopus Custom Data, Elsevier, version 4.2014, January 2015.

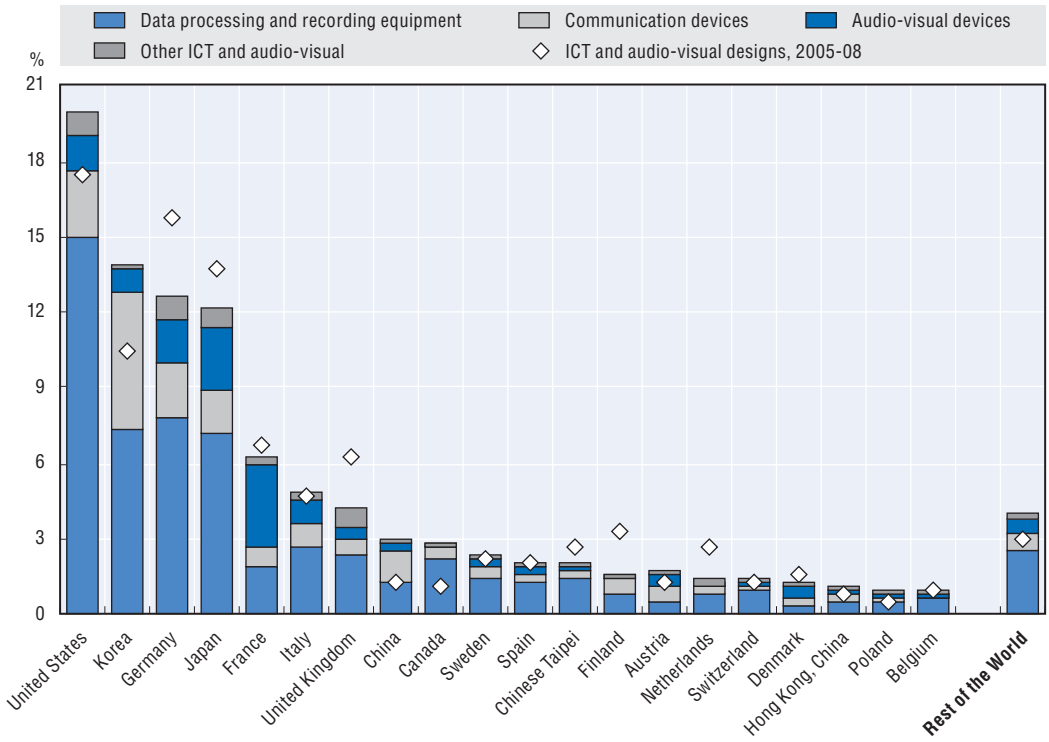
Branding activities of ICT-related products, as measured by trademark registrations, are also strong and increasing (Figure 2.20). In 2010-13, they accounted for about one third of total trademark filings at the European Office for Harmonisation in the Internal Market (OHIM), and one fifth at the United States Patent and Trademark Office (USPTO).

The distribution of trademarks offers a distinctive perspective on the competitive position of economies concerning ICT products. Indeed, national trademark shares do not align with R&D, patents or export shares. The United States appears to be the largest overall player, accounting for almost 80% of total ICT-related trademark applications at the USPTO and more than 12% at OHIM. ICT-related trademarks on the European market are conversely led by applicants in Germany, followed by the United States, the United Kingdom, Spain, France and Italy.

In the last five years, a number of large trademark players, such as Japan and the United States, but excluding Germany and Spain, lost shares in EU branding to the benefit of China, Korea and smaller EU economies.

Figure 2.19. **Top 20 applicants' share in ICT and audio-visual-related designs, 2005-08 and 2010-13**

As a percentage of total ICT and audio-visual-related Registered Community Designs



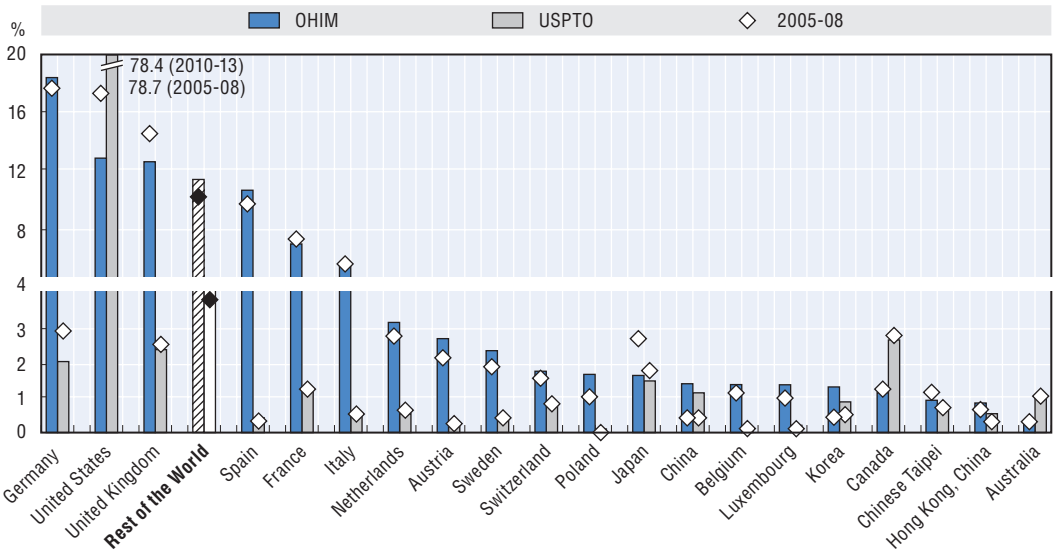
Notes: Total ICT and audio-visual designs correspond to designs in the following sub-classes of the Locarno classification: Data processing and recording equipment (14-01, 14-02 and 14-04); Communication devices (14-03); Audio-visual devices (16); Printing and Office machinery (18).

Source: OECD, 2014a. *http://dx.doi.org/10.1787/888933148580*.

StatLink *http://dx.doi.org/10.1787/888933224530*

Figure 2.20. **ICT-related trademarks, top 20 applicants, 2005-08 and 2010-13**

As a percentage of total ICT-related trademark applications



Source: OECD, 2014a. *http://dx.doi.org/10.1787/888933148613*.

StatLink *http://dx.doi.org/10.1787/888933224547*

Box 2.1. **ICT sector developments in Brazil**

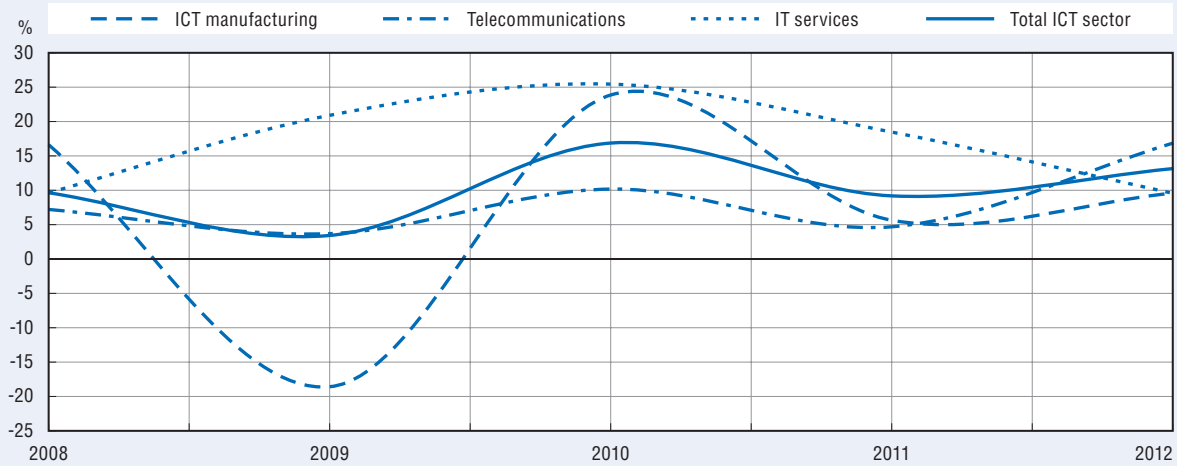
As with many emerging countries, Brazil has experienced a rapid increase in mobile communication services. From 2010 to 2014, Brazil saw a 79% increase in fixed broadband subscriptions, from 12.9 million to 23.1 million subscriptions. Mobile broadband access rose 825% over the same period, reaching 123.6 million subscriptions, and the proportion of active users (individuals who used the Internet on their mobile phone in the last three months) went from 15% in 2011 to 31.4% in 2013, with a further acceleration in 2014 (ANATEL, 2014).

This elevated growth in the use of ICTs is an indication of broader changes in the Brazilian economy and society. Although currently experiencing an economic downturn, Brazil has witnessed substantial growth of real income in the last 12 years, especially in the poorest cohort. Many Brazilians have embraced digital media rapidly and engage intensely in social media platforms. Such major economic and societal changes have contributed to rapid growth in the use of ICTs. The ICT sector overall proved resilient throughout the global economic crisis, supported by the domestic demand.

ICT value added, output and employment

Since 2008, ICT value added in Brazil has seen year-to-year growth. All sectors, with the exception of ICT manufacturing, have maintained a positive trend. The value added of ICT manufacturing dipped briefly to negative growth in 2009, with a decline of 19%, and peaked with positive growth of 24% in 2010, showing higher sensitivity to broader economic conditions than other sectors. The telecommunication services sector presented lower growth rates in 2009 and 2011 (4% and 5% respectively), while the ICT services sector demonstrated lower volatility and higher growth rates in terms of value added, peaking at 25% growth in 2010, and with lower levels of growth in 2008 and 2012 of about 10%.

Growth of ICT sector and sub-sectors value added in Brazil



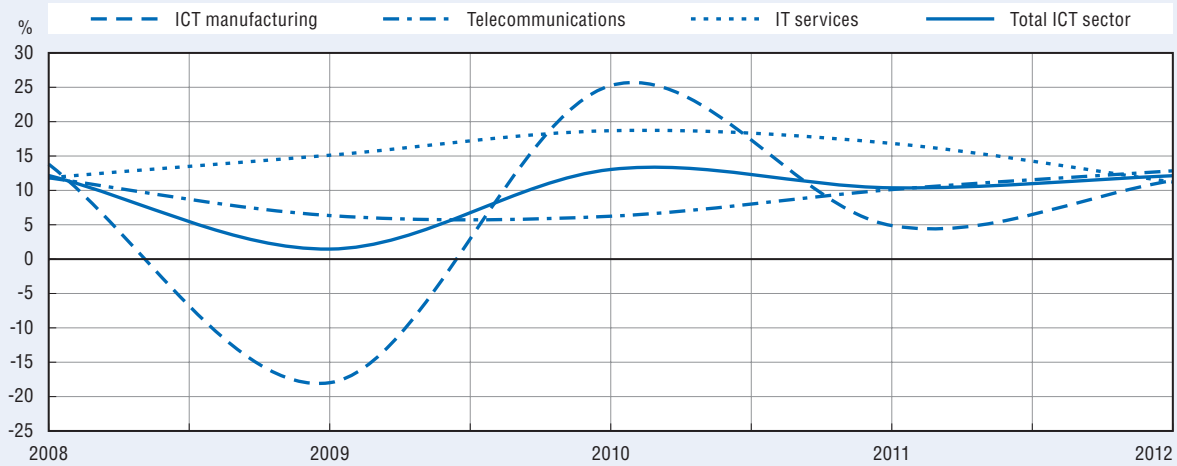
Source: Official statistics from the Brazilian Institute of Geography and Statistics (IBGE, 2014).

StatLink http://dx.doi.org/10.1787/888933224491

Similar to other OECD countries, the ICT services industry weathered the economic crisis much better than ICT manufacturing. Growth in ICT services output ranged between 19% in 2010 and 11%, in 2012, while ICT manufacturing output declined 19% in 2009, before recovering the following year. Between 2008 and 2012, the telecommunications sector maintained stable output growth ranging from 6% in 2009 to 13% in 2012. As a whole, the ICT sector sustained levels of growth of 12% and 13%, with the exception of 2009 when it grew 2%, driven by the output fall in the ICT manufacturing sector and outweighed by the growth in ICT services.

Box 2.1. **ICT sector developments in Brazil** *(cont.)*

Growth in annual output in ICT sector and sub-sectors in Brazil



Source: Official statistics from the Brazilian Institute of Geography and Statistics (IBGE, 2014).

StatLink http://dx.doi.org/10.1787/888933224508

The ICT sector in Brazil employed around 900,000 people in 2012. It contributed 0.9% of total employment in the country, with ICT services representing the largest share of 0.5%. Until 2010, ICT manufacturing accounted for a larger share than telecommunications, but was slightly surpassed by the telecommunication sector in 2011, which achieved a share of employment of 0.2% in 2012, while ICT manufacturing had 0.18%. The share of the ICT sector in employment has continued to grow in recent years, but remains a small fraction of the labour market. As in other emerging countries, Brazil faces the challenge of meeting market demand for skilled professionals. The Ministry of Labour calculated that in 2014 approximately 78,500 IT-related jobs were created, while only 33,600 people were trained to fill them (Ministry of Labour, 2014).

In comparison with employment growth across the economy as a whole, ICT sector employment has shown higher growth rates. While total employment in Brazil grew between 3% in 2008 and 1% in 2012, ICT sector employment accounted for a minimum growth of 3% in 2009 and a maximum of 11% in 2011. The largest employment growth in the period was exhibited by the telecommunication sector, which peaked at a 22% growth rate in 2011. Similarly to OECD countries, the sector most affected by the crisis was manufacturing with negative growth of 6% of employment in 2009, where more than 10,000 jobs were lost during the crisis – although these were recovered in 2010.

ICT research and investment

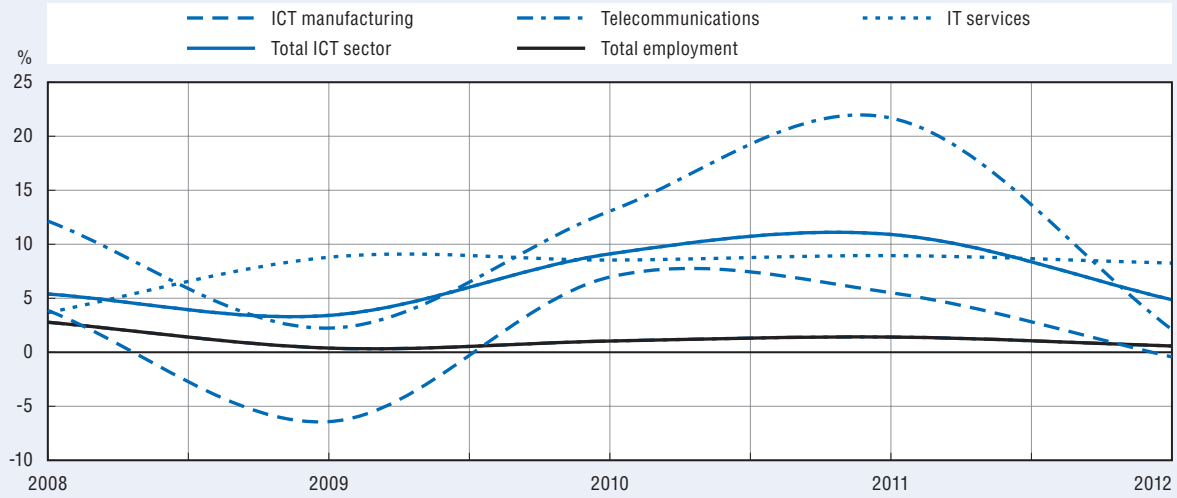
Business research and development expenditure (BERD) in Brazil reached the equivalent of 0.59% of national GDP in 2011 – a stable figure compared to 0.58% in 2008 (IPEA, 2013), but low when considered against 1.6% of GDP in the OECD area (OECD, 2012b).

BERD data for 2011 in Brazil pointed to higher R&D investments within the ICT sector when compared to R&D revenue proportions for the overall economy. BERD corresponded to 2.5% of revenue in the ICT sector businesses, while firms as a whole expended only 0.96% of their revenue in R&D globally in the same year. Of all ICT subsectors, ICT manufacturing dedicated the most to R&D, with 1.9% of revenue spent in 2011, while ICT services spent 1.7% and telecommunication services 0.8%.

Data on ICT sector firms also highlight the importance of innovation, with 44% of firms in the ICT sector implementing innovation in a product or process in 2011, compared to 28% for firms in all sectors. In Brazil, ICT manufacturing reported the largest share of innovative firms (52%), compared with ICT services (38%) and telecommunication services (26%).

Box 2.1. **ICT sector developments in Brazil** *(cont.)*

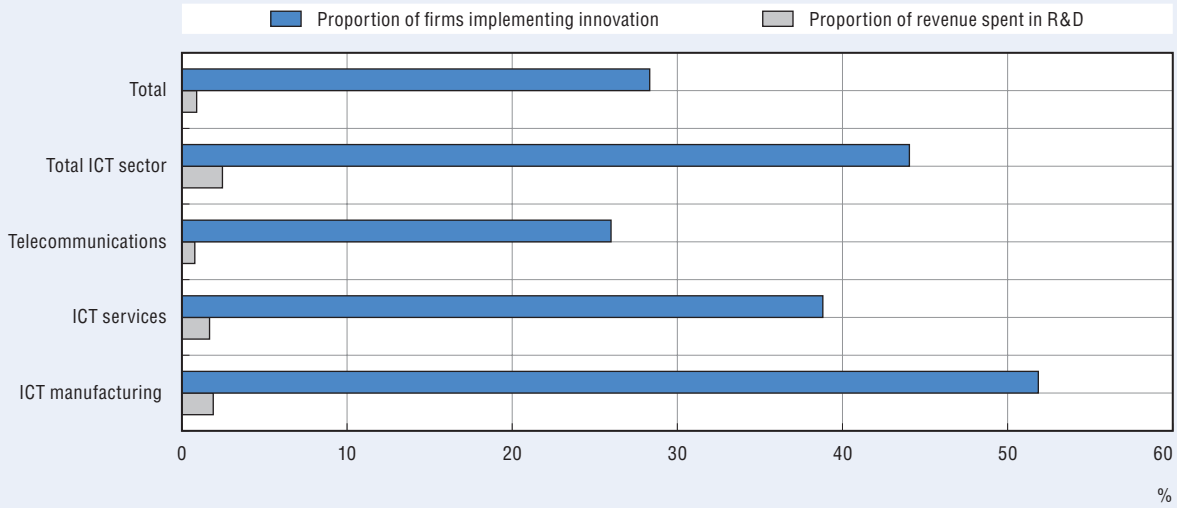
Growth of ICT sector and sub-sectors employment in Brazil



Source: Official statistics from the Brazilian Institute of Geography and Statistics (IBGE, 2014).

StatLink http://dx.doi.org/10.1787/888933224518

Innovation and R&D in Brazilian firms, 2011



Note: Based on national sources with the ICT sector and sub-sector aggregated by the OECD.

Source: Official statistics from the Brazilian Institute of Geography and Statistics (IBGE, 2013).

StatLink http://dx.doi.org/10.1787/888933224523

2.2 Communication market size and network development

This section examines developments in communication infrastructure and network performance. More robust and better performing networks and wider coverage assist in providing a reliable platform to facilitate economic and social interactions in modern societies. In particular, broadband networks, whether fixed or mobile, have become critical infrastructures that need to be accessed ubiquitously, at competitive prices and at sufficient speeds. In that respect, measuring the development of networks in terms of coverage, speeds or other quality parameters remains crucial to assessing the readiness of countries to support the increasing capacity demands from applications and services on the Internet.

Telecommunication industries in the OECD accounted for 21% and 17% of total value added and total employment, respectively, in 2013. Between 2012 and 2014, communication markets in the OECD area remained relatively stable in terms of overall subscriptions, penetration levels, revenues and investment. The decrease in fixed telephone subscriptions was offset by growth in wireless broadband subscriptions, which increased by 14% per annum, a lower rate than in previous years.

Fixed broadband subscriptions experienced modest growth levels, increasing 3.6% per annum between June 2012 and June 2014. However, fibre increased its share of total fixed broadband subscriptions to 16.5% in June 2014. Average fixed broadband penetration in the OECD area was 27 subscriptions per 100 inhabitants in June 2014, but reached over 40 subscriptions in Denmark, the Netherlands and Switzerland. Japan and Korea were clear outliers in terms of fibre-to-the-home (FTTH) penetration with over 71% of broadband subscriptions. Over 2012-14, large OECD countries doubled fibre penetration every year (e.g. Australia, Chile, Mexico, New Zealand and Spain), albeit from relatively small bases.

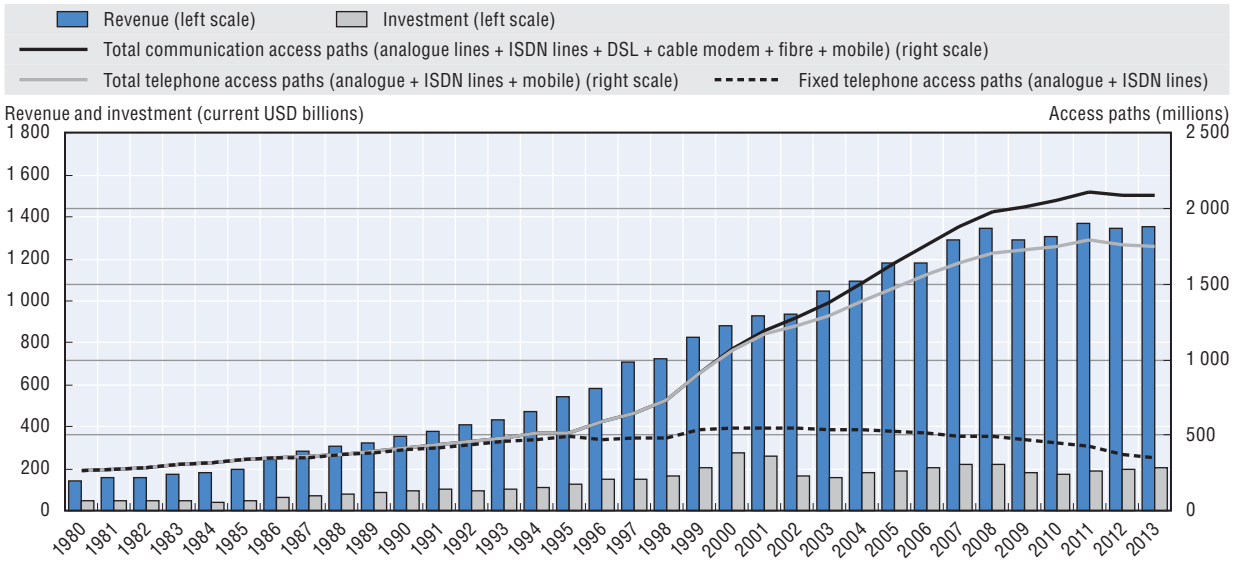
In addition to reporting fixed broadband penetration, OECD countries have started to publish data on broadband uptake by advertised speed tiers. Average broadband penetration was 15.07 lines per 100 inhabitants for speeds above 10 Mbps, and 5.83 lines for speeds above 25/30 Mbit/s. In June 2014, average wireless broadband penetration reached 78.23 subscriptions per 100 inhabitants in the OECD area, with Australia, Denmark, Finland, Japan, Korea, Sweden and the United States exceeding one subscription per inhabitant. The compound average growth rate for June 2012 to June 2014 was 14.22%, well below the 20%-30% growth rates found in preceding years.

Revenue and investment levels remained relatively stable with an overall telecommunication turnover in the OECD area of USD 1.353 trillion, just below the 2011 level of USD 1.372 trillion, while investment stabilised at about 14.5% of total turnover. Breaking down investment levels by technology remains a challenge. The increasing capacity and coverage of the fixed networks used to feed new 4G mobile networks are blurring the borders between fixed and mobile networks, with fibre networks at the backhaul and backbone segments being used for both fixed and mobile communications (Figure 2.21). This trend is expected to increase in coming years as fixed mobile converged offers gain momentum in OECD countries.

Between 2012 and 2014, Internet traffic continued to grow, although at a slower pace than in previous years. Globally, Internet traffic grew by 20% in 2013, compared to 40% from a smaller base over the 2005-09 period. Mobile data represent a growing share of Internet traffic, although their relative importance in global IP traffic remains small.

After many years of co-ordinated effort, IPv6 usage experienced considerable growth over the past two years, although starting from a very low base, with operators in selected countries implementing ambitious deployment initiatives. Following IPv4 depletion in all regional registries, with the exception of Africa and North America, the IPv6 user ratio reached over 30% in Belgium and over 10% in Germany, Luxembourg, Norway, Switzerland and the United States. This represents a remarkable achievement, as in 2012 the most advanced country in this respect was France with a user ratio of less than 5%. Despite these gains, the share of traffic using IPv6 remains small at approximately 3.5%, as of April 2014. Further efforts are clearly needed to achieve significant levels of IPv6 usage.

Figure 2.21. **Trends in telecommunication revenue, investment and access paths, 1980-2013**



StatLink http://dx.doi.org/10.1787/888933224551

In a context of stable revenues and investment, the performance of communication networks has continued to increase dramatically. In addition to fast deployment of long-term evolution (LTE) technology, fixed and mobile operators are pushing fibre technology closer to the end user, either through backhaul or access networks. In the OECD area, advertised download broadband speeds for the operators retained in the dataset were 23.65 Mbit/s for DSL technology, 56.68 Mbit/s for cable and 124.59 Mbit/s for fibre subscribers.

Actual broadband speeds can differ from advertised speeds significantly. Measuring quality of service and download and upload speeds, in particular, requires a number of methodological choices linked to the choice of available tools. This section has retained a number of data sources (Google's MLab, Akamai and Ookla) that provide statistics on actual broadband speeds. Official measurements are also emerging in the OECD area; for example, the European Commission (since 2012) and the FCC in the United States (since 2011) are both measuring actual broadband speeds (EU, 2014; FCC, 2014).

To ensure service expansion and adoption, policy makers need to maintain communication prices at affordable levels that promote uptake by a large majority of the population and do not impose an unfair burden on consumers and businesses. Since the early 1990s, the OECD has been measuring communication prices by constructing consumption patterns that mirror services purchased by consumers and businesses.

Throughout the years, the OECD has developed communication baskets for fixed telephony, mobile telephony, fixed and wireless broadband, and leased lines. More recently, the OECD has been looking at ways to develop communication price baskets for bundles of services, in view of the growing importance of bundles in today's communication markets. The OECD has recently modified its fixed broadband baskets to accommodate higher speeds and to bring them in line with existing speed tiers for benchmarking penetration. The new speed tiers are defined in terms of advertised download speeds: higher than 256 Kbit/s (basic broadband), higher than 1.5/2 Mbit/s, higher than 10 Mbit/s, higher than 25/30 Mbit/s, higher than 100 Mbit/s, and equal or higher than 1 Gbit/s.

Fixed broadband prices per megabit per second of advertised download speed decreased significantly between 2012 and 2014, largely due to increases in speeds rather than absolute declines in prices. In September 2014, broadband plans with prices below USD 0.75 per megabit per second of advertised speed were available in every OECD country, although only in the largest cities in some cases.

Prices for mobile services (telephony, SMS and broadband) have decreased dramatically, with a few exceptions. On average across OECD countries, prices for mobile broadband baskets for smartphones have declined between 13% and 52%. These declines are more significant for higher consumption baskets, which may be a natural outcome of lower termination rates and larger buckets of minutes and data offered by communication providers.

Network development

At the end of 2013, the total number of communication access paths in the OECD area was just below 2.1 billion, approximately the same level as in 2011, of which 67% were mobile subscriptions. For the first time since the OECD began collecting statistics on the number of access paths, the number has remained stable, declining slightly between 2011 and 2013. These aggregate numbers do not take into account wireless broadband subscriptions bundled with mobile plans, as these are considered a single communication access path. Wireless broadband subscriptions for laptops and tablets and smartphones that necessitate a separate subscription or payment (dedicated mobile broadband subscription) are counted separately.

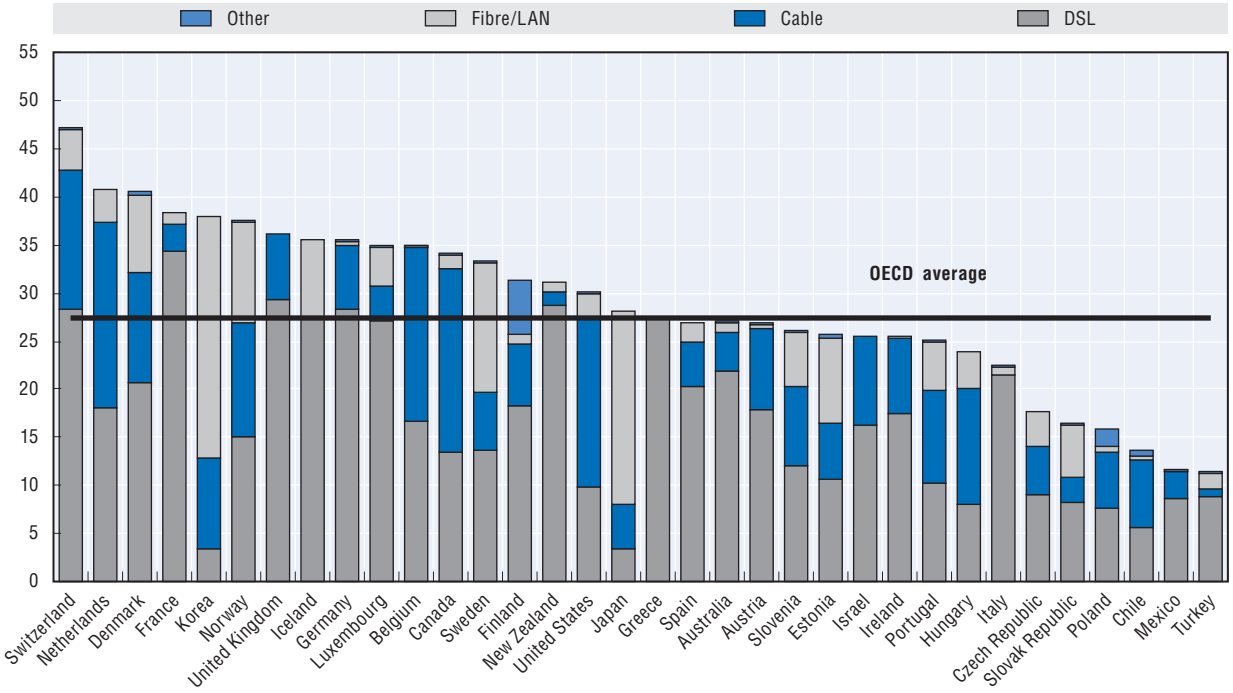
In most OECD countries, mobile voice markets have reached maturity, at least in terms of penetration rates. Growth in mobile subscriptions was 1.59% compound annual growth rate (CAGR) between 2012 and 2014, which did not offset the continuous decline in fixed telephone lines. Between 2012 and 2014, fixed broadband subscriptions also grew at the modest rate of about 3-4% per annum. Over the same period, decline in the number of fixed telephone access paths accelerated (10% per annum), a downward trend that started after penetration peaked in 2001 (CAGR was minus 4.23% between 2003 and 2013). This trend underscores the increasing substitution of fixed mobile and possibly the replacement of traditional voice fixed telephony services by over-the-top applications, such as Skype, Viber or FaceTime. Certainly, the higher penetration of fixed and mobile broadband provides a substantial opportunity for substitution.

Mobile subscriptions per 100 inhabitants have remained relatively stable. Average mobile penetration in the OECD was 111.4 lines per 100 inhabitants at the end of 2013 and some countries have even experienced slight declines. For example, the Czech Republic, Spain and Luxembourg experienced yearly declines of 1%, 2.1% and 3.5%, respectively, over the period 2012-14. These reductions in mobile subscribers may be due to decreases in prepaid subscriptions (representing 38.34% of mobile subscriptions, down from 42.6%

in 2009) and reductions in termination rates, which have considerably reduced off-net/on-net price differentials in most countries. This has rendered the use of SIM cards from different operators to avoid high off-net charges less attractive. Moreover, some operators may have re-evaluated existing criteria that count a prepaid SIM card as an active customer. Finally, the emergence of "roam like at home" offers in some European countries has diminished the incentive for users to purchase foreign SIM cards when travelling to another country on a regular basis.

The growth rate in communication access paths, broken down by technology, provides an interesting overview of developments between 2012 and 2014. Wireless broadband subscriptions maintained a healthy growth rate of 18.14% (dedicated mobile broadband) and 13.61% (standard mobile broadband) per annum. Fixed broadband subscriptions grew on average by 3.7% per annum, but experienced very different growth rates depending on the underlying technology. Strong growth in fibre subscriptions (CAGR 11.79%) indicates that FTTH technology is gradually replacing DSL and cable broadband services. Not surprisingly, DSL subscriptions experienced a very low increase in relative terms (CAGR 0.4% in the same period), whereas cable grew at a moderate rate (5.49% year on year). This is the outcome of DSL networks being more easily replaced by FTTH, as opposed to the smaller replacement rate for cable networks, for which DOCSIS 3.0 is more mature and provides higher speeds than deployed VDSL technologies (see Chapter 1, Figure 1.12).

Figure 2.22. **OECD fixed (wired) broadband subscriptions per 100 inhabitants by technology, June 2014**



Note: Fibre includes FTTH/B/P and excludes FTTC.

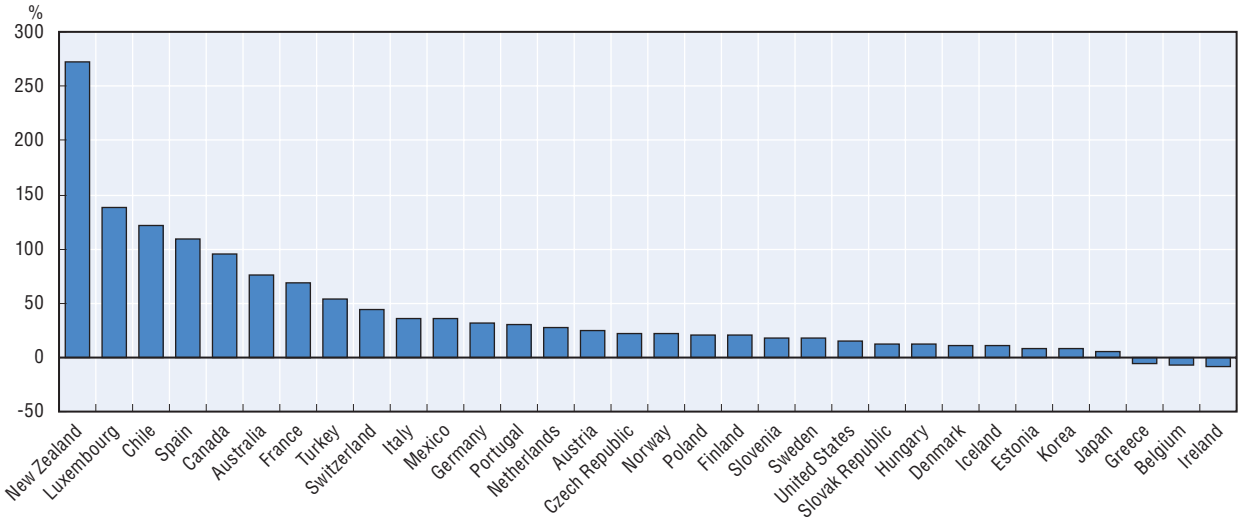
StatLink http://dx.doi.org/10.1787/888933224566

In June 2014, average fixed (wired) broadband penetration in the OECD area was 27 subscriptions per 100 inhabitants (Figure 2.22). The highest penetration levels were found in Switzerland (47.3 subscriptions), the Netherlands (40.8) and Denmark (40.6).

DSL was the most widely used technology (51.54% of subscriptions), although its share is diminishing, as is that of cable (31.36%). Conversely, fibre subscriptions are increasing (16.46%) and are gradually replacing other technologies (Figure 2.23). Between June 2012 and June 2014, annual growth (CAGR) of broadband penetration in OECD countries was 3.66%, with a few countries experiencing higher growth rates, including Greece (18.12%), followed by Chile, Ireland, Mexico and Switzerland (all between 14% and 15%).

Between 2012 and 2014, some OECD countries with relatively low fibre broadband penetration rates have experienced remarkable growth rates. Yet, in most cases these countries will need several years to achieve the fibre penetration levels of the most advanced countries, Japan (71.5% of fixed broadband subscriptions) and Korea (66.3%). New Zealand (272%), Luxembourg (139%) and Chile (122%) achieved the highest growth rates between June 2013 and June 2014 (Figure 2.23), while large OECD countries such as Australia, France, Spain and Turkey achieved growth rates of between 180% and 290% over the same two-year period.

Figure 2.23. **Growth of fibre connections among countries reporting fibre subscriptions, June 2012 – June 2014**



Note: Fibre includes FTTH/B/P and excludes FTTC.

StatLink http://dx.doi.org/10.1787/888933224576

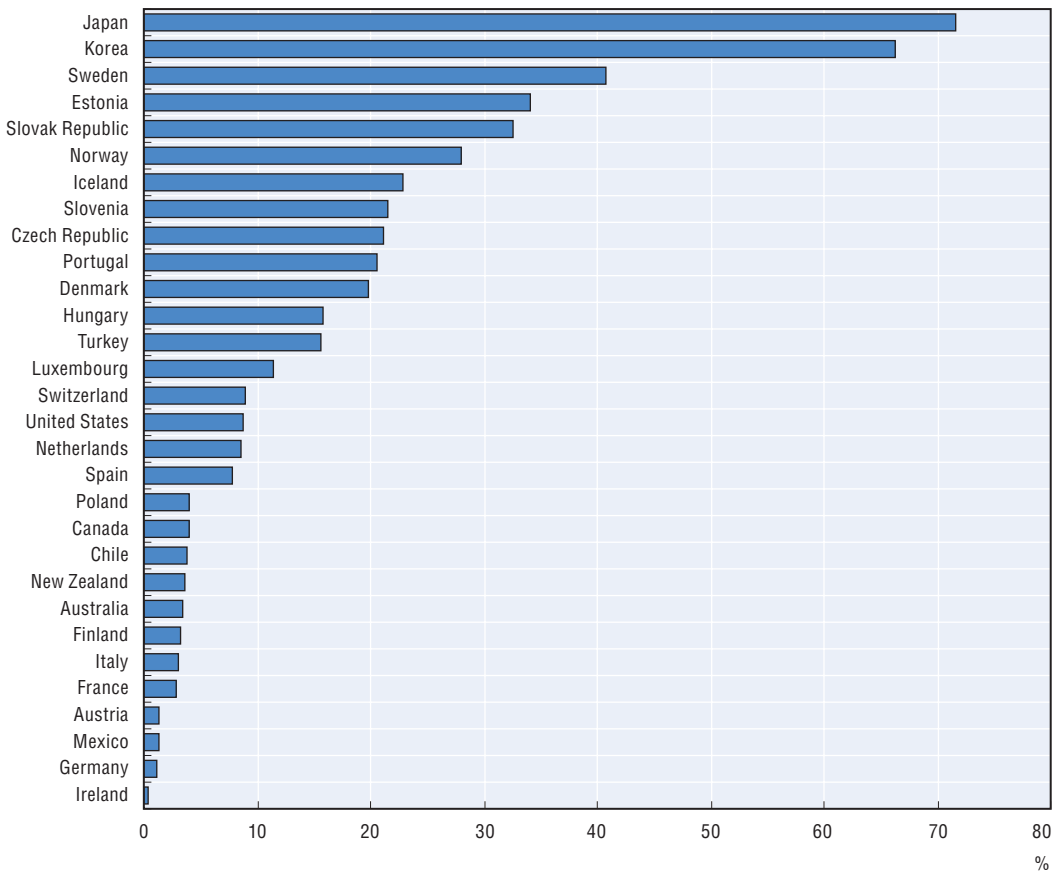
In conclusion, the transition from copper and cable to fibre is occurring at a gradual pace, despite increasing adoption of FTTH technology in large OECD countries. At present, only 14 OECD countries have more than 10% of broadband subscriptions with FTTH technology (Figure 2.24). While the OECD methodology only counts subscriptions consisting of FTTH, FTTB (fibre-to-the-building) or FTTP (fibre-to-the-premises) as "fibre", some countries may also include FTTC (fibre-to-the-cabinet) or cable (DOCSIS 3.0) subscriptions, which calls for a level of caution in interpreting these results. Moreover, technologies such as DOCSIS 3.0 can deliver high speeds without qualifying as "fibre" under the OECD methodology.

Wireless broadband subscriptions are experiencing remarkable growth across the OECD area, although growth slowed between 2012 and 2014. The annual growth rate (CAGR) between June 2012 and June 2014 was 14.23%, below the 20%-30% growth rates of previous years from a lower base. These rates need to be considered carefully as, in some cases, actual implementation of the OECD methodology used to count wireless broadband subscriptions

may have significant effects on the measurement of penetration rates. Nevertheless, the methodology, first implemented in 2009, is sufficiently mature to provide a good view of service penetration and growth in OECD countries.

In June 2014, average wireless broadband penetration in the OECD area was 78.23 subscriptions per 100 inhabitants, with a few countries exceeding one subscription per inhabitant: Finland (131.58), Japan (116.4), Australia (115.23), Sweden (113.19), Denmark (111.56), Korea (105.27) and the United States (101.43). The total number of wireless broadband subscriptions reached 983 million in June 2014, including standard mobile subscriptions, dedicated data subscriptions, and fixed wireless and satellite subscriptions, the latter accounting for a much lower share of the total (Figure 2.25).

Figure 2.24. **Percentage of fibre connections in total fixed broadband subscriptions, June 2014**



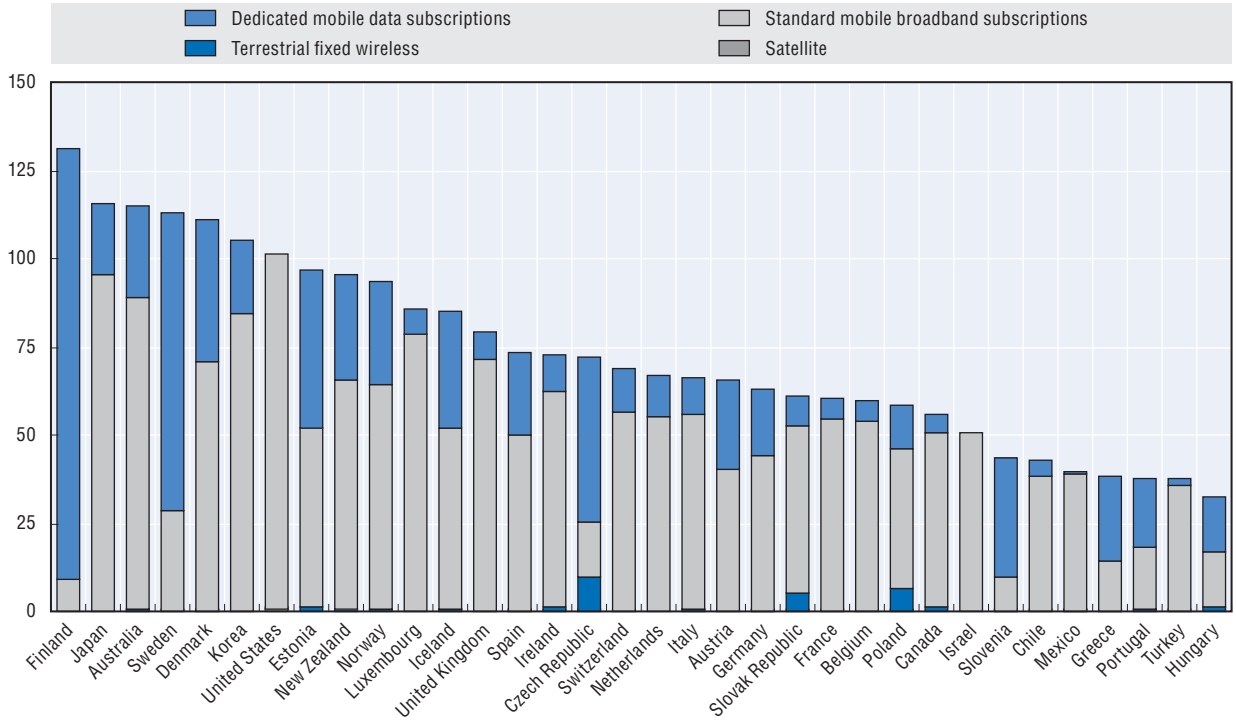
Note: Fibre includes FTTH/B/P and excludes FTTC.

StatLink http://dx.doi.org/10.1787/888933224587

Broadband speeds and quality of service

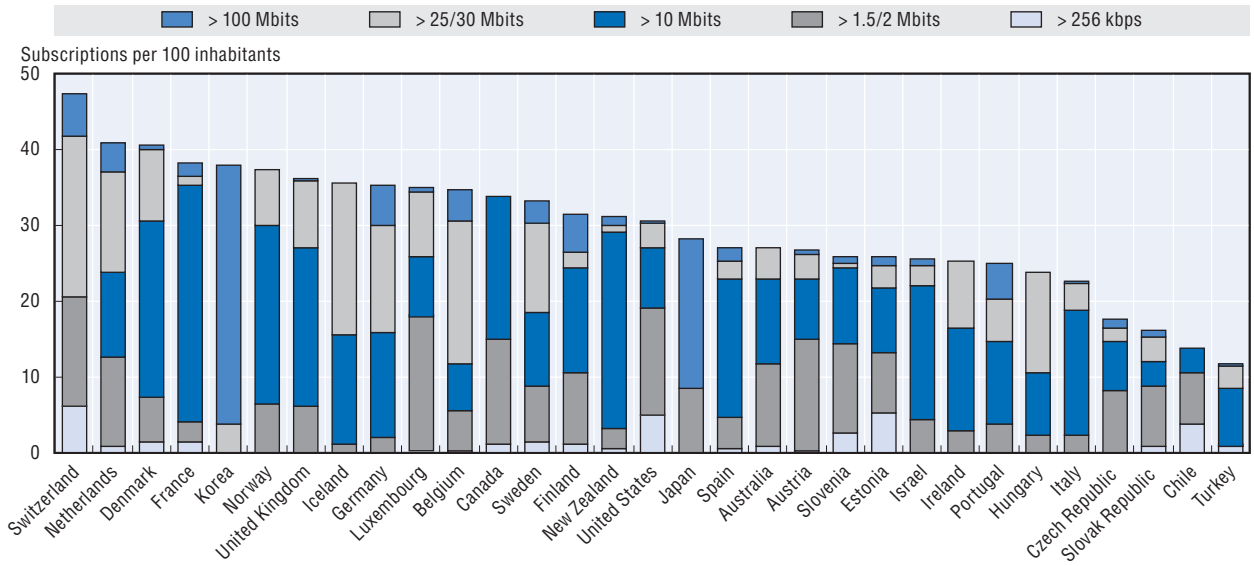
In 2012, the OECD adopted a harmonised set of tiers to report advertised download broadband speeds. They can be used for broadband statistics on both prices and penetration. The tiers break down broadband subscriptions into those with advertised speeds higher than 1 Gbit/s, 100 Mbit/s, 25/30 Mbit/s, 10 Mbit/s, 1.5/2 Mbit/s and subscriptions not fulfilling these speed requirements but still qualifying as a broadband service (at least 256 Kbit/s of advertised download speed). Most OECD countries have used this breakdown to report broadband subscriptions (Figure 2.26).

Figure 2.25. **OECD wireless broadband subscriptions per 100 inhabitants, by technology, June 2014**



StatLink http://dx.doi.org/10.1787/888933224593

Figure 2.26. **Fixed (wired) broadband penetration by speed tiers, June 2014**



Notes: For Japan, data are OECD estimates with tiers lower than 100 Mbits unseparated. They may also include an auxiliary portion of the top tier. For Korea, 10.0% refers to below 50Mbits and 90.0% refers to above 50 Mbits.

StatLink http://dx.doi.org/10.1787/888933224603

If an OECD fixed broadband penetration ranking were to be developed using only subscriptions with an advertised download speed of 10 Mbps or higher, the top countries would be Korea (37.9), Iceland (35.5) France (31.1) and Japan (28.2). If the ranking were to cover

speeds higher than 25/30 Mbps, the leaders would be Korea (37.9), Japan (28.2), Switzerland (21.2) and Iceland (19.9). Regarding subscriptions of 100 Mbps or higher download speeds, Korea and Japan are clear leaders with a far higher penetration than any other OECD country. These numbers allow an OECD average broadband penetration to be derived for speeds higher than 10 Mbps (12.6) and higher than 25/30 Mbit/s (7.3), still well below the OECD average fixed broadband penetration of 27 subscriptions per 100 inhabitants.

A different way to examine advertised speeds is to calculate the advertised speeds of broadband plans in OECD countries, even though these do not provide information on the distribution of consumers across speed tiers (actual take-up rates by speed). Notwithstanding these challenges, these statistics provide a good overview of the types of plans being marketed to consumers (restricted to residential broadband). Figure 2.27 includes both median and average advertised speeds of broadband plans, broken down by country. Even though average speeds are also informative, median speeds provide a more reliable view of advertised plans, as the average may differ greatly, especially in the presence of 1 Gbit/s offers. Sweden (100 Mbit/s), the Netherlands (95 Mbit/s) and Korea (75 Mbit/s) have the highest median download speeds in the OECD area. Slovenia and Mexico (15.36 Mbit/s) have the lowest median speeds. In the case of Slovenia, the results may be reduced slightly by multiple offers, with different upload and download speed combinations at entry level, whereas higher speeds only offer one or two different options per speed tier. The fixed average OECD median speed has increased markedly, from 20.48 Mbit/s in 2011 to 30 Mbit/s at the end of 2013 (Figure 2.27). Additional data on fixed broadband upload speeds in the OECD area, available on a per country basis, can be consulted online.[2]

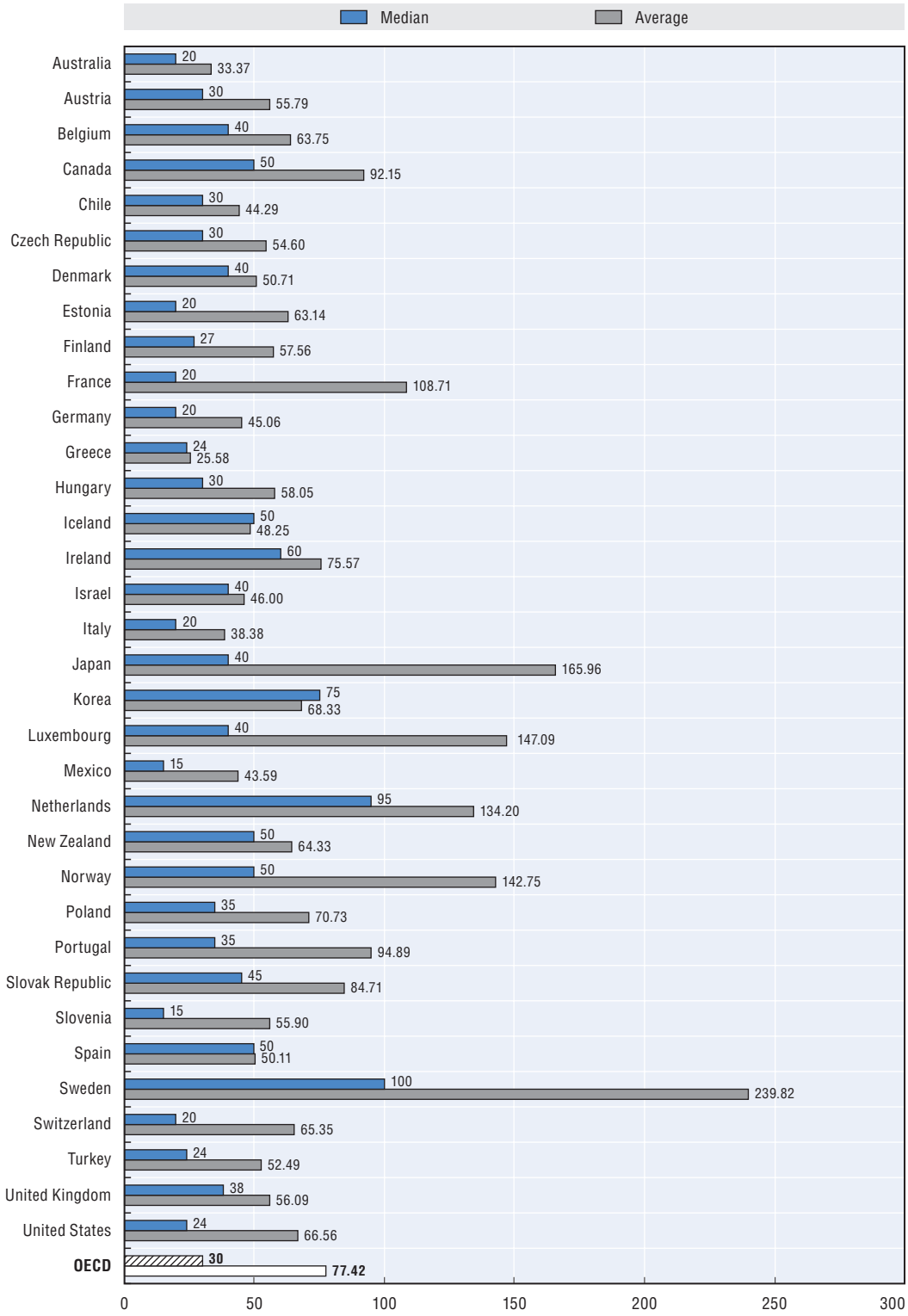
An alternative way to look at fixed broadband download speeds is to separate the different access technologies. This exercise is not without its challenges, as in many cases it may not be easy to ascertain which high-speed offers fall under the categories of "fibre" (FTTH), cable or DSL technologies. Many operators advertised VDSL and DOCSIS 3.0 technology as "fibre" and the state of deployment may vary across different areas within a country. In September 2012, average download speeds were 16.54 Mbit/s (DSL offers), 44.14 Mbit/s (cable subscriptions) and 89.03 Mbit/s (fibre plans). By September 2014, download and upload speeds had increased significantly (Figure 2.28).

Between 2012 and 2014, mobile broadband network performance improved considerably due to LTE deployments. According to Teligen/Strategy Analytics data from September 2014, 21 out of 34 OECD countries had at least one mobile operator offering mobile broadband download speeds for laptops and tablets of 100 Mbit/s, in terms of theoretical advertised speeds (those reached under very specific conditions, especially with regard to the number of users in a cell, distance to a tower and so forth). In September 2012, only eight OECD countries had an operator offering comparable speeds (Figure 2.29).

Actual broadband speeds

Policy makers and regulators have expressed increasing concern regarding the quality of service experienced by consumers, which can differ significantly from that inferred from advertised speeds. In addition to potential gaps between actual and advertised broadband speeds, other quality parameters, such as delay and jitter (delay variation), may affect the end user experience. In this regard, measuring quality of service, and actual speeds in particular, gives rise to a broad range of technical choices, which may affect the results. Accordingly, some stakeholders have developed tools for measuring performance.

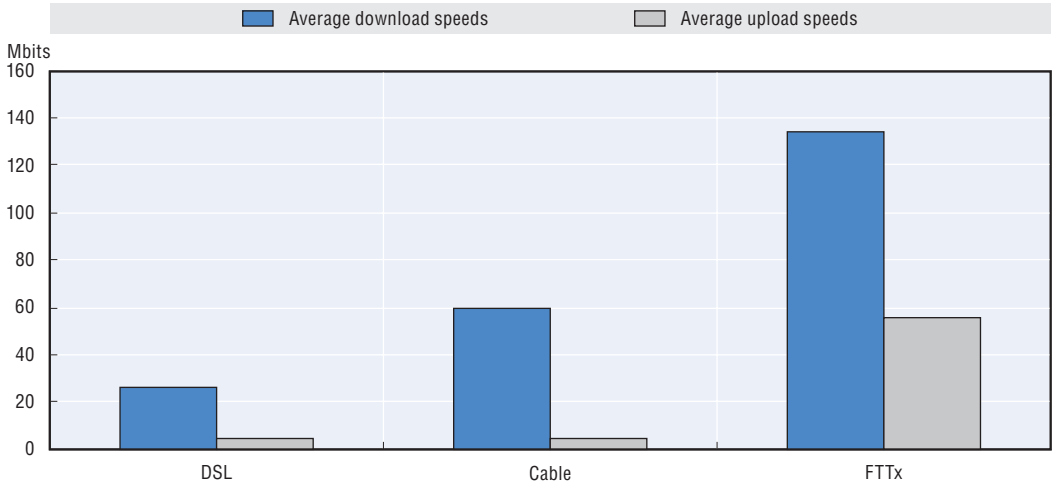
Figure 2.27. **Average and median advertised download speeds, fixed broadband, September 2014**



StatLink http://dx.doi.org/10.1787/888933224610

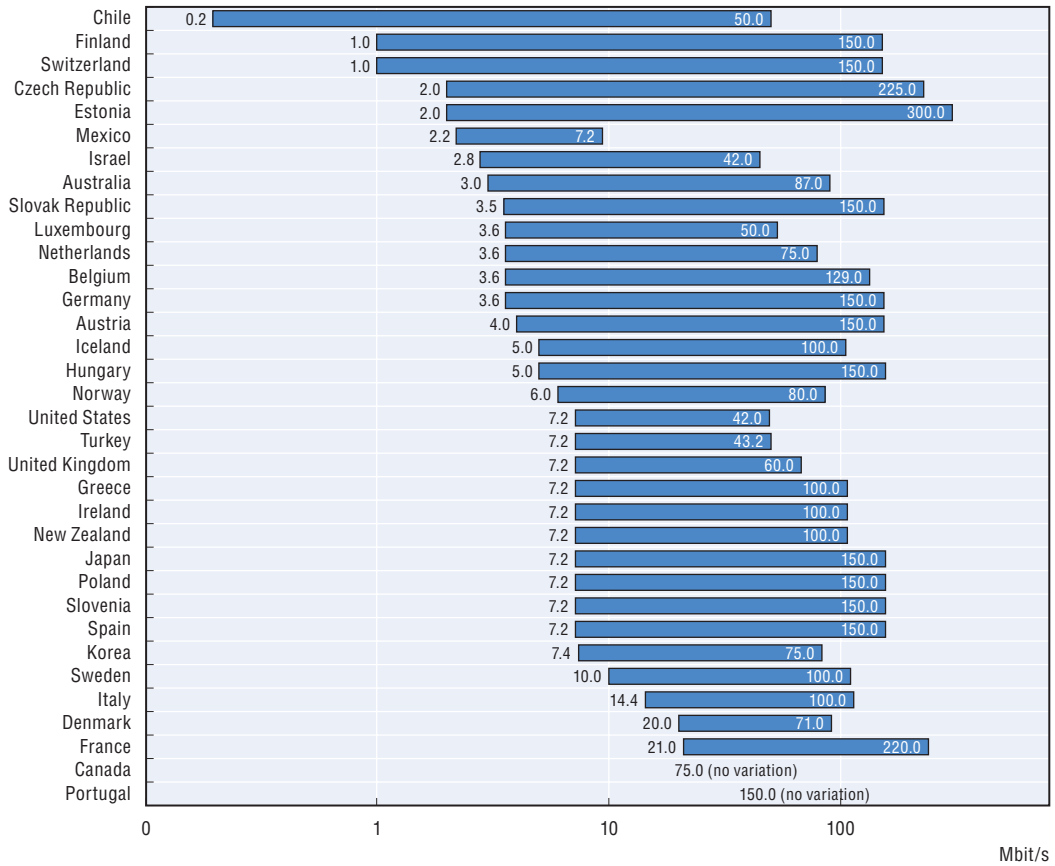
Akamai, M-Lab and Ookla, for example, are all initiatives that take different approaches to measuring and publishing actual broadband speed indicators for a wide range of countries (see Figure 2.30).[3]

Figure 2.28. **Average advertised download and upload speeds, fixed broadband by technology, September 2014**



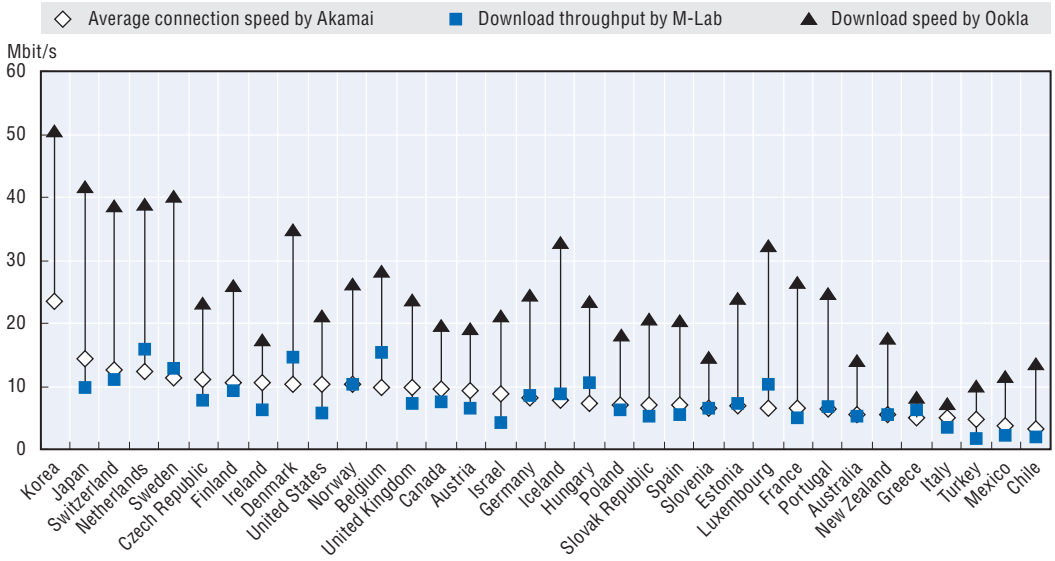
StatLink http://dx.doi.org/10.1787/888933224628

Figure 2.29. **Mobile broadband advertised speed ranges, logarithmic scale, September 2014**



StatLink http://dx.doi.org/10.1787/888933224638

Figure 2.30. **Actual download speeds, fixed or unspecified broadband, Akamai, M-Lab and Ookla, Mbit/s**



Sources: Akamai [*www.akamai.com*], M-Lab [*www.measurementlab.net*] and Ookla [*www.ookla.com*]. Data collected in the 1st quarter of 2014.

StatLink http://dx.doi.org/10.1787/888933224641

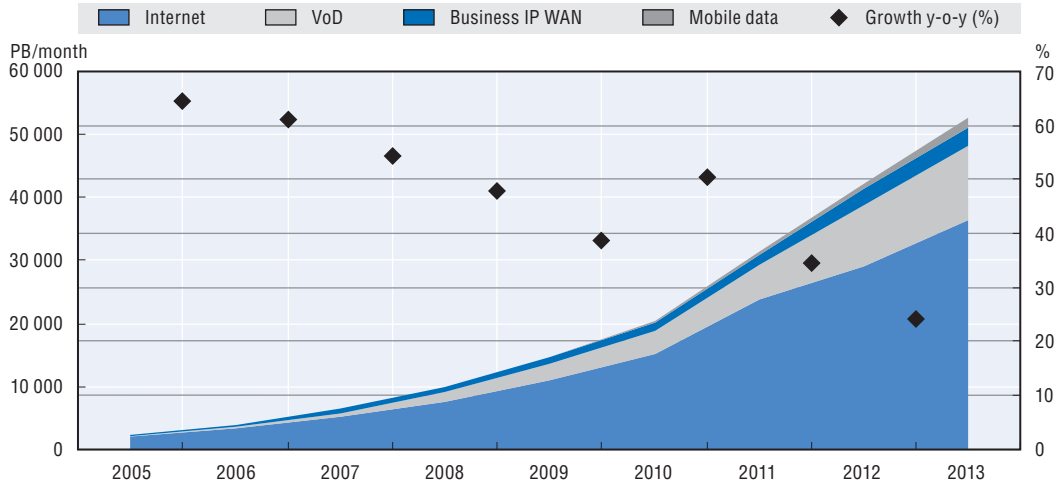
In some cases, the underlying technologies are not evident, although Akamai has recently improved its methodology to identify and exclude mobile broadband users from its average connection speed metrics. Ookla reports measurements separately by mobile applications, although its data may still include tests conducted from Internet browsers on mobile devices. M-Lab data do not specify which type of networks are measured, but most of its speed tests appear to have been conducted on fixed networks, according to other data reported, such as the round trip time.

The OECD report *Access Network Speed Tests* (OECD, 2014c) examined official measurement approaches taken in OECD countries and challenges encountered when pursuing a harmonised approach. The report provided a classification of these approaches together with suggestions on how they may be selected and implemented depending on different policy goals. Actual speed measurement is becoming an important tool, as it provides data to inform various policy areas such as consumer empowerment, network development and competition. Official measurement tools can also overcome possible selection biases (i.e. users more interested in service quality are likely to perform more speed tests than the average user).[4]

Internet traffic

According to Cisco's Visual Networking Index (VNI), global Internet traffic continued to grow in 2012-14, reaching 51.2 Petabytes (PB) in 2013, up from 30.7 PB in 2011 and 14.7 PB in 2009. Although total IP traffic is still growing at double-digit rates, growth slowed considerably between 2011 and 2013. In 2013, growth of total IP traffic was 24% per annum, considerably lower than in 2012 (39%) or 2007 (61%). In 2013, mobile data growth was 81% year-on-year, lower than the 140%-160% growth rates measured between 2008 and 2011 (Figure 2.31). Even though global and mobile Internet traffic are still growing at extraordinary rates, the lower growth rates presented here may reflect approaching maturity in Internet adoption, with over two thirds of the population in many OECD countries now using the Internet.

Figure 2.31. **Global IP traffic, 2005-13**



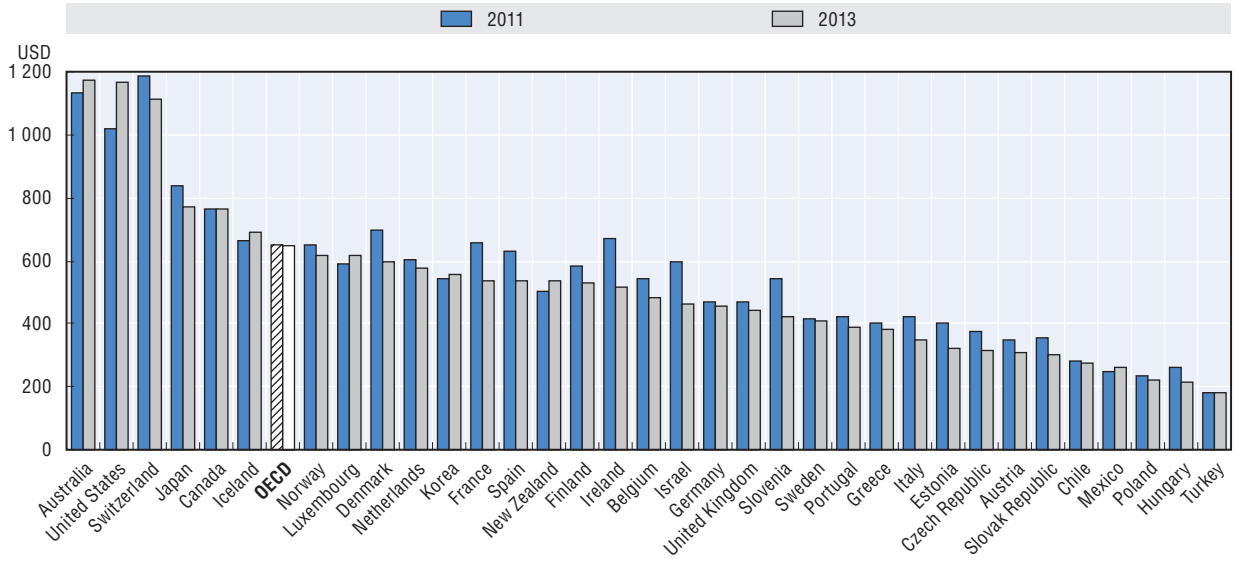
Source: Cisco, October 2014. *www.cisco.com*.

StatLink http://dx.doi.org/10.1787/888933224651

Industry revenues and investment

As noted earlier, telecommunication revenue remained stable in the OECD area in 2012-14, at an overall turnover of 1.353 trillion, slightly below the 2011 level of 1.372 trillion. In terms of communication revenue per access path, the downward trend observed in 2000-10 has now stabilised. Revenue declined progressively from USD 823 per access path in 2000 to USD 629 in 2009, but increased to USD 648 in 2011, the same level as 2013. Some countries such as Australia and the United States have experienced positive growth, whereas in most OECD countries revenue per communication access paths declined between 5% and 10% (see Figure 2.32).

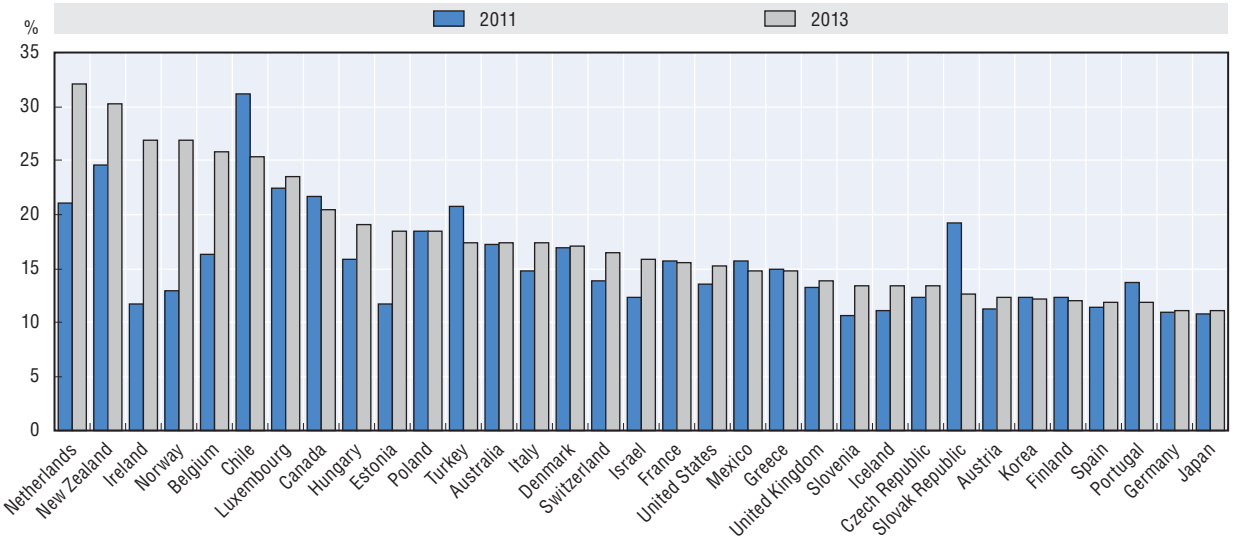
Figure 2.32. **Telecommunication revenue per communication access path, 2011 and 2013**



StatLink http://dx.doi.org/10.1787/888933224666

In a context of stable revenues, telecommunication investment has increased steadily following the 2009 financial crisis, growing from USD 190.5 billion in 2011 to USD 196.7 billion in 2013. Investment as a percentage of communication revenues also remained fairly stable between 2011 and 2013, with a slight increase from 13.9% (2011) to 14.5% (2013) on average in the OECD area. The highest levels correspond to the Netherlands (32.1%) and New Zealand (30.3%) where nationwide fibre networks are currently being deployed (Figure 2.33). An alternative measure, presented in the tables online,[5] is investment per capita or per access path.

Figure 2.33. **Investment in telecommunications as % of total revenues, spectrum fees excluded, 2011 and 2013**



StatLink http://dx.doi.org/10.1787/888933224673

Price benchmarking statistics

An important driver of adoption is affordability. Over the years, the OECD has developed communication price baskets in order to produce a comprehensive set of indicators to inform policy makers about the affordability of communication services and, more generally, to provide a view on the efficiency of the industry. From all the baskets available for the different services (i.e. fixed and mobile telephony, fixed and mobile broadband and leased lines), only some examples are included in this section. Data for all OECD communication baskets are provided online.[6] This section highlights fixed and wireless broadband baskets, given the importance of broadband services to the digital economy. In addition, it also discusses current efforts to develop a basket of bundled services, reflecting the increasing popularity of bundled communication services among consumers.

Figures and text on communication prices in this report are based on purchasing power parity (PPP) terms, which provide a better view of actual prices faced by consumers relative to domestic prices for goods and services. The tables available online[7] report prices in exchange rate and PPP terms and in nominal exchange rates (USD), to provide a comprehensive view of prices for telecommunication services. The OECD uses purchasing power parities to overcome two deficiencies associated with using nominal exchange rates

to compare price baskets across countries. First, exchange rates vary from day to day and sometimes change abruptly. Second, exchange rates do not simply reflect the relative prices of goods and services produced in a country, since they are affected by the relative prices of tradable goods and by factors such as interest rates and financial flows. Price indicators should also be analysed in conjunction with other indicators such as penetration, performance and efficiency indicators, included in this report. The main drawback of PPPs is difficulty with measurement.

Fixed broadband services

Following OECD workshops on broadband metrics held in 2011 and 2012, existing fixed broadband baskets were amended to account for recent changes in consumption patterns and to align them with broadband speed tiers for broadband penetration data. Accordingly, the new service speed tiers are: baseline broadband (higher than 256 Kbps), higher than 1.5/2 Mbit/s, 10 Mbit/s, 25/30 Mbit/s, 10 Mbit/s, higher than 100 Mbit/s and higher than 1 Gbit/s. Each speed tier requires a minimum upload speed and has three different bandwidth usage profiles (Table 2.1).

Table 2.1. **Fixed broadband baskets, download speeds, minimum upload speed and bandwidth usage profile**

Service speeds		Bandwidth usage profile (in GB/month)		
Download speed (in Mbit/s)	Minimum upload speed	Low	Median	High
≤1.5/2.0	256 Kbit/sec	5	10	20
>1.5/2.0 –≤10	512 Kbit/sec	5	15	50
>10 –≤25/30	768 Kbit/sec	10	25	100
>25/30 –≤100	1 Mbit/sec	15	50	200
>100 -≤1 000	3 Mbit/sec	25	100	400
>1 000	10 Mbit/sec	100	250	1000

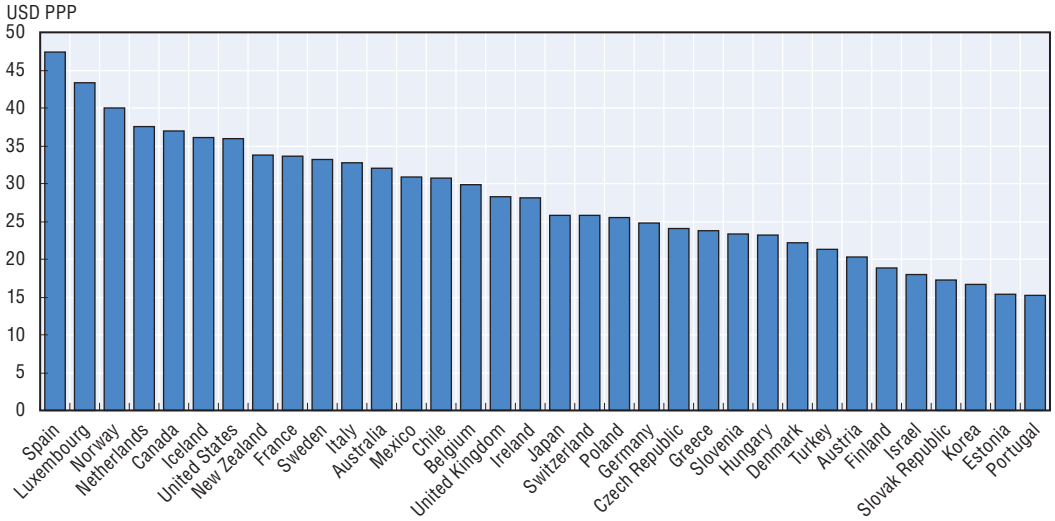
The results of the September 2014 fixed broadband baskets, as compiled by Teligen/Strategy Analytics for the OECD, are presented in tables online.[8] Two examples of these baskets are shown here: the low use 1.5/2 Mbit/s basket and the high use 25/30 Mbit/s basket (Figures 2.34 and 2.35). In line with the basket definitions, the minimum speed sampled for a given country and basket may be higher than the minimum requirements of that basket.

Price ranges (Figure 2.36) are a notable indicator of the tariffs consumers are paying, and of the diversity of broadband offers. Even thoug h minimum broadband subscription prices may be biased by the uptake of certain bundles, as in many countries no or very little standalone broadband is available, minimum prices do indicate the lowest possible price for subscribers to obtain access to broadband services, even at low speeds. Between September 2012 and September 2014 there was little change in this measure. The lowest entry prices ranged from USD 13 to USD 15 per month (e.g. Estonia, Portugal, Turkey), while the highest were around USD 40 per month (e.g. Luxembourg, Spain, Norway, Iceland). The average entry broadband price in the OECD area was USD 26.84, only USD 0.8 per month lower than in 2012.

A key variation in this indicator is the range of prices per Mbit/s, which takes into account a prominent quality characteristic of broadband services: advertised download broadband speed. Considering one quality characteristic (i.e. download speed) equates to a

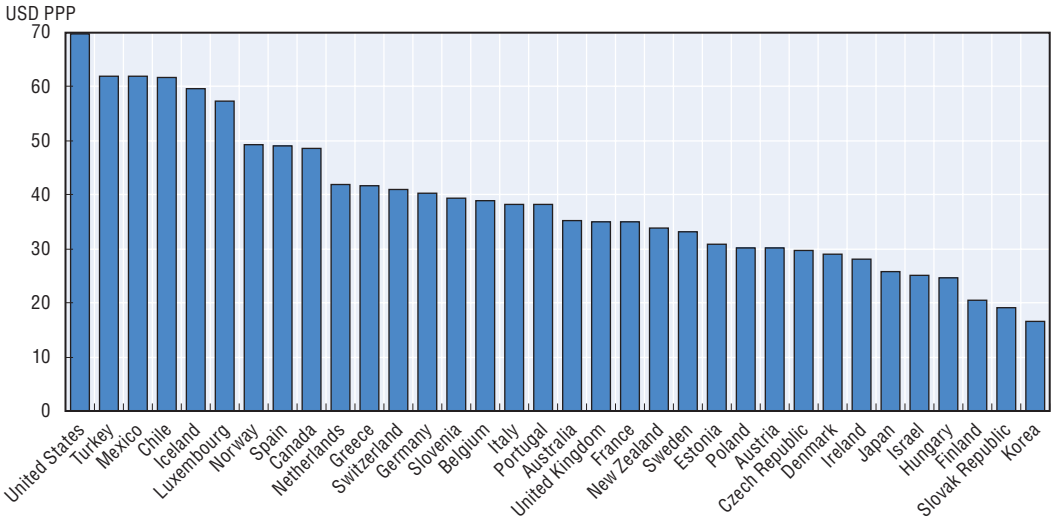
simplified version of hedonic price analysis. In general, the lowest entry prices per megabit per second of advertised speed correspond to those providers offering high speeds in the range of 200 Mbit/s, 500 Mbit/s or 1 Gbit/s.

Figure 2.34. **Fixed broadband basket, low use, >1.5/2 Mbps, USD PPP**



StatLink http://dx.doi.org/10.1787/888933224689

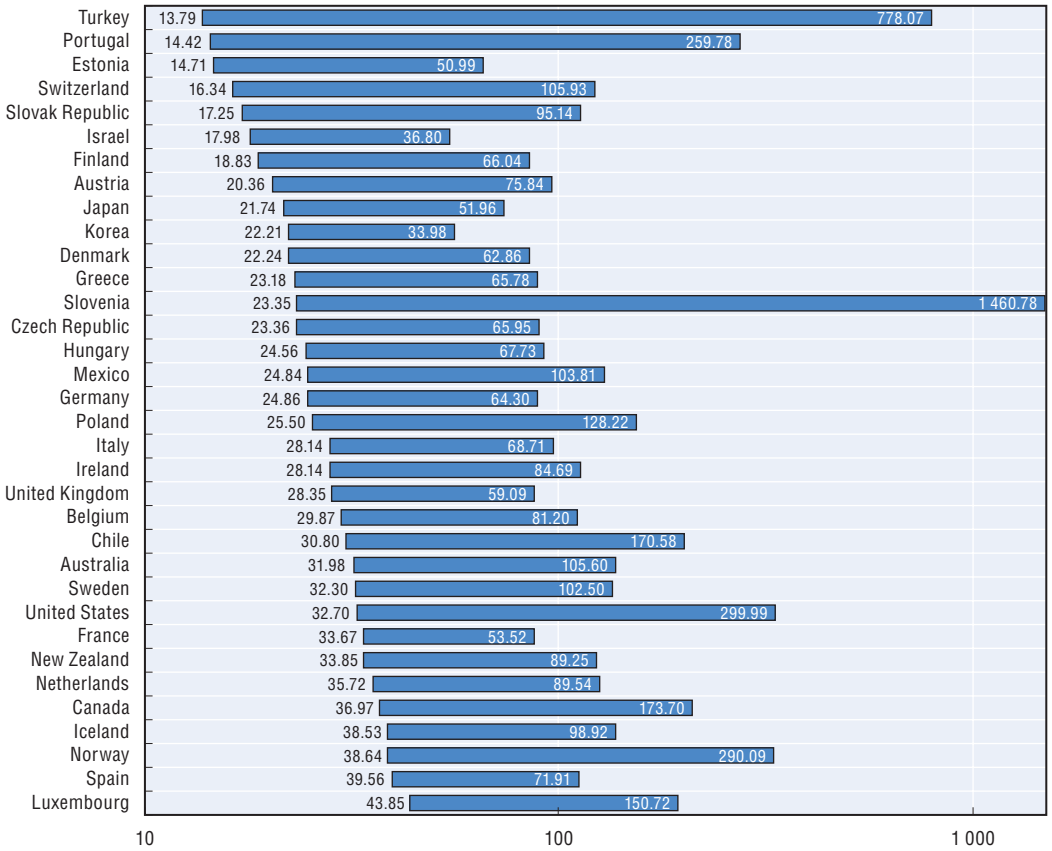
Figure 2.35. **Fixed broadband basket, high use, >25/30 Mbit/s, USD PPP**



StatLink http://dx.doi.org/10.1787/888933224696

Conversely, countries with lower broadband speeds also report higher prices per Mbit/s. Japan (USD 0.02), Sweden (USD 0.08) and France (USD 0.10) have the lowest prices per Mbit/s (Figure 2.37). Many countries have shown remarkable progress in bringing down entry prices per megabit per second. In 2012, three OECD countries had minimum prices over USD 1, whereas in September 2014, the most expensive country was Greece with USD 0.74. Certain counties have considerably reduced their entry prices, such as Mexico (from USD 1.69 to USD 0.52) and Israel (from USD 0.77 to USD 0.32). Operators in those countries have also started offering higher speeds, usually through fibre networks, even though these deployments may be restricted to the largest cities.

Figure 2.36. **Fixed broadband subscription price ranges, September 2014, all platforms, logarithmic scale, USD PPP**



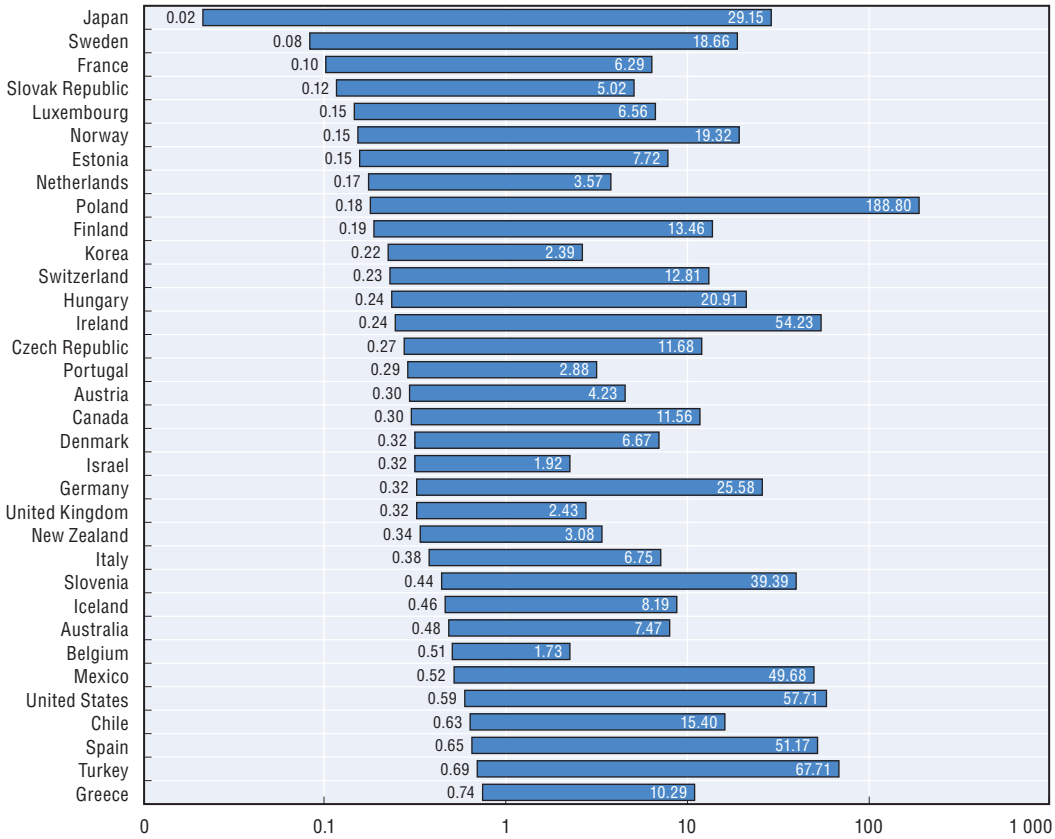
StatLink http://dx.doi.org/10.1787/888933224706

Wireless broadband baskets

The new OECD wireless broadband baskets include mobile broadband services for laptop, tablet and smartphone use, each with different parameters, as usage patterns are very different. Moreover, while laptop and tablet-based baskets are designed around a standalone service (mobile broadband only), smartphone baskets are designed as bundles (i.e. prices for a set of services, typically mobile voice, SMS and data), compared across countries and operators. These baskets reuse existing mobile voice and SMS baskets, adding the mobile broadband component. Accordingly, some of the baskets cover 30 calls plus 100 MB, 100 calls plus 500 MB, 900 calls plus 2 GB and so on.

Prices for mobile services have fallen markedly between 2012 and 2014. On average, prices for the 30 calls + 100 MB basket dropped by 10.24%, from USD 19.74 to USD 17.72 per month. Prices for the 100 calls plus 500 MB basket fell by 17%, the 300 calls plus 1 GB basket by 31%, the 900 calls plus 2 GB basket by 44%, and the 100 calls plus 2 GB basket by 15%. Countries that experienced the largest price declines were Italy (52% on average across all baskets), New Zealand (46%) and Turkey (44%), while prices in Canada, France, Ireland, Slovak Republic and Switzerland remained relatively stable. Prices increased in Austria (36%), following a merger from four to three operators, and Greece (13%) over the two-year period (Table 2.2).

Figure 2.37. **Fixed broadband prices per megabit per second of advertised speed, September 2014, USD PPP**



StatLink http://dx.doi.org/10.1787/888933224711

Unlike wireless broadband services for smartphones, which are considered within the mobile bundle for price benchmarking purposes, laptop and tablet-based mobile broadband are benchmarked as standalone services, according to different consumption patterns: 500 MB to 10 GB (for laptops) and 250 MB to 5 GB (for tablets). By way of example, in September 2014 the average price for laptop-based 2 GB wireless broadband baskets was USD 18.49 per month, for a price range in the OECD area between USD 5.89 (Finland) and USD 37.25 (Canada) (Figure 2.38).

Extending the OECD price basket methodologies to include communication bundles

The OECD price basket methodologies cover a wide range of services, but do not include bundles of services, with the exception of the mobile broadband baskets for smartphone use. This implies that bundled services may be included in the baskets in cases where the selected offer for a given country or operator includes a bundle of services, but, as a general rule service bundles are not compared with one another. The OECD report *Triple and Quadruple-play Bundles of Communication Services* (OECD, 2015) put forward, for the first time, a set of bundles for triple-play (fixed telephony, broadband and pay television) services and quadruple-play (triple-play plus mobile services) and benchmarked a number of large OECD countries. One of the most challenging aspects of this comparison is comparing pay television services, arguably the most heterogeneous component in triple and quadruple-play bundles. In this case, the criteria for including a package in the premium bundle

Table 2.2. **Mobile baskets, comparison between September 2012 and September 2014, USD PPP**

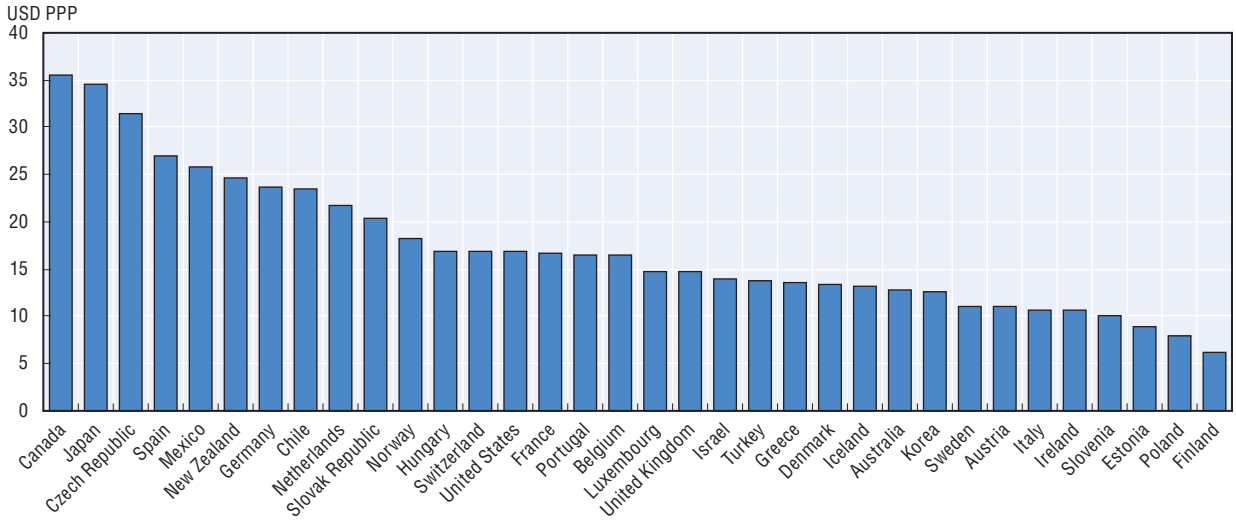
	30 calls + 100 MB		100 calls + 500 MB		300 calls + 1 GB		900 calls + 2 GB		100 calls + 2 GB		30 calls + 100 MB	100 calls + 500 MB	300 calsl + 1 GB	900 calls + 2 GB	100 calls + 2 GB
	2012	2014	2012	2014	2012	2014	2012	2014	2012	2014					
Australia	16.78	12.51	20.13	19.26	26.83	19.56	26.83	25.72	26.83	25.72	-25.46%	-4.32%	-27.08%	-4.14%	-4.14%
Austria	8.97	11.56	10.08	11.56	10.08	11.56	17.83	22.82	10.08	19.37	28.87%	14.73%	14.73%	28.01%	92.17%
Belgium	12.83	13.62	37.79	22.70	62.11	45.12	94.48	51.07	56.69	28.37	6.14%	-39.94%	-27.35%	-45.95%	-49.95%
Canada	23.61	28.40	37.97	36.76	60.48	48.72	74.13	56.70	51.53	56.70	20.30%	-3.20%	-19.45%	-23.52%	10.02%
Chile	32.35	28.00	62.90	50.97	137.34	77.96	235.37	166.57	61.34	58.44	-13.45%	-18.96%	-43.24%	-29.23%	-4.73%
Czech Republic	26.70	22.97	54.35	47.27	90.63	50.52	132.79	63.94	69.06	60.76	-13.97%	-13.03%	-44.26%	-51.85%	-12.02%
Denmark	11.89	9.92	20.11	12.57	27.90	21.48	41.55	23.84	19.51	15.57	-16.54%	-37.47%	-23.00%	-42.63%	-20.20%
Estonia	8.38	8.07	11.05	11.91	15.30	15.30	29.06	17.85	10.96	11.81	-3.79%	7.75%	0.02%	-38.57%	7.75%
Finland	11.51	10.10	16.35	15.90	19.25	19.90	37.63	24.16	18.28	15.90	-12.21%	-2.73%	3.38%	-35.80%	-13.02%
France	12.82	9.07	21.25	22.69	21.25	22.69	21.25	22.69	21.25	22.69	-29.25%	6.74%	6.74%	6.74%	6.74%
Germany	17.70	14.49	36.61	27.44	92.72	47.59	104.09	59.26	84.87	59.26	-18.15%	-25.03%	-48.67%	-43.07%	-30.18%
Greece	21.56	24.79	31.61	39.92	66.33	82.68	135.57	96.74	47.41	60.42	14.98%	26.29%	24.65%	-28.64%	27.45%
Hungary	29.60	26.57	45.59	56.57	107.72	79.48	272.47	103.14	64.21	70.67	-10.22%	24.07%	-26.22%	-62.15%	10.06%
Iceland	11.10	7.70	22.74	23.90	39.63	47.16	133.34	57.22	28.00	23.90	-30.61%	5.07%	19.00%	-57.09%	-14.65%
Ireland	17.16	21.09	25.88	30.58	36.36	31.63	49.21	36.91	39.62	36.91	22.92%	18.15%	-12.99%	-25.00%	-6.85%
Israel	25.36	16.51	25.36	16.51	25.36	26.08	27.49	26.08	27.49	26.08	-34.89%	-34.89%	2.85%	-5.12%	-5.12%
Italy	29.07	18.04	43.62	18.04	56.03	22.82	115.83	51.61	53.79	27.45	-37.95%	-58.66%	-59.28%	-55.44%	-48.98%
Japan	62.68	49.05	74.40	61.54	109.78	63.96	214.30	67.50	74.40	61.54	-21.75%	-17.28%	-41.74%	-68.50%	-17.28%
Korea	15.79	10.84	29.92	18.07	51.50	27.71	73.71	43.37	31.44	25.30	-31.34%	-39.60%	-46.20%	-41.16%	-19.53%
Luxembourg	14.91	18.59	32.61	21.59	44.58	34.98	44.58	34.98	42.47	34.98	24.62%	-33.77%	-21.53%	-21.53%	-17.63%
Mexico	17.68	20.93	39.57	31.53	87.30	41.46	159.60	131.75	42.40	56.87	18.36%	-20.32%	-52.51%	-17.45%	34.12%
Netherlands	19.63	14.94	26.31	26.61	41.91	35.32	72.85	39.86	44.06	39.86	-23.87%	1.14%	-15.72%	-45.29%	-9.55%
New Zealand	16.61	12.04	43.07	18.33	59.14	33.22	115.70	49.71	68.52	37.12	-27.48%	-57.43%	-43.83%	-57.04%	-45.82%
Norway	15.33	8.14	20.61	19.71	30.97	19.71	49.50	25.66	36.97	25.66	-46.86%	-4.34%	-36.33%	-48.17%	-30.60%
Poland	11.21	15.19	25.57	25.61	58.86	35.44	58.86	43.22	40.28	28.42	35.44%	0.15%	-39.78%	-26.56%	-29.44%
Portugal	21.94	16.72	35.55	41.16	74.73	43.52	127.92	58.07	55.75	58.07	-23.78%	15.80%	-41.76%	-54.61%	4.15%
Slovak Republic	24.84	17.92	39.22	38.26	52.20	56.17	73.16	70.04	43.60	47.67	-27.84%	-2.44%	7.61%	-4.27%	9.35%
Slovenia	21.23	15.08	27.91	26.97	40.20	26.97	72.65	34.34	46.40	31.39	-28.95%	-3.37%	-32.90%	-52.73%	-32.36%
Spain	15.63	19.32	53.39	31.55	84.98	41.21	180.46	41.21	58.92	41.21	23.56%	-40.91%	-51.51%	-77.17%	-30.06%
Sweden	11.15	10.89	22.05	18.32	28.18	21.45	37.95	26.95	26.65	26.95	-2.35%	-16.94%	-23.87%	-28.99%	1.12%
Switzerland	19.06	18.70	35.33	33.09	35.33	33.09	35.33	38.91	35.33	38.91	-1.88%	-6.34%	-6.34%	10.15%	10.15%
Turkey	28.83	20.57	34.80	20.57	54.69	27.66	69.60	39.01	61.55	27.66	-28.67%	-40.90%	-49.42%	-43.95%	-55.06%
United Kingdom	8.32	10.32	11.10	11.60	23.38	20.64	29.73	23.22	29.73	19.35	23.98%	4.46%	-11.74%	-21.89%	-34.91%
United States	29.09	39.94	55.00	45.44	55.00	52.04	55.00	67.44	55.00	62.74	37.29%	-17.38%	-5.38%	22.62%	14.06%
OECD average	19.74	17.72	33.63	28.07	54.58	37.79	90.70	51.22	44.17	37.76	-10.24%	-16.51%	-30.77%	-43.52%	-14.52%

StatLink http://dx.doi.org/10.1787/888933224802

were a minimum requirement of 40 channels plus the inclusion of premium movies and sports content. The proposed triple and quadruple-play services build on existing OECD price baskets for standalone services, such as mobile services, fixed broadband and so on. The proposed triple and quadruple-play baskets have two possible profiles: a basic service (drawing from basic standalone services) and a premium service (Table 2.3).

By way of example, the advanced triple-play basket costs USD 100 per month on average in the 12 selected OECD countries (Figure 2.39) and includes unlimited fixed telephony, broadband service at 30 Mbit/s of download speed with at least 200 GB (high bandwidth), and premium pay television service (with premium sports and movies content). Accordingly, the basic quadruple play basket includes fixed line rental only, 10 Mbit/s broadband service, basic pay television service and a 30-call mobile voice basket (Figure 2.40) for an average price of USD 65 per month in these 12 countries.

Figure 2.38. **Laptop mobile broadband basket, 2 GB, September 2014, USD PPP**

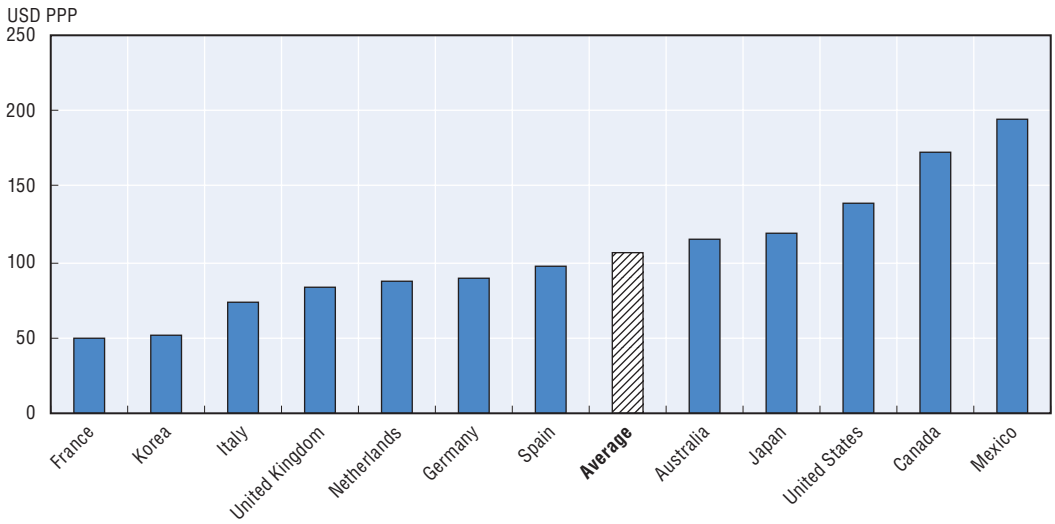


StatLink http://dx.doi.org/10.1787/888933224727

Table 2.3. **Elements included in the bundle baskets**

	Fixed telephony	Fixed broadband	Pay television	Mobile
Basic service	Line rental only	At least 10 Mbps download speed and 25 GB data allowance	Basic pay-TV (channels not available FtA)	30 calls basket
Advanced service	Unlimited national calls to landlines (or 420 calls basket)	At least 30 Mbps download speed and 200 GB data allowance	At least 40 channels, including premium sports and premium movies content	300 calls + 1 GB basket

Figure 2.39. **Triple-play basket (30 Mbps download speed and 200 GB, unlimited fixed calls, premium pay television including sports and movies), April 2014, USD PPP**

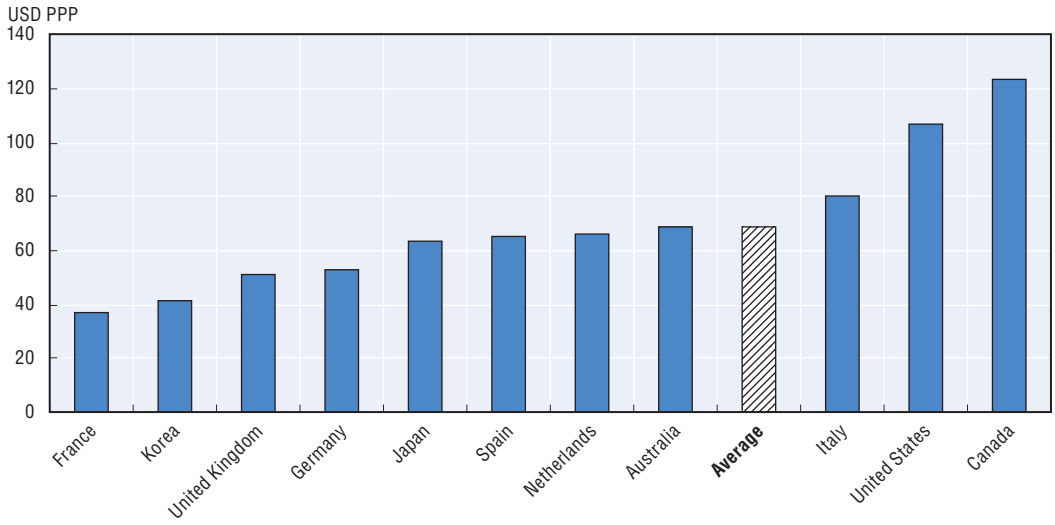


Source: OECD (2015).

StatLink http://dx.doi.org/10.1787/888933224734

A complementary approach to comparing prices as a function of quality characteristics is hedonic price analysis. Hedonic prices have been used to assess pricing behaviour by taking into account different quality levels or specific features of products and services. For example, economists have constructed hedonic price indices for automobiles and computers (Griliches, 1961; OECD, 2006). A hedonic function relates the prices of a certain good or service to its quality characteristics, and relies on the hypothesis that the price of the good/service (e.g. a computer or other ICT products) is equal to the total expenditure of the individual "bundled" features purchased by the consumer. This means that consumers value *per se* a "bundle" of characteristics rather than a specific final product/service. The OECD is currently assessing whether hedonic price analysis could be used for communication services, either to match pricing with quality characteristics, or to compare prices across countries or operators, accounting for quality differences.

Figure 2.40. **"Basic" quadruple-play – at least 10 Mbps broadband download speed and 25 GB capacity, fixed-line connection, basic pay-tv and 30-call mobile basket, April 2014, USD PPP**



Source: OECD (2015).

StatLink http://dx.doi.org/10.1787/888933224743

Internet infrastructure

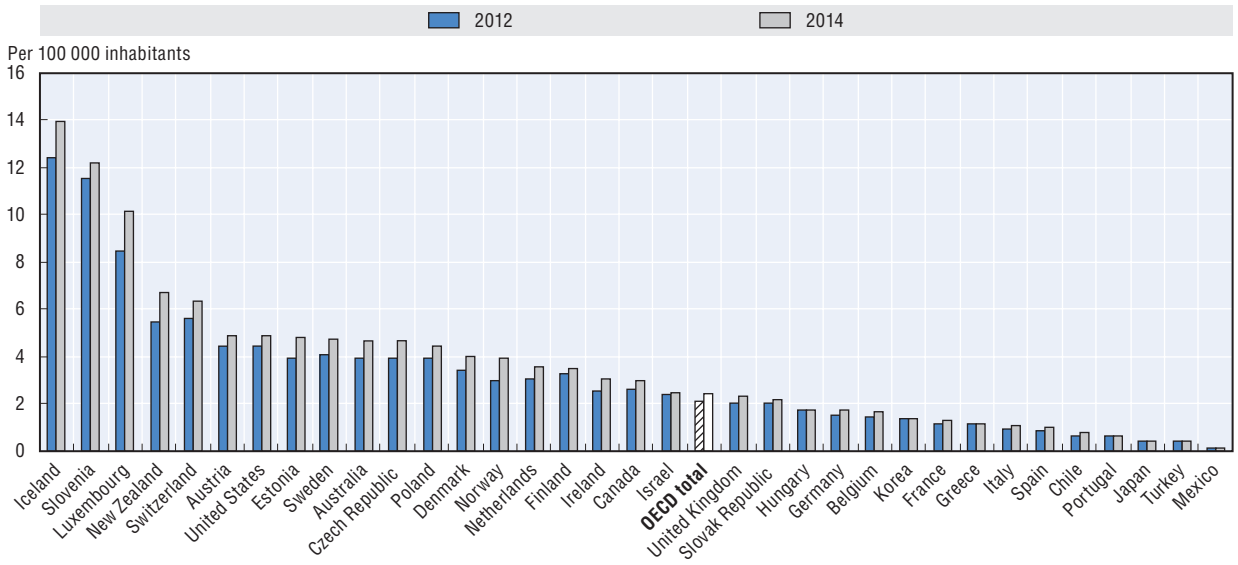
The Internet Protocol (IP) is an enabling technology for networks and the devices that communicate over them. An increasing number of applications and data transport protocols have already moved to IP technology. For example, SMS is gradually being replaced by messenger applications that run over IP, such as WhatsApp, Google Hangouts or Kakao Talk. The same process is occurring for other services that are migrating to IP-based networks, whether fixed or mobile.

A notable development is the upcoming shift of voice mobile communication towards all-IP technology through Voice over LTE (VoLTE), which envisages the provision of all services over an IP-enabled mobile network. Most mobile operators currently use 2G or 3G technologies to make and receive phone calls, even if they already run a parallel 4G/LTE network. The next step is the surge in smart devices, linked via machine-to-machine communications (M2M technology), which some believe will lead to the connection of as many as 50 billion devices by 2022.

The Internet is composed of millions of individual networks, from residential consumer networks to large networks that span the globe. Traffic is routed from networks, such as a home or business premise, to an Internet Service Provider (ISP). Borders exist between networks, but these are no longer national frontiers. The Border Gateway Protocol (BGP) is the method by which traffic is routed between networks on the Internet. The essence of BGP is that the owner of a network compiles lists of IP address blocks that are directly reachable from within its network. In the context of BGP each network is identified by a unique Autonomous System Number (ASN). Such a network is called "autonomous" because it can determine to some extent the routing of traffic to and from its network independently from any other network. Every such network is assigned a unique ASN by a Regional Internet Registry (RIR).

The number of routed Autonomous Systems (AS) a country has may be one proxy for the amount of competition in a market. It indicates the ease with which a company may take control over routing its traffic and exchange this traffic with other networks. Iceland has the most routed ASNs per capita with 13.46 per 100 000 inhabitants (Figure 2.41). At the end of 2014, the OECD average was 2.43 with 19 countries exceeding this level. All countries, except Korea, saw an increase in the number of AS per capita between 2012 and 2014. The average number of routed ASNs per capita in the OECD increased by 15.17%.

Figure 2.41. **Routed AS numbers per 100 000 inhabitants, 2012 and 2014**



Source: Potaroo, 28 October 2014. *www.potaroo.net*

StatLink http://dx.doi.org/10.1787/888933224759

IPv4 exhaustion and IPv6 adoption

The Internet Assigned Numbers Authority (IANA) delegates blocks of IP addresses and Autonomous Systems (AS) numbers to each Regional Internet Registry (RIR) to meet the needs of that region. RIRs follow regional policies to allocate resources to Local Internet Registries (LIRs) or to National Internet Registries (NIRs). LIRs either assign address space to end users or allocate address space to ISPs who, in turn, assign IP addresses to enterprises and end users. The IANA assigned the last five unallocated IPv4 address blocks to the regional registries (RIRs) in February 2011. The Asia Pacific Registry (APNIC) assigned all general use unallocated IPv4 blocks by 2011 and the RIPE

Box 2.2. **Estimating the customer population of Autonomous System Networks**

The size of networks and their customer base can be a useful indicator for policy makers and regulators considering issues as diverse as the level of competition and penetration through to market growth. This raises the question of how many customers are served by any particular Internet Service Provider. While some network operators publish such numbers, others regard this information as commercially sensitive. A number of techniques can be used, however, to estimate the size of each service provider from public information sources. These include the number of IP addresses announced by the network or the number of transit customers who use the network. However, the widespread use of network address translators (NAT) in IPv4, the varying IPv6 address plans used by IPv6 service providers, and the issue of so-called "stub" Autonomous Systems (AS) by retail service providers add considerable uncertainty to such indirect measurements.

One alternative approach is to use Google's Ad delivery network in a non-targeted advertisement placement programme, aimed at assembling a very large collection of user's IP addresses over an extended period. Using the data from the BGP routing system, each user IP address can be mapped to an originating AS number. If the advertisement placement strategy enabled each AS in the Internet to be targeted uniformly for ad placement, irrespective of location, then these counts of advertisement impressions[9] per AS would be a good indicator of the relative size of each AS in terms of the population of customers served by each AS. This is not the case, however, as the advertisements are placed with different rates in different countries. Thus, this needs to be compensated for at the national level to compile a uniform estimate of the customer population served by each AS.

The data set used to normalise the original ad impression numbers is the estimate of Internet users, per country published by the ITU-T.[10] It is also assumed that the Google ad placement process is uniformly distributed within each country. This then permits an estimation of the relative size of each AS in terms of the estimated population of users served by each AS.[11] This constitutes an estimate of customer populations per AS, assuming that each AS operates its customer base in the country where the AS has been registered. It should also be noted that some large networks operate multiple AS, as is the case of Level 3, AT&T, Verizon and many others.

While this is the case for many situations, there are a number of cases where large retail service providers span a number of countries with a single AS. This approach also does not use secure connections to the server used for measurement in this exercise. While care has been taken over the use of unique URLs in the measurement, it still supports the use of web proxy middleware, and the measurement approach is biased towards over-counting in networks that use web proxy services. This is an issue particularly when the web proxy is located in a different AS than the end customers. Additionally, the instrumentation in the advertisement is not accessible in all forms of mobile devices, and this approach tends to undercount the customers in service networks with high populations of mobile users. Nonetheless, the data shown here provides an indication of the relative size of the largest AS networks in the world (see Table 2.4). Moreover, in the future, changes being introduced in the measurement process are intended to improve on some of the assumptions and current limitations of this measurement.

NCC (serving members in Europe, the Middle East and parts of Central Asia) reached this stage in September 2012. LACNIC exhausted its general use pool of unallocated IPv4 blocks in May 2014. The North American Regional registry (ARIN) is expected to assign all unallocated addresses by early 2015, while AFRINIC still has a small number of blocks available for a longer period (Figure 2.42).

In the context of decreasing unallocated IPv4 blocks, an interesting metric is the number of addressable points using the IPv4 protocol. It can hint at ways that ISPs use to function using a limited number of IPv4 addresses, in view of the low adoption of IPv6, by themselves or other stakeholders. According to Akamai's "State of the Internet" covering

Table 2.4. **Five views on top ten largest networks in the world, 2014**

Customer Cone			IPV4 Adjacencies		
ASN	Company name	Customer Cone	ASN	Name	Count
AS3356	Level 3 Communications, Inc.	72%	AS174	Cogent Communications	4452
AS2914	NTT America, Inc.	43%	AS3356	Level 3 Communications, Inc.	4061
AS3257	Tinet SpA	39%	AS6939	Hurricane Electric, Inc.	3492
AS1299	TeliaSonera International Carrier	36%	AS3549	Level 3 Communications, Inc. (GBLX)	3162
AS174	Cogent Communications	34%	AS7018	AT&T Services, Inc.	2390
AS6453	Tata Communications (America), Inc.	28%	AS4323	tw telecom holdings, inc.	1963
AS3549	Level 3 Communications, Inc. (GBLX)	26%	AS24482	SG.GS	1760
AS6762	Telecom Italia Sparkle S.p.A	18%	AS9002	RETN Limited	1747
AS6939	Hurricane Electric, Inc.	13%	AS209	Qwest Communications Company, LLC	1601
AS1273	Cable and Wireless Worldwide plc	11%	AS701	Verizon Business/UUnet	1600

IPv4 Prefixes Announced			IPv4 Addresses Originated		
ASN	Name	Count	ASN	Name	Count
AS3356	Level 3 Communications, Inc.	151181	AS4134	China Telecom Backbone	116.6M
AS2914	NTT America, Inc.	83170	AS7018	AT&T Services, Inc.	76.7M
AS1299	TeliaSonera International Carrier	66446	AS721	DoD Network Information Center	72.3M
AS6939	Hurricane Electric, Inc.	58744	AS7922	Comcast Cable Communications, Inc.	71.2M
AS174	Cogent Communications	54410	AS4837	China Unicom Backbone	56.1M
AS6453	Tata Communications (America), Inc.	51018	AS4766	Korea Telecom	47.4M
AS3257	Tinet SpA	40208	AS3549	Level 3 Communications, Inc. (GBLX)	46.3M
AS6762	Telecom Italia Sparkle S.p.A	37703	AS701	Verizon Business/UUnet	46.1M
AS3491	PCCW Global	30040	AS17676	Softbank BB Corp.	44.5M
AS7018	AT&T Services, Inc.	25694	AS3356	Level 3 Communications, Inc.	43.8M

Estimated Customer Populations		
ASN	Name	Count
AS4134	China Telecom Backbone	272 968 573
AS4837	China Unicom Backbone	138 857 993
AS7922	Comcast Cable Communications, Inc.	41 167 618
AS9829	National Internet Backbone	32 717 138
AS8151	Uninet S.A. de C.V.	30 510 175
AS4713	OCN NTT Communications Corporation	28 705 061
AS9121	TTNET Turk Telekomunikasyon Anonim Sirketi	24 613 012
AS3320	DTAG Deutsche Telekom AG	22 786 268
AS7018	ATT Services, Inc.	21 014 943
AS4812	China Telecom (Group)	20 426 799

Note: Data point is 1st March 2014 for customer cone and 27th October 2014 for the rest. Customer cone shows each AS's percentage of all IPv4 addresses.

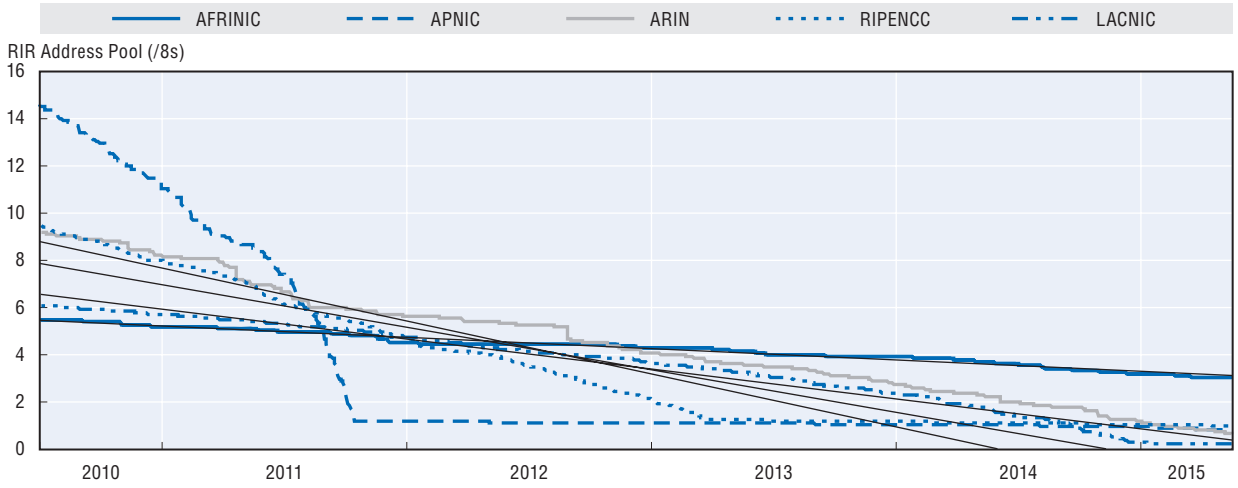
Sources: Route Views [*www.routeviews.org*], CAIDA [*www.caida.org*], APNIC [*www.apnic.net*].

StatLink http://dx.doi.org/10.1787/888933224812

Q2 2014, the estimate of the number of active (not "available") IPv4 addresses has declined by about 7 billion from Q1 2014, equivalent to about 0.9% of the total space.[12]

This might suggest that some providers are implementing network address translation (NAT) technologies or increasing support for IPv6 connectivity among carriers. In this respect, some are discussing the arrangement that will service the "Internet of Things" (IoT) in the near future, in particular whether IoT devices in small networks will use public IPv4 or IPv6 addresses, or whether they will be assigned to a hub. A hub would typically have the only public address, thus reducing the need for new addresses. Notwithstanding exhaustion concerns, the number of routed IPv4 addresses per inhabitant still provides an indication of the development of Internet infrastructure (Figure 2.43).

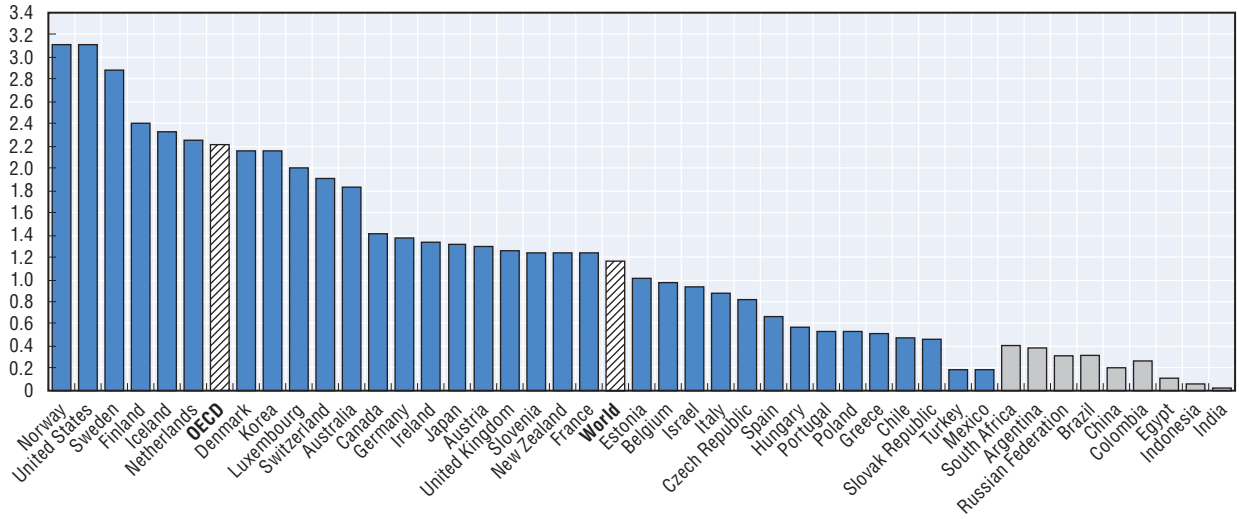
Figure 2.42. **IPv4 depletion per RIR, 2014**



Source: Potaroo, 28 October 2014. *www.potaroo.net*

StatLink http://dx.doi.org/10.1787/888933224761

Figure 2.43. **Routed IPv4 addresses per inhabitant, mid-2014**



Source: Potaroo, 28 October 2014. *www.potaroo.net*

StatLink http://dx.doi.org/10.1787/888933224775

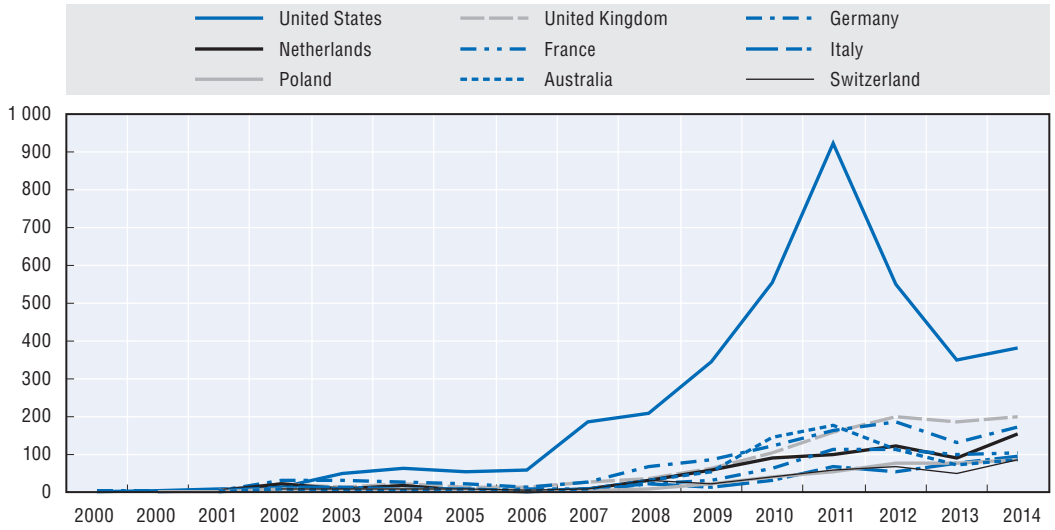
The size of IPv6 prefix allocation can provide one indication of the scale of planned deployments; however, extremely large allocations (given the magnitude of the IPv6 space) were provided in the past to some operators and large users skewing the "by size" results. Perhaps a more reasonable measure is the number of IPv6 allocations. At the end of 2014, the leader in IPv6 allocations was the United States (384 allocations), followed by the United Kingdom (198 allocations) and Germany (174 allocations) (Figure 2.44).

IPv6 user penetration

Another measure of IPv6 deployment is the user penetration rate. Google reports data on IPv6 user penetration by measuring the percentage of terminal devices that "talk" IPv6 language. APNIC calculated their ratio by using YouTube's advertising distribution to reach a very significant sample of the entire Internet user base. The test measures the percentage

of users in each country who show a preference for using IPv6 to download a dual-stack web object. This metric is termed the IPv6 user ratio. Data from APNIC reveal that the IPv6 global user penetration ratio grew from around 0.71% in mid-2012 to 2.53% at the end of October 2014, more than threefold, and showed the following penetration ratios by country: Belgium (33.3%), Germany (13.89%) and Norway (12.91%), which lead the OECD. Large countries, such as Japan (7.16%) and the United States (10.53%), have also experienced enormous growth in the past two years (Figure 2.45). In mid-2012, the OECD country with the highest IPv6 user penetration was France, with 4.7%. A growing number of networks are adopting IPv6, with content and devices installing IPv6 by default. In Belgium, the cable operator Telenet enabled IPv6 by default for over 1 million customers in an effort that, together with other

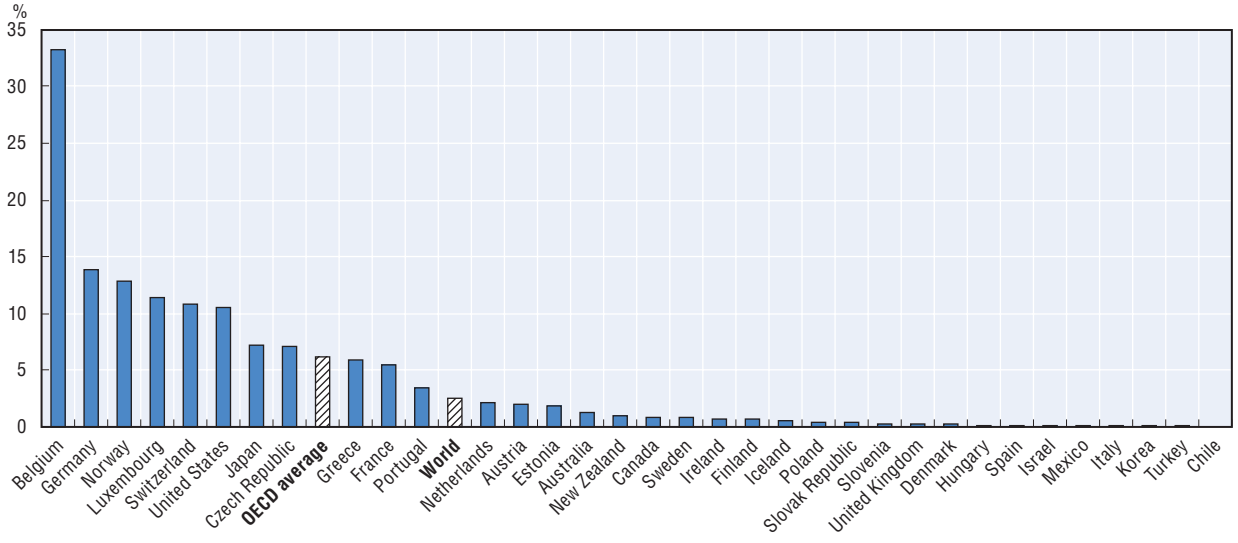
Figure 2.44. **Numbers of IPv6 allocations per year, top ten OECD countries, 1999-2014 (year-end)**



Source: Potaroo, 28 October 2014. *www.potaroo.net*

StatLink http://dx.doi.org/10.1787/888933224786

Figure 2.45. **IPv6 user ratio, October 2014**



Source: Potaroo, 28 October 2014. *www.potaroo.net*

StatLink http://dx.doi.org/10.1787/888933224793

ISPs in that country, made Belgium the leader in IPv6 user adoption. However, content providers and device vendors have not enabled IPv6 accordingly, therefore IPv6 traffic is not growing at the same pace. Similar efforts are being undertaken by ISPs in Germany (Kabel Deutschland and Deutsche Telekom) and Norway (Lyse), among other countries. The OECD has recommended higher IPv6 use by all relevant stakeholders, highlighting its benefits and the challenges involved in the transition (OECD, 2014b)

Notes

1. This group includes photographic, cinematographic and optical apparatus mainly bundled with ICTs.
2. See Table 2.39. Advertised speeds, Fixed broadband, Sep. 2014 , available online at *www.oecd.org/sti/DEO-tables-2015.htm*.
3. For further information, see the websites of Akamai (*www.akamai.com/stateoftheinternet/*), M-Lab (*www.measurementlab.net/*) and Ookla (*www.ookla.com/*).
4. A list of official speed measurement projects can be found in the OECD Broadband Portal at *www.oecd.org/sti/broadband/speed-tests.htm*.
5. See Tables 2.30. Public telecommunication investment per total communication access path and 2.31. Public telecommunication investment per capita, available online at *www.oecd.org/sti/DEO-tables-2015.htm*.
6. See tables on pricing baskets : Tables 2.58 to 2.103, available online at *www.oecd.org/sti/DEO-tables-2015.htm*.
7. See tables on pricing baskets : Tables 2.58 to 2.103, available online at *www.oecd.org/sti/DEO-tables-2015.htm*.
8. See tables on pricing baskets : Tables 2.58 to 2.103, available online at *www.oecd.org/sti/DEO-tables-2015.htm*.
9. An "impression" in the context of online advertising, is described when an ad is viewed, and is countable. Each time an ad displays it is counted as one impression. Online advertising rates are determined through a combination of ad size, ad location, ad performance and market demand.
10. See *www.itu.int/net4/itu-d/icteye/*.
11. See *http://stats.labs.apnic.net/cgi-bin/aspop*.
12. See *www.fierceenterprisecommunications.com/story/akamai-reports-l*.

References

ANATEL (2014), Dados, *www.anatel.gov.br/dados/* (accessed November 2014).

EU (2014), "Quality of broadband services in the EU – SamKnows study on Internet speeds (second report)", *Digital Agenda for Europe*, Press release, 23 March 2014, European Commission, Brussels, *https://ec.europa.eu/digital-agenda/en/news/quality-broadband-services-eu-samknows-study-internet-speeds* (accessed 15 April 2015).

FCC (2014), *Measuring Fixed Broadband: 2014 Report*, Federal Communications Commission, Washington DC, *www.fcc.gov/encyclopedia/measuring-broadband-america-measuring-fixed-broadband* (accessed 15 April 2015).

Griliches, Z. (1961), "Hedonic prices indexes for automobiles: An econometric study of quality change", in *The Price Statistics of the Federal Government*, Columbia University Press for the National Bureau of Economic Research, New York, pp. 137-196.

IBGE (2013), Pesquisa de Inovação (PINTEC) 2011, *www.ibge.gov.br/home/estatistica/economia/industria/pintec/2011/*

IBGE (2014), SIDRA Database, *www.sidra.ibge.gov.br/bda/pesquisas/* (accessed November 2014).

IPEA (2013), "Análise dos dados da PINTEC 2011", Nota Técnica, n.15, Brasília.

Kamada, T. and S. Kawai (1989), "An algorithm for drawing general undirected graphs", *Information Processing Letters*, No. 31, pp. 7-15.

Ministry of Labour, Brazil (2014),"Cadastro Geral de Empregados e Desempregados – CAGED", *Dados e Estatísticas*, Brasília, Ministry of Labour, *http://portal.mte.gov.br/caged/estatisticas.htm*.

OECD (2015), "Triple- and quadruple play bundles of communication services", *Digital Economy Papers*, forthcoming, OECD Publishing, Paris.

OECD (2014a), *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, DOI: 10.1787/9789264221796-en.

OECD (2014b), "The economics of transition to Internet Protocol version 6 (IPv6)", *OECD Digital Economy Papers*, No. 244, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5jxt46d07bhc-en*.

OECD (2014c), "Access network speed tests", *OECD Digital Economy Papers*, No. 237, OECD Publishing, Paris, DOI: 10.1787/5jz2m5mr66f5-en.

OECD (2013), *ICT Jobs and Skills: New Estimates and the Work Ahead*, Working Party on Indicators for the Information Society, OECD, Paris, DSTI/ICCP/IIS(2013)6.

OECD (2012a), "ICT skills and employment: New competences and jobs for a greener and smarter economy ", *OECD Digital Economy Papers*, No. 198, OECD Publishing, DOI: 10.1787/5k994f3prlr5-en.

OECD (2012b), *OECD Internet Economy Outlook 2012*, OECD Publishing, Paris, *www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm*.

OECD (2011), *OECD Guide to Measuring the Information Society 2011*, OECD Publishing, Paris, DOI: 10.1787/9789264113541-en.

OECD (2006), Handbook on Hedonic Indexes and Quality Adjustments in Price Indexes: Special Application to Information Technology Products, OECD Publishing, Paris, DOI: 10.1787/9789264028159-en.

OECD (2005), "New perspectives on ICT skills and employment", *OECD Digital Economy Papers*, No. 96, OECD Publishing, Paris, DOI: 10.1787/232342747761.

PricewaterhouseCoopers (2015), MoneyTree Survey Report, February, London Pwc.

WSTS (World Semiconductor Trade Statistics) (2014), *WSTS Semiconductor Market Forecast Autumn 2014*, *www.wsts.org/PRESS/PRESS-ARCHIVE/WSTS-Semiconductor-Market-Forecast-Autumn-2014*.

Sci2 Team (2009). *Science of Science (Sci2) Tool*, Bloomington, Indiana University and SciTech Strategies, *https://sci2.cns.iu.edu*.

© OECD 2015

Chapter 3

The growing and expanding digital economy

The digital economy transcends the ICT sector. While the Internet, broadband, mobile applications and IT services constitute its foundations, the digital economy today encompasses all sectors of the economy and society. The ways in which individuals use ICT goods and services affect the benefits they receive from the digital economy. The success and growth of firms is also crucially dependent on their capability to compete in the new economic environment, which ICTs are helping to shape. Despite the universal availability of ICTs, their use continues to differ across firms, individuals and countries. Difference in age and education significantly affect how people use the Internet. Differences in firm size and market characteristics influence the diffusion of e-business. This chapter looks at ICT usage by individuals and firms, the emergence of new sectors and new business models, and the overall contribution of the digital economy to growth and employment.

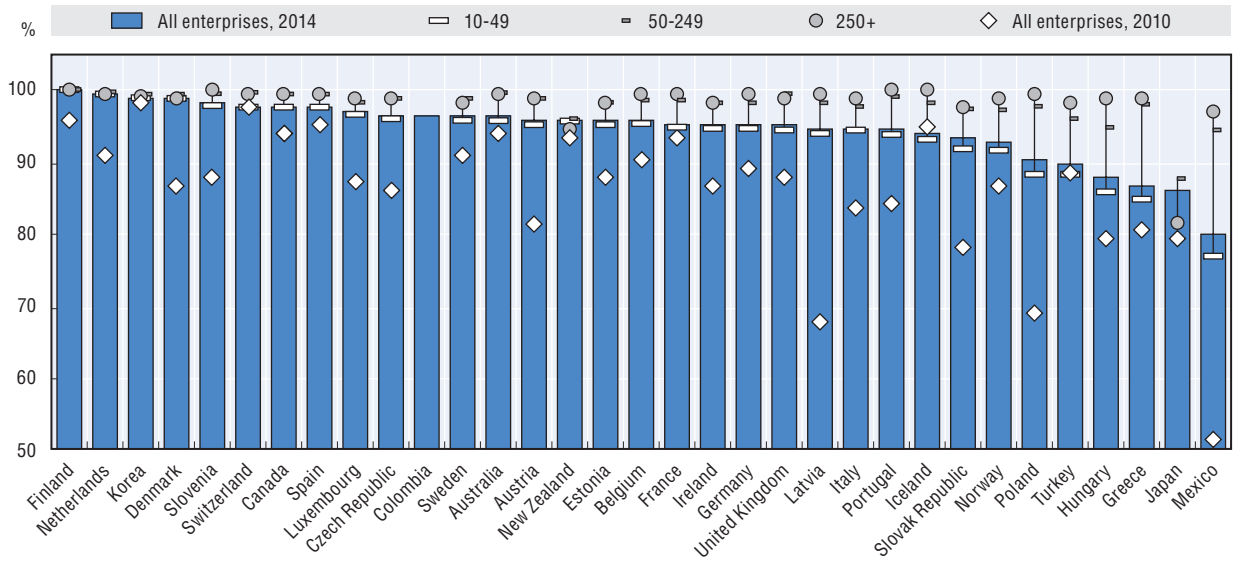
3.1 ICT adoption and use across economic and social activities

ICT adoption and use by firms

The large majority of businesses today make use of ICTs. In 2014, on average 95% of enterprises in OECD countries had a broadband connection (Figure 3.1), up from 86% in 2010. The increase in connectivity was particularly high in Mexico (28 percentage points), Latvia (27) and Poland (21). Higher uptake has also narrowed the gap between large and small firms[1] to less than 5 percentage points, on average. Nonetheless, the gap remains more significant in Mexico (20 percentage points), Greece (14), Hungary (12), Poland and Turkey (just above 10).

Figure 3.1. **Broadband connectivity by size, 2010 and 2014**

Percentage of enterprises in each employment size class



Notes: Broadband connections include both fixed and mobile Internet connections with an advertised download speed of at least 256 Kbit/s and, include connections based on the following technologies: xDSL, cable modem, optical fibre (e.g. FTTx), leased lines, Ethernet, PLC, BPL, public-WIFI, satellite and terrestrial fixed wireless such as fixed WiMAX, LMDS and MMDS, 3G/LTE/4G, UMTS and CDMA2000. For Japan, broadband connections include only optical fibre (FTTH), Cable modem , DSL and terrestrial fixed wireless (FWA and BWA). For Australia, Canada, Japan, Korea and Colombia, data refer to 2013. For Australia and New Zealand, data refer to the fiscal year ending 30 June 2013 instead of 2014. For Australia, the total includes Agriculture, forestry and fishing. For Canada, data refer to 2007 instead of 2010; medium-sized enterprises have 50 to 299 employees and large enterprises have 300 or more employees. For Japan, data refer to businesses with 100 or more persons employed instead of 10 or more; medium-sized enterprises have 100-299 persons employed, and large enterprises have 300 or more persons employed. For Mexico, data refer to 2008 and 2012, instead of 2010 and 2014. In 2008, data refer to businesses with 20 or more persons employed instead of 10 or more. For Switzerland, data refer to 2008 and 2011. For Colombia, data refer to enterprises with 10 or more persons employed in the manufacturing sector (excluding ISIC Rev.4 divisions 12-14, 17, 21 and 33) and enterprises with 75 or more persons employed in the non-financial market services (excluding ISIC Rev.4 divisions 49-51, 58, 75 and 77). In addition, the scope population excludes enterprises with less than 20 persons employed for wholesale and retail trade industries and, enterprises with less than 40 persons employed for transportation and storage, accommodation and food service activities and information and communication industries.

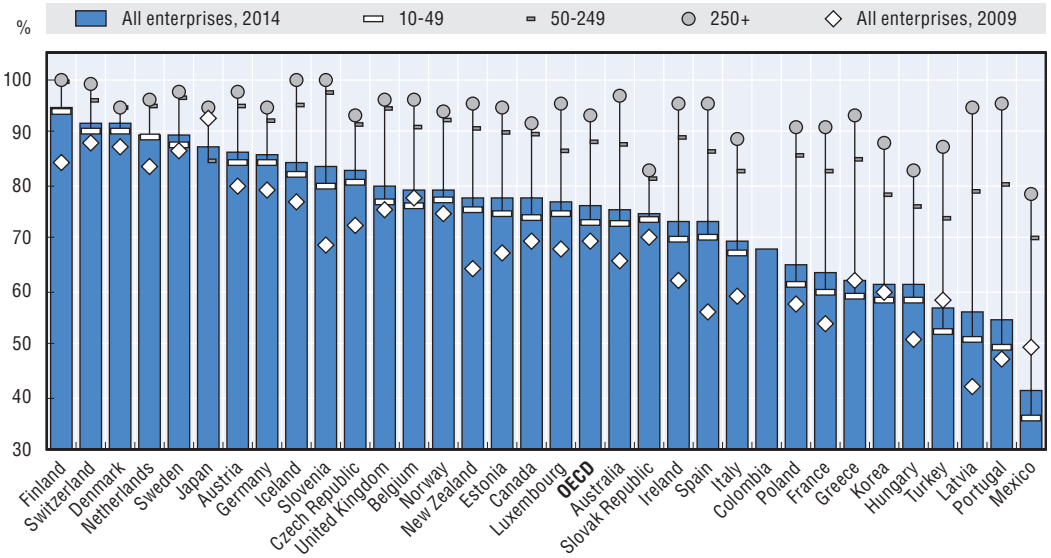
Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224829

More than 76% of all OECD enterprises had a website or homepage in 2014, up from 70% in 2009 (Figure 3.2). The share of enterprises with a web presence ranges from over 90% in Denmark, Finland and Switzerland to 54% in Portugal and 42% in Mexico. Progress since 2009 was particularly strong in Spain (17 percentage points), Slovenia (15), Latvia and New Zealand (14).

Figure 3.2. **Enterprises with a website or home page by size, 2009 and 2014**

As a percentage of enterprises in each employment size class



Notes: Except otherwise stated, the sector coverage consists of all activities in manufacturing and non-financial market services. Only enterprises with ten or more persons employed are considered. Size classes are defined as: small (from 10 to 49 persons employed), medium (50 to 249) and large (250 and more). For Australia, Canada, Japan, Korea and Colombia, data refer to 2013 instead of 2014. For Australia, data refer to the fiscal years 2008/09 and 2012/13, ending on 30 June, instead of 2009 and 2014. Data for the fiscal year 2012/13 include Agriculture, forestry and fishing. For Canada, data refer to 2007 instead of 2009. Medium-sized enterprises have 50-299 employees. Large enterprises have 300 or more employees. For Japan, data refer to businesses with 100 or more employees. Medium-sized enterprises have 100-299 employees. Large enterprises have 300 or more employees. For Mexico, data refer to 2012. Small-sized enterprises have 10-50, medium-sized enterprises have 51-250 persons employed, and large enterprises have 251 or more persons employed. For New Zealand, data refer to the fiscal years 2007/08 and 2011/12, ending on 31 March, instead of 2009 and 2014. For Switzerland, data refer to 2011. For Colombia, data refer to enterprises with 10 or more persons employed in the manufacturing sector (excluding ISIC Rev.4 divisions 12-14, 17, 21 and 33) and enterprises with 75 or more persons employed in the non-financial market services (excluding ISIC Rev.4 divisions 49-51, 58, 75 and 77). In addition, the scope population excludes enterprises with less than 20 persons employed for wholesale and retail trade industries and, enterprises with less than 40 persons employed for transportation and storage, accommodation and food service activities and information and communication industries.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224836

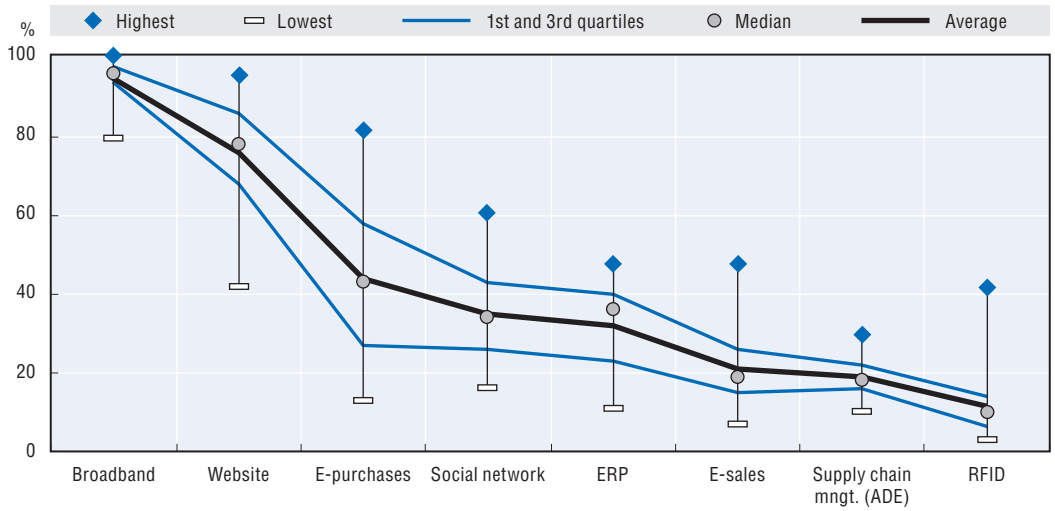
As with broadband access, web presence is lower among small firms. In 27 out of 32 OECD countries 90% or more of larger enterprises have a website, while web presence in SMEs ranges between 90% and above in Denmark, Finland and Switzerland, and 50% or less in Latvia, Portugal and Mexico.

The speed of adoption depends in some cases on prior uptake. It took 15 to 20 years for slightly more than three quarters of enterprises to develop a website, but only a few years for around 30% of businesses to subsequently become active on social networks. Figures for participation in e-commerce are lower. In reporting OECD countries, 21% of firms with at least ten persons employed received electronic orders in 2014 (Figure 3.3), representing an increase of 4 percentage points from 2009.

Differences in e-sales among countries remain considerable. In New Zealand the share is above 45%, while in Greece, Turkey, Italy and Mexico, the share is 10% or lower. These differences follow closely the differences in shares of smaller firms among countries. For enterprises with 250 or more persons employed, participation in e-commerce is 40%, with the share above 30% even in some lagging countries. Differences between large and small firms are even larger with regard to e-commerce turnover.

Figure 3.3. **Diffusion of selected ICT tools and activities in enterprises, 2014**

Percentage of enterprises with ten or more persons employed



Notes: Supply chain management refers to the use of automated data exchange (ADE) applications. For countries in the European Statistical System, e-commerce variables (online purchases and online sales) refer to 2013. For Australia, Canada, Japan and Korea, data refer to 2013. For Mexico and New Zealand, data refer to 2012. For Switzerland, data refer to 2011.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224847

The share of e-commerce sales stands at 17.1% of total turnover on average in reporting countries. Up to 90% of the value of e-commerce comes from business-to-business (B2B) transactions over electronic data interchange (EDI) applications. The observed patterns are dominated by the economic weight of large enterprises, for which e-commerce sales represent on average 22.1% of turnover against 9% for small firms.

The use of more sophisticated ICT technologies is less widespread. These include ICT applications used to manage information flows, where implementation requires changes in business organisation, and Radio Frequency Identification (RFID), where uptake is limited to certain types of businesses.

In 2013, the large majority of OECD enterprises (90%) interacted online with public authorities. Compared to 2010, the share of enterprises completing and submitting forms electronically has increased by almost 20 percentage points in the Czech Republic and Italy, and by over 10 percentage points in Ireland, New Zealand and Norway.

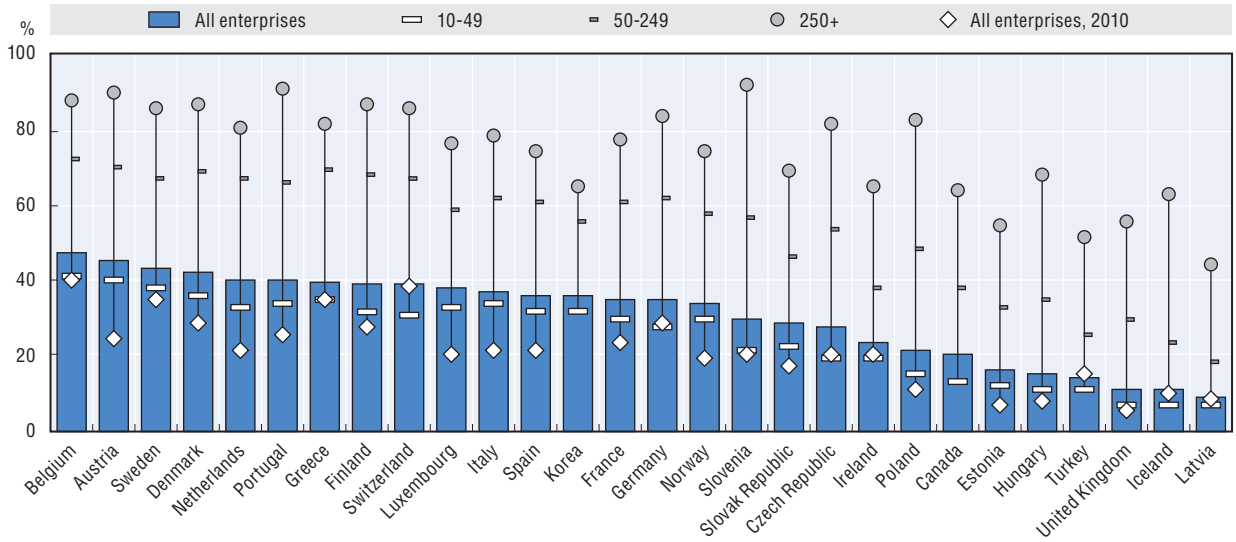
Much larger cross-country differences remain in the management of information flows within companies (Figure 3.4). The role of e-business processes in handling internal information flows can be seen in the diffusion of enterprise resource planning (ERP) software applications. In 2014, on average, such technologies were used to share information by 31%

of enterprises, against less than 22% in 2010. ERP software was used in 75% of larger (and more complex) enterprises, but by less than 25% of small firms, for which it is only recently becoming more affordable.

Adoption rates for ERP software across countries range between 44% and 92% for larger enterprises and between 7% and 41% for smaller ones, with Belgium, Austria, Sweden and Denmark leading, and Latvia, Iceland and the United Kingdom lagging for enterprises of all sizes.

Figure 3.4. **Use of enterprise resource planning software, by size, 2010 and 2014**

As a percentage of enterprises in each employment size class



Notes: Unless otherwise stated, sector coverage consists of all activities in manufacturing and non-financial market services. Only enterprises with ten or more persons employed are considered. Size classes are defined as: small (from 10 to 49 persons employed), medium (50 to 249) and large (250 and above). For Canada, medium-sized enterprises have 50 to 299 employees. Large enterprises have 300 or more employees. For Korea, data refer to 2013. For Switzerland, data refer to 2011.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224852

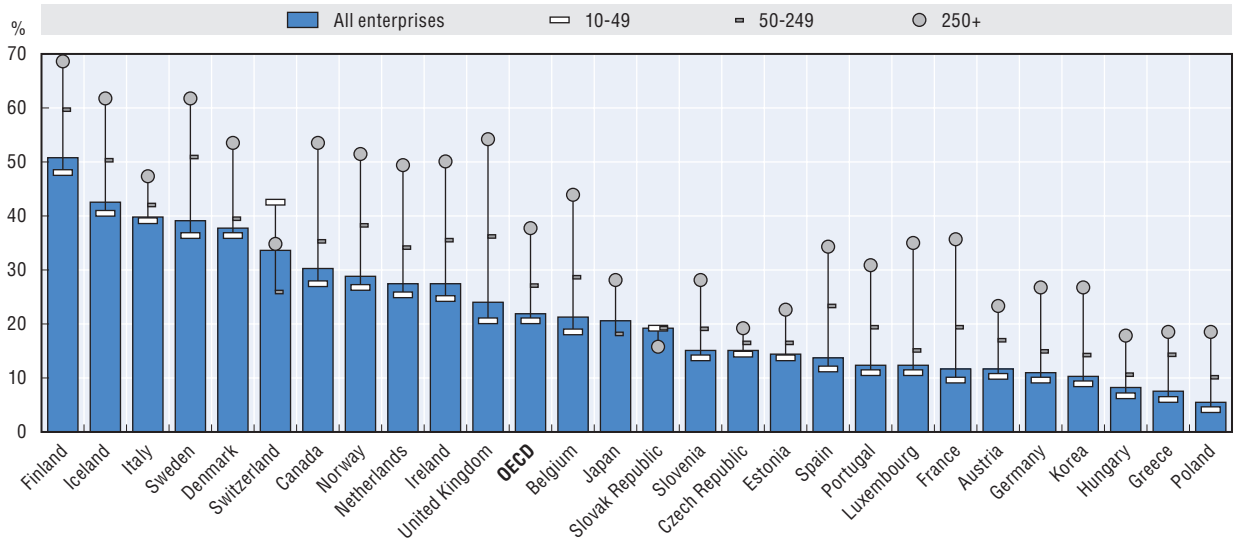
Among the new uses of ICTs by firms, cloud computing deserves special attention. Cloud computing can be understood as a service model for computing services, based on a set of computing resources that can be accessed in a flexible, on-demand way with low management effort (OECD, 2014a).

Cloud computing services permit users to access software, computing power, storage capacity and other services. Those services can be easily scaled up or down, be used on-demand by the user, and are paid for either per user or by capacity used. They can take the form of software or be extended to platforms or infrastructure, and may be deployed either privately (for exclusive use by a single organisation), publicly (open use by the general public) or under a hybrid format (a mix of the two former categories).

Diffusion of cloud computing among firms has accelerated in recent years: in 2014, over 22% of businesses used cloud computing services. This share ranges from over 50% in Finland down to 6% in Poland. In most countries, uptake is higher among large businesses (close to 40%) compared to small or medium-sized enterprises (around 21% and 27%, respectively). By contrast, in Switzerland and the Slovak Republic, uptake is higher among small businesses than large ones (Figure 3.5).

Figure 3.5. **Enterprises using cloud computing services by size, 2014**

As a percentage of enterprises in each employment size class



Notes: Unless otherwise stated, sector coverage consists of all activities in manufacturing and non-financial market services. Only enterprises with ten or more persons employed are considered. Size classes are defined as: small (from 10 to 49 persons employed), medium (50 to 249) and large (250 and more). For Canada, data refer to enterprises with expenditures on "Software as a Service" (e.g. cloud computing). Medium-sized enterprises have 50-299 employees. Large enterprises have 300 or more employees. For Japan, data refer to businesses with 100 or more employees. Medium-sized enterprises have 100-299 employees. Large enterprises have 300 or more employees. For Canada and Korea, data refer to 2012 instead of 2014. For Japan and Switzerland, data refer to 2011 instead of 2014. For Switzerland, data refer to enterprises with five and more employees.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, January 2015.

StatLink http://dx.doi.org/10.1787/888933224863

Businesses more frequently invest in cloud computing services with a high level of sophistication, such as finance/accounting software, CRM software and computing power, than less sophisticated services such as emails, office software or file storage (Figure 3.6). In Finland, for example, 53% of firms using cloud computing purchased high-level services, while only 28% bought low-level services.

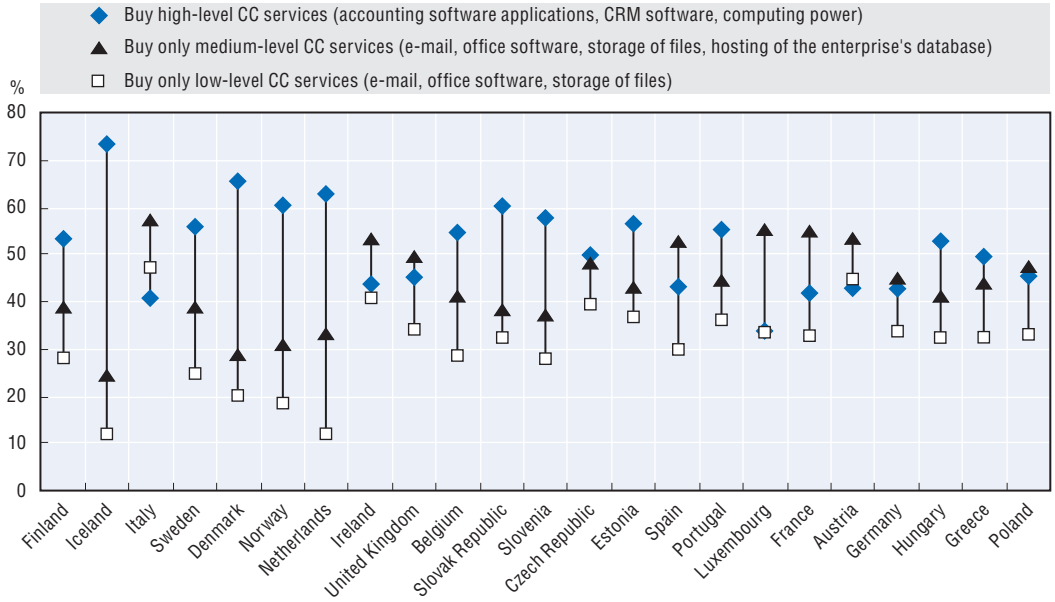
The main benefits from cloud computing, as perceived by European firms, are quick and easy deployment of solutions, higher flexibility due to scaling up or down, and a reduction in ICT-related costs (Figure 3.7). In Austria, Iceland, the Netherlands and Norway, a large majority of businesses buying cloud computing services have not found benefits linked to reduction in ICT costs or have noticed only limited benefits.

Factors preventing firms from using cloud computing services relate primarily to the risk of security breaches – large firms express uncertainty about the location of data, while small firms emphasise a lack of sufficient knowledge.

ICT adoption and use by individuals

In 2014, 81% of the adult population in the OECD accessed the Internet, of which over 75% used it on a daily basis. Developments in mobile technology have also enabled people to conduct daily personal computing and communications activities "on the go". In 2013, more than 40% of adults used a mobile or smartphone to connect to the Internet across the OECD.

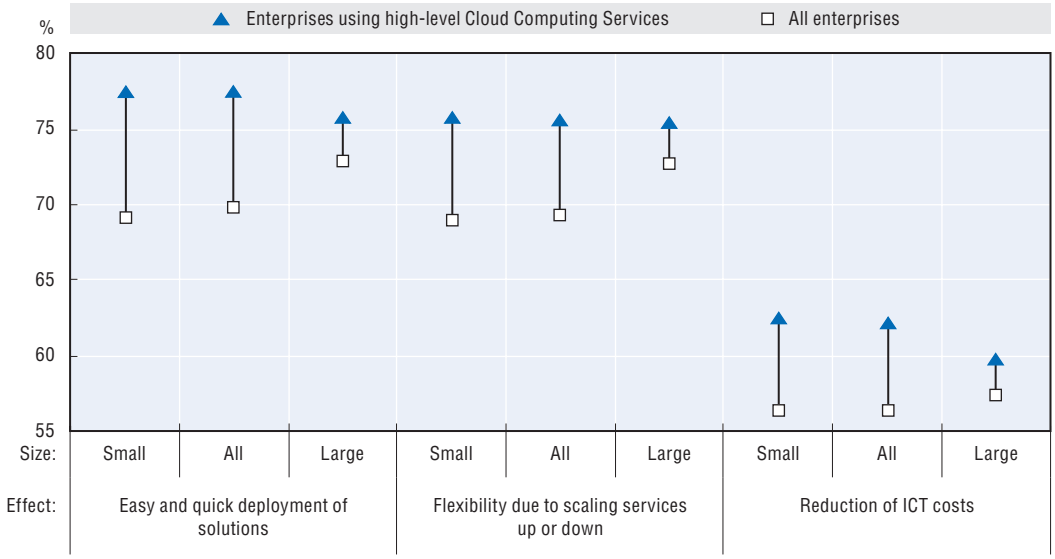
Figure 3.6. **Enterprises using cloud computing services by type of services, 2014**



Source: Eurostat, Information Society Statistics, January 2015.

StatLink http://dx.doi.org/10.1787/888933224874

Figure 3.7. **Cloud computing services perceived effects in 15 EU countries**



Notes: Perceived effects relate to "high or some degree". High cloud computing services include Finance or accounting software applications (as a cloud computing service), Customer Relationship Management (CRM) – a software application for managing information about customers (as a cloud computing service), and computing power to run the enterprise's own software (as a cloud computing service). Data refer to the average of the following EU countries: Austria, Denmark, Estonia, Greece, Spain, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Slovenia and the Slovak Republic.

Sources: Based on Eurostat, Information Society Statistics, January 2015.

StatLink http://dx.doi.org/10.1787/888933224888

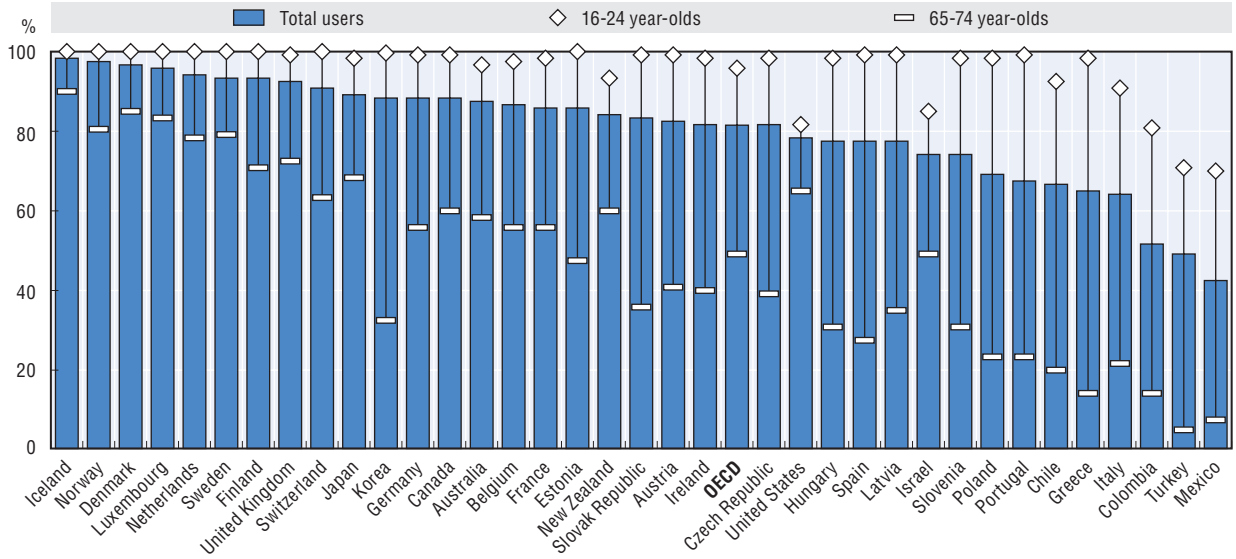
Internet usage continues to vary widely across OECD countries and among social groups. In 2014, 95% and above of the adult population accessed the Internet in Denmark, Iceland, Luxembourg and Norway, but less than 50% in Mexico and Turkey. In Iceland and Italy, the share of daily users is very similar to that of total users. In Chile, Japan and Mexico, however, many users access the Internet on an infrequent basis.

Differences in Internet uptake are linked primarily to age and education, often intertwined with income levels. In most countries, uptake by young people is nearly universal, but there are wide differences for older generations (Figure 3.8). Over 95% of 24 year-olds in the OECD used the Internet in 2014 against less than 49% among 65-74 year-olds.

Education appears to be a much more important factor for older people than for youth. Usage rates for 65-74 year-olds with tertiary education are generally in line with those of the overall population, and in leading countries approach the usage rates among 16-24 year-olds. Differences between high and low educational attainments among 65-74 year-olds are particularly large in Hungary, Poland and Spain (OECD, 2014c).

Figure 3.8. **Internet users by age, 16-24 and 65-74 year-olds, 2014**

As a percentage of population in each age group



Notes: Unless otherwise stated, Internet users are defined for a recall period of 12 months. For Switzerland, the recall period is 6 months. For the United States, no time period is specified. For the United States, data refer to individuals aged 18 and over living in a house with Internet access, and to age intervals of 18-34 instead of 16-24 and 65 and over, instead of 65-74. Data are sourced from the US Census Bureau. For Australia, data refer to 2012/13 (fiscal year ending in June 2013) instead of 2013, and to individuals aged 65+ instead of 65-74. For Canada, Japan and New Zealand, data refer to 2012 instead of 2014. For Chile, Israel, the United States and Colombia, data refer to 2013 instead of 2014. For Israel, data refer to individuals aged 20 and over instead of 16-74, and 20-24 instead of 16-24. For Colombia, data refer to individuals of 12 years old and above instead of 16-74, 12-24 year-olds instead of 16-24, and 55 year-olds and over instead of 65-74. For Japan, data refer to 15-69 year-olds instead of 16-74, 15-28 year-olds instead of 16-24, and 60-69 year-olds instead of 65-74.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224896

According to the 2012 OECD Programme for International Student Assessment (PISA), 90% of students surveyed first accessed the Internet before the age of 13. On average, for countries where data are available, less than 0.5% of 15 year-olds reported never having accessed the Internet.

Age of first access to the Internet varies widely across countries. More than one third of students started using the Internet aged 6 or younger in Denmark and the Netherlands. In the Nordic countries, the Netherlands and Estonia, 80% of students accessed the Internet before the age of 10, as opposed to 30% in Greece and the Slovak Republic.

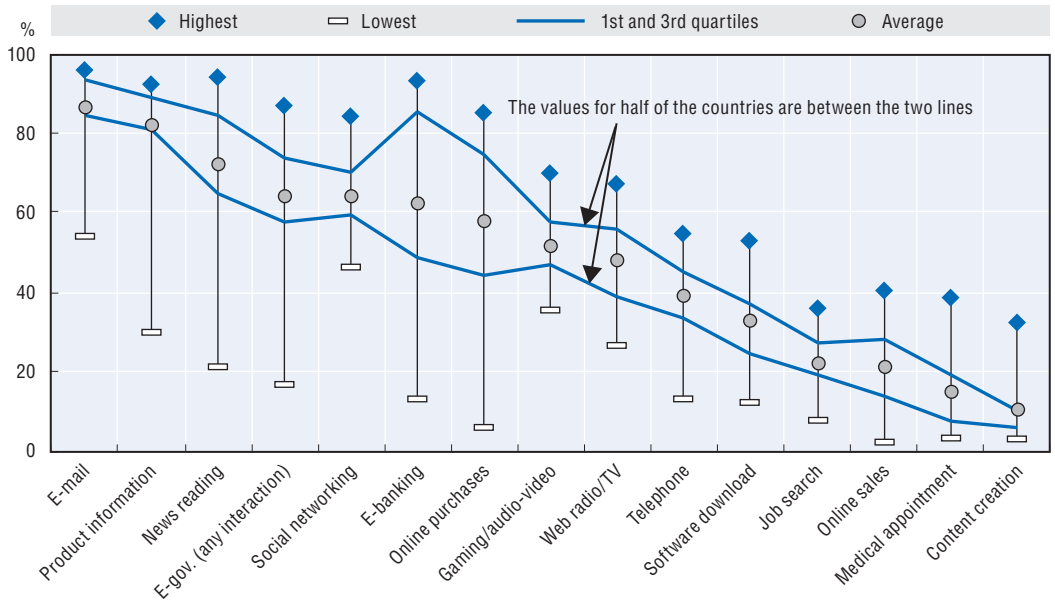
Early use of the Internet appears to be correlated with time spent online by 15 year-olds, across countries. In Australia, Denmark and Sweden, the average student spends about 4 hours online on a typical weekday, whereas students in Korea spend less than 1.5 hours. Students use the Internet mostly outside of school. Time spent online at school amounts to slightly more than half an hour per day in the OECD, with little variation among countries.

Over 2013-14, on average 87% of Internet users reported sending emails, 82% used the Internet to obtain information on goods and products, and 72% read online news. While 58% of Internet users ordered products online, only 21% sold products over the Internet (Figure 3.9).

Activities such as sending emails, searching product information or social networking show little variation across all countries. However, the shares of Internet users performing activities usually associated with a higher level of education (e.g. those with cultural elements or more sophisticated service infrastructures), tend to show larger cross-country variability. This is the case, for example, for e-banking, online purchases, news reading and e-government.

Figure 3.9. **The diffusion of selected online activities among Internet users, 2013-14**

Percentage of Internet users performing each activity



Notes: Unless otherwise stated, a recall period of three months is used for Internet users. For Australia, Canada, Chile, Japan, Korea, Mexico and New Zealand, the recall period is 12 months. For Switzerland, the recall period is six months. For the United States, no time period is specified. For web-based radio/television, data refer to 2012. For job search and software download categories, data refer to 2013. For online purchases and e-government categories, the recall period is 12 months instead of three months, and data relate to individuals who used the Internet in the last 12 months instead of three months. For countries in the European Statistical System and Mexico, data refer to 2014. For Australia, Canada and New Zealand, data refer to 2012. For Chile, Israel and Japan, data refer to 2013. For Australia, Chile and New Zealand with regard to interactions with public authorities, data refer to obtaining information from public authorities. For Japan, data refer to individuals aged 15-69. For job search, data refer to 2012.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, April 2015.

StatLink http://dx.doi.org/10.1787/888933224908

The breadth of activities performed on the Internet can be regarded as an indication of user sophistication. In 2013, the average Internet user performed 6.3 out of the 12 activities selected, up from 5.4 in 2009. This figure ranges from 7.5 to 8 activities in the Nordic countries and the Netherlands, to 5 activities or less in Greece, Italy, Korea, Poland and Turkey.

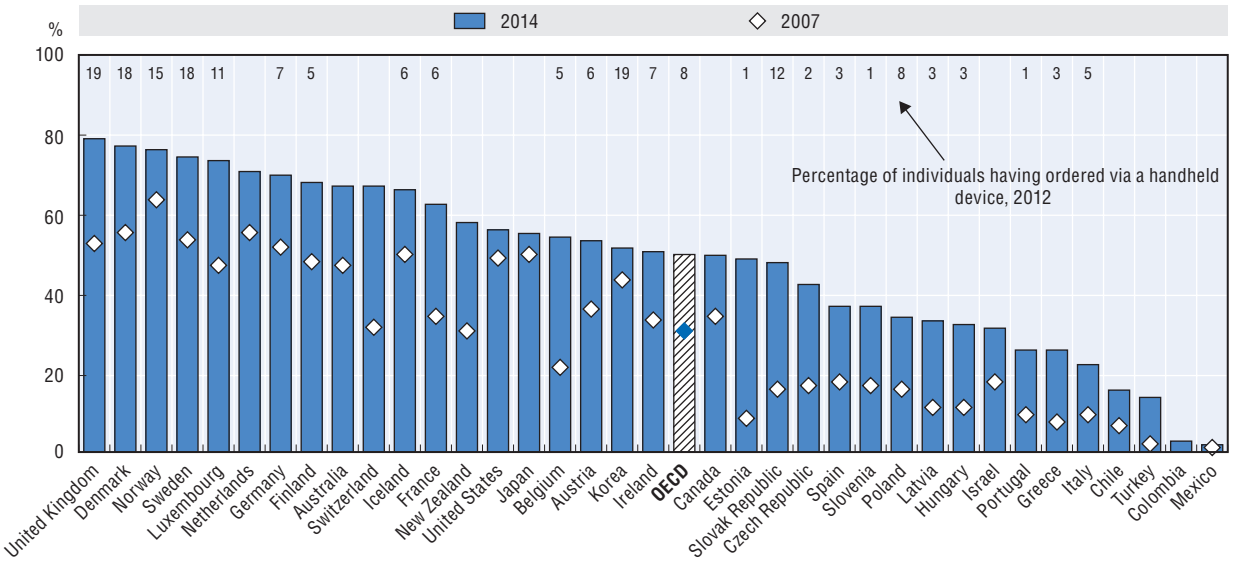
Education plays a key role in shaping the range of activities on the Internet. While users with tertiary education perform on average 7.3 different activities, those with lower secondary education and below perform only 4.6 activities. Differences by level of education are particularly high for Belgium, Hungary, Ireland, Korea and Turkey.

Half of individuals in OECD countries bought products online in 2014, up from 31% in 2007 (Figure 3.10). The increase in online purchases for this period was particularly large in Belgium, Estonia, France, the Slovak Republic and Switzerland. This trend is very likely to continue in the near future and has already disrupted traditional distribution channels for some categories of products. The rapid diffusion of smart mobile devices has resulted in a growing number of individuals buying products via their mobile device.

The share of online purchases varies widely across countries as well as across different product categories, with age, education, income and experience all playing a role in determining the uptake of e-commerce by individuals.

Figure 3.10. **Diffusion of online purchases including via handheld devices, 2007 and 2014**

Individuals having ordered goods or services online as a percentage of all individuals



Notes: For Australia, data refer to 2012/13 (fiscal year ending in June 2013) instead of 2013. For 2007, data refer to 2006/07 (fiscal year ending in June 2007), and to individuals aged 15 and over instead of 16-74 year-olds. For Canada, data refer to 2012 and relate to individuals who ordered goods or services over the Internet from any location (for personal or household use). For Chile, data refer to 2009 and 2013. For Israel, data refer to all individuals aged 20 and over who used the Internet for purchasing all types of goods or services. For Japan, data refer to 2013 and to individuals aged 15-69 instead of 16-74 year-olds. For Korea, data refer to 2013 instead of 2014. For online purchases via handheld devices, data refer to the population aged 12 and over. This data point is an OECD estimation based on data sourced in the Survey on Internet Usage 2012. In 2013, the share of individuals buying via handheld devices reached 35.5%. For New Zealand, data refer to 2006 and 2012 and relate to individuals who made a purchase through the Internet for personal use, which required an online payment. For Switzerland, data refer to 2005 instead of 2007. For the United States, data originate from May 2011 and September 2007 PEW Internet Surveys and cover individuals aged 18 or more. For Colombia, data refer to individuals of 12 year-olds and above instead of 16-74.

Sources: OECD, ICT Database; Eurostat, Information Society Statistics and national sources, March 2015.

StatLink http://dx.doi.org/10.1787/888933224913

In Denmark, Norway and the United Kingdom, more than 75% of adults have made purchases online. In Chile and Turkey, the percentage is between 10% and 20% and in Colombia and Mexico it is below 5%. However, these shares increase and the differences between leading and lagging countries narrow when only the population of Internet users is considered. In Denmark, Germany and the United Kingdom, 80% or more of Internet users make purchases online, against less than 30% in Chile, Estonia or Turkey and below 10% in Mexico.

The most common items purchased online are travel and holiday services (about half of online consumers on average), tickets for events, digital products and books. Other categories, such as food and grocery products, have experienced fast growth in recent years. The diffusion of different categories of products via online purchase is likely to depend on income levels, consumer habits, the availability of e-commerce channels by local providers, and the price strategies of e-selling firms.

Security and privacy are among the most challenging issues facing online services and the development of e-commerce. In 2009, security was cited as the main reason for not buying online for over one third of Internet users in the European Union who had not made any purchases online. Privacy concerns accounted for a slightly smaller share (30%). The high variation in perceptions of security and privacy risks across countries with comparable degrees of law enforcement and technological know-how suggests that cultural attitudes towards online transactions play a significant role.

There has been a significant rise in the use of cloud computing services among Internet users. The cloud functions as a virtual storage space for documents, pictures, music or video files, which are saved or shared with other users. Cloud computing is also meeting demand for flexibility and ease of access to software and content, which can be accessed by users irrespective of location or time.

In 2014, uptake of cloud computing among Internet users in European countries ranged from 13% in Poland to 46% in Denmark. In all countries, the propensity to use cloud computing services is much higher among younger and more educated people (Figure 3.11). The share of Internet users paying for these services remains low and ranges from 10% in Norway to less than 1% in Slovenia.

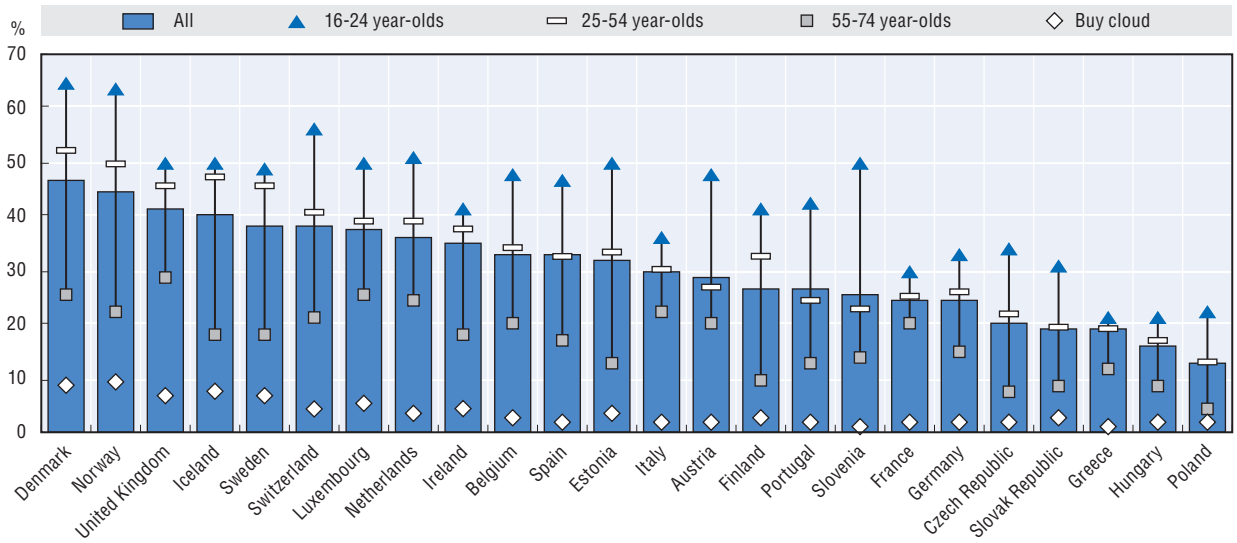
The share of individuals using e-government services on the Internet has increased in recent years, but remains widely dispersed across countries – ranging from 88% in Iceland to less than 40% in Chile, Italy and Poland in 2014. Explanations for these differences include insufficient infrastructure and supply of e-services by public authorities, and structural issues linked to institutional, cultural or economic factors.

The perception and utility of the services provided by public authority websites and their coherence with individual user needs are also key elements. Ease of access and use of a website appear to be strategic factors fostering usage and user satisfaction (Figure 3.12).

Results from the 2012 OECD Programme for International Student Assessment (PISA) show that 70% of students in the OECD use the Internet at school. This share ranges from 97% in Denmark to 40% in Turkey. In Japan and Mexico, 30% of students stated that Internet access was unavailable in schools compared with the OECD average of 10%. In Korea, more than 40% of 15-year-olds reported that they did not use the Internet at school, despite its availability.

Figure 3.11. **Use of cloud computing by individuals in selected OECD countries by age class, 2014**

As a percentage of Internet users



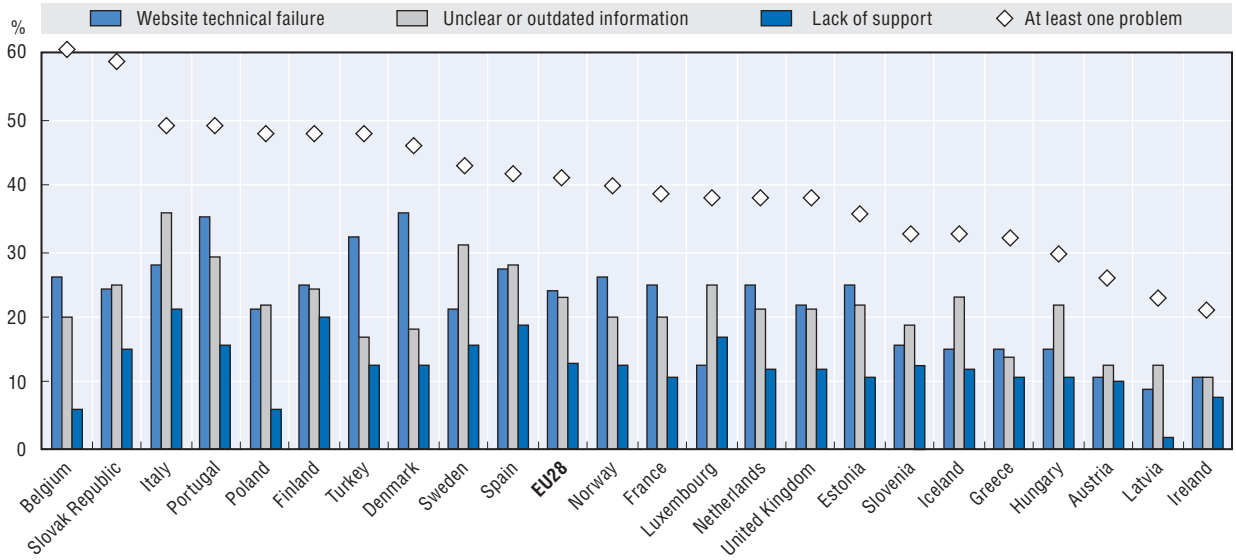
Notes: Cloud computing refers to the use of storage space on the Internet to save or share documents, pictures, music, video or other files. "Buy cloud" refers to purchased Internet storage space or file-sharing services.

Source: Eurostat, Information Society Statistics, January 2015.

StatLink http://dx.doi.org/10.1787/888933224920

Figure 3.12. **Problems with the use of e-government services, 2013**

Percentage of individuals having used e-government services in the last 12 months



Note: The category "At least one problem" includes website technical failure, unclear or outdated information, lack of support (online or offline) and other problems (unspecified).

Source: Eurostat, Information Society Statistics, March 2015.

StatLink http://dx.doi.org/10.1787/888933224930

In most countries, the majority of students use computers for practising and drilling sessions, once or twice a month. The percentage of students using computers for this purpose on a daily basis remains low, at 12% in Denmark, 10% in Norway, and around 2% in Finland and Germany.

Box 3.1. **Achieving public sector transformation through digital technologies**

Public sectors across OECD countries are undergoing a profound transformation as they capitalise on opportunities provided by digital technologies. Key objectives shaping this transformation process include improved efficiency, effectiveness, and governance of public service design and delivery. Governments are expected to shift from a citizen-centred to a citizen-driven service delivery approach, which would enable citizens and businesses to determine their own needs and address them in partnership with public authorities. Where such change does not occur as expected, individuals and organisations can exert pressure through the use of digital technologies, including online petitions, mobile applications, open (government) data, crowdfunding and social media.

Few technological shifts illustrate this new reality better than social media. The majority of governments around the world now draw on social media to communicate and engage with their citizens. As of November 2014, the office representing the top executive institution (head of state, head of government or government as a whole) in 28 out of 34 OECD countries had a Twitter account, and 21 had a Facebook account. Some governments have achieved significant popularity rates (calculated by comparing the number of Twitter followers to the domestic population; see Chapter 1, Figure 1.17) (Androsoff and Mickoleit, 2015).

However, OECD analysis highlights uncertainty among government institutions regarding how to exploit social media to improve public services or to create trusted relationships with citizens. Moreover, social media do not automatically empower all societal groups equally. In particular, level of education determines the probability of social media usage in many OECD countries. The situation calls for context-dependent strategies, as well as better impact assessment methods built around the public sector's unique goals and objectives (OECD, 2014b).

The application of digital technologies to better respond to the changing context implies new governance frameworks, funding arrangements and skills. The purpose is not to introduce new digital technologies into public administrations or to simply transfer existing services online ("e-government"); it is to leverage technology to re-engineer existing processes and transform the delivery of public services, and to integrate it in public sector modernisation ("digital government"). In order to address the challenges of digital transformation and its associated new dilemmas (e.g. professional ethics, issues relating to security and control of personal data), governments need to formulate and implement digital government strategies and firmly embed them in mainstream modernisation policies.

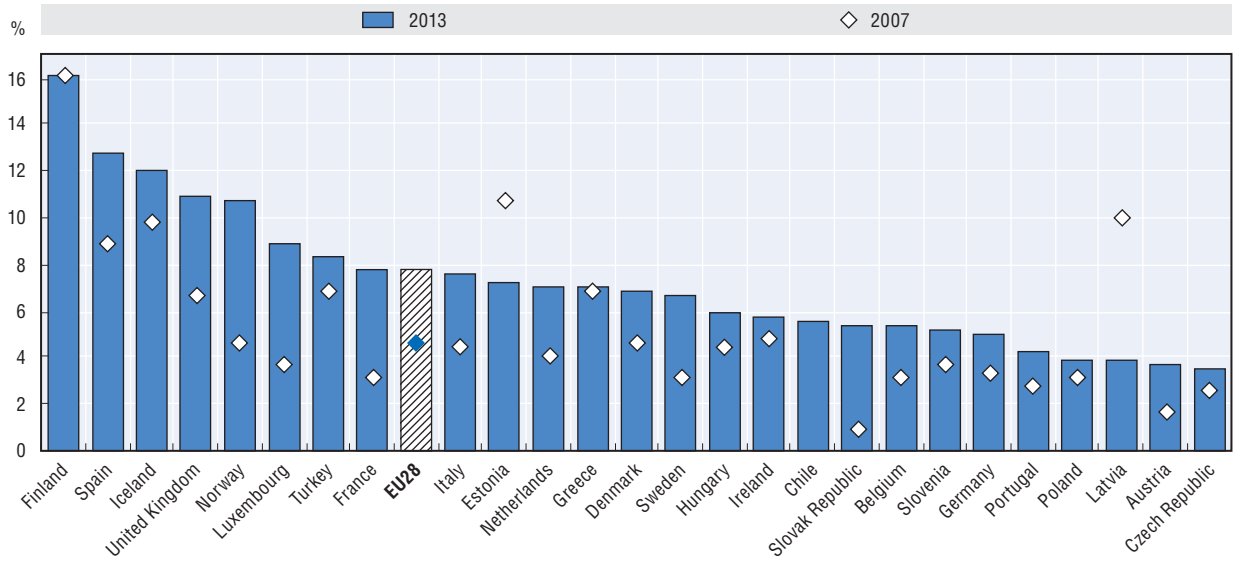
Better frameworks for monitoring and realising benefits are also essential, and leading OECD countries have turned to business case approaches to review and guide government IT investment decisions. The OECD Council Recommendation on Digital Government Strategies was adopted in 2014 to assist governments in establishing those frameworks and guide them through digital transformation efforts towards the realisation of digital opportunities (OECD, 2014d).

Finally, many governments use open government data (OGD) as an essential strategic enabler to increase public sector transparency and deliver societal and economic benefits. Reuse of government data allows NGOs to better monitor government activities, companies to create new types of commercial content and services, individuals to make more informed choices in their daily lives, and governments to work with citizens to create more liveable public spaces. Countries are capitalising on open data opportunities, regardless of their level of development. However, many legal, institutional and policy-related issues still need to be addressed before governments and citizens can fully capture the value of data usage to transform operations, services and policy making, and make public services and public sectors more data-driven and inclusive (OECD, 2013a).

Over the last few years, ICTs have contributed to a wider array of learning opportunities and education programmes through the development of online courses, in particular, massive open online courses (MOOCs). In 2013, 7.8% of Internet users in the European Union followed an online course compared with 4.7% in 2007 (Figure 3.13). This percentage varied from 16% in Finland to less than 3% in the Czech Republic.

Figure 3.13. **Individuals who attended an online course, 2007 and 2013**

As a percentage of individuals who used the Internet in the last three months



Notes: For Chile, data refer to 2012, with a recall period of 12 months. For Poland, data refer to 2008 and 2011 instead of 2007 and 2013.

Source: OECD, ICT Database; Eurostat, Information Society Statistics, April 2015.

StatLink http://dx.doi.org/10.1787/888933224942

3.2 New and evolving business models and markets

Key digital trends influencing business models and markets

Several digital trends are driving the emergence of new business models and the transformation of established markets. Three deserve particular attention: the intensity of use and variety of activities carried out on smartphones; the surge in mobile social networking; and the harnessing of large volumes of data, known as "big data", through data analytics to drive value creation and foster new products, processes and markets (i.e. data-driven innovation) (see OECD, 2015a). Each of these plays a role in the evolution of business models and in driving transformation in established markets.

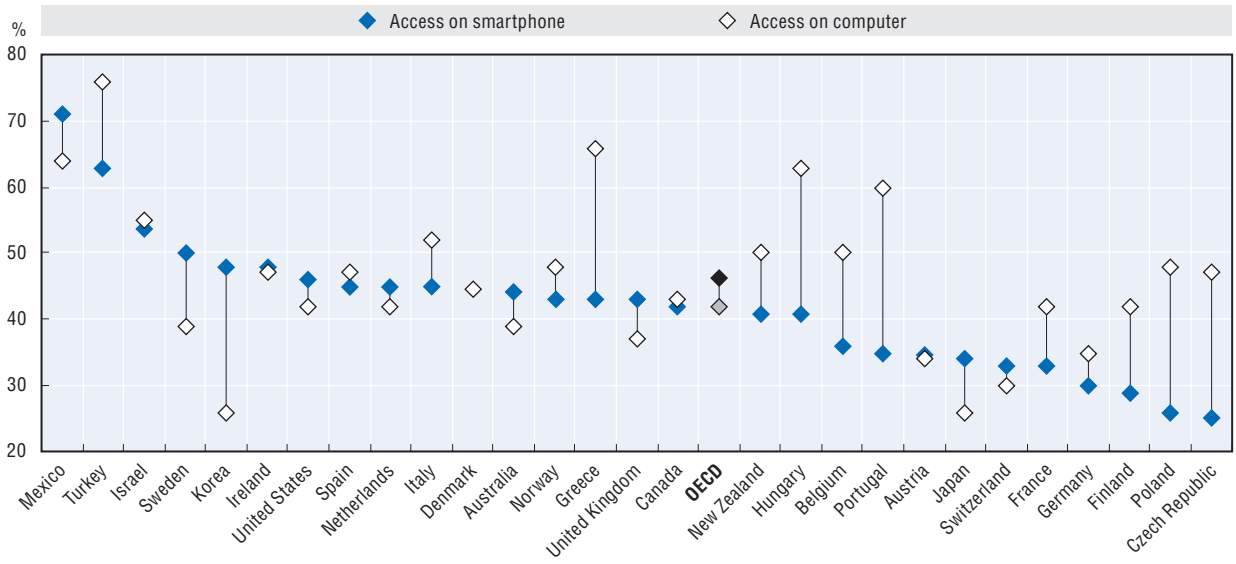
Smartphone penetration and activities are growing fast. According to Our Mobile Planet (2013), average smartphone penetration in the OECD grew by 30% in 2012-13, reaching almost 50% in 2013. Individuals owning a smartphone perform an increasing variety of activities, with increasing intensity. Our Mobile Planet (2013) state that activities carried out on smartphones other than making or receiving a phone call or sending an SMS have increased by 24% over 2011-13. Some activities traditionally carried out on a computer, such as browsing the Internet, emailing or accessing a social network, are also increasingly carried out on smartphones. More sophisticated activities, including online banking, mobile purchases and job search, are also experiencing fast growth.

Many smartphone activities are carried out on dedicated mobile applications (apps). Over several years, social networking and gaming applications have dominated the top ranks of application downloads in the main app stores. However, travel, mobility and retail apps have made a recent appearance among the most downloaded apps (TechCrunch, 2014), indicating the increasing impact of digital services delivered via mobile apps in a wider array of sectors.

Online social networking has largely gone mobile, both in terms of network access and content sharing. In 2013, 42% of smartphone users in OECD countries accessed social networks on their smartphones several times per day (Figure 3.14). This represents a 19% increase from 2012. The share of people accessing social networks from their computer was still slightly higher in 2013 (46%), but has stagnated since 2012. Several central elements of social networking, such as having an online identity, online and mobile sharing of content (Figure 3.15), and frequent status updates, play an important role in preparing the ground for new business models to flourish, notably those building on collective consumption in the sharing economy and exploring the possibilities of collaborative production.

Figure 3.14. **Access to information on social networks, 2013**

As a percentage of smartphone users who use the Internet



Note: No data available for Chile, Estonia, Iceland, Luxembourg, the Slovak Republic, or Slovenia. The sample covers private smartphone users who use the Internet in general. "Access" refers to multiple visits per day.

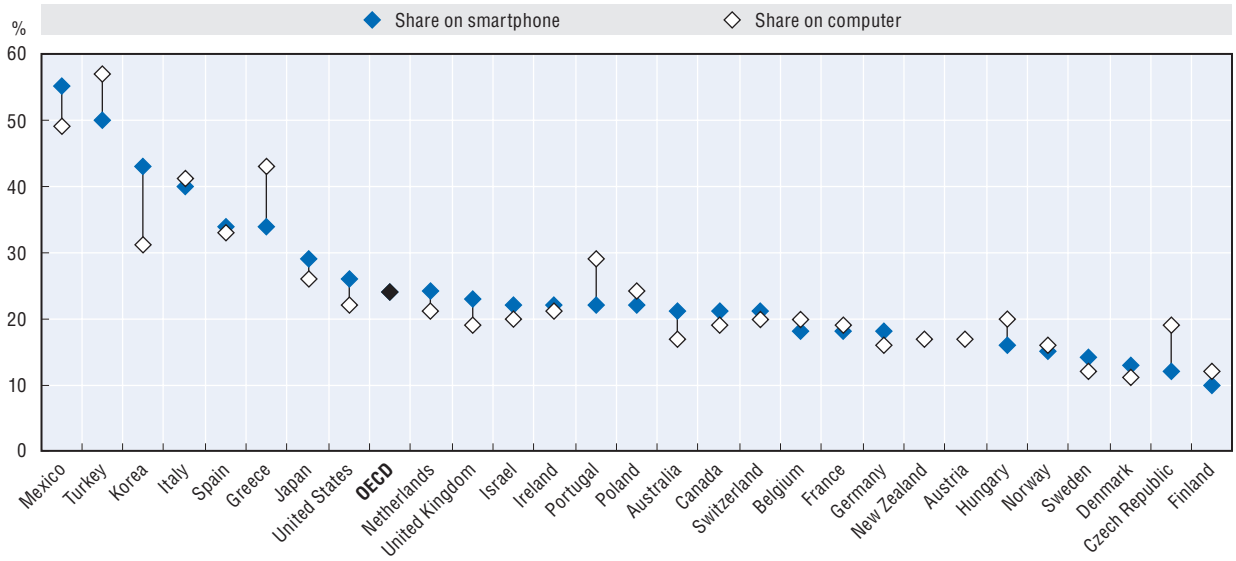
Source: Our Mobile Planet, 2013.

StatLink http://dx.doi.org/10.1787/888933224958

Many mobile applications not only function with but also produce data, which can be used by innovative entrepreneurs and businesses to offer new services. The exponential growth in data generated and collected, together with the pervasive power of data analytics thanks to cloud computing in particular, has enabled the exploitation of data for innovation in ways previously unheard of (OECD, 2015a). Smartphones are an important source of data, however data are increasingly generated by other smart devices, embedded in the Internet of Things and enabled by machine-to-machine communication (M2M) (see Chapter 6). The data generated by these devices are collected by and used in numerous mobile applications and services (increasingly in real time), such as online maps, navigation and recommendation systems. In 2013, for instance, 68% of smartphone users in the OECD looked up directions or used a map on their smartphone, up 18% from 2012; while over 32% searched for information about local businesses, and 14% visited the businesses afterwards (Figure 3.16). Beyond its use for online mobile maps, geo-locational real-time data promotes innovation in areas such as peer-to-peer mobility services and multichannel retailing.

Figure 3.15. **Sharing of information on social networks, 2013**

As a percentage of smartphone users who use the Internet



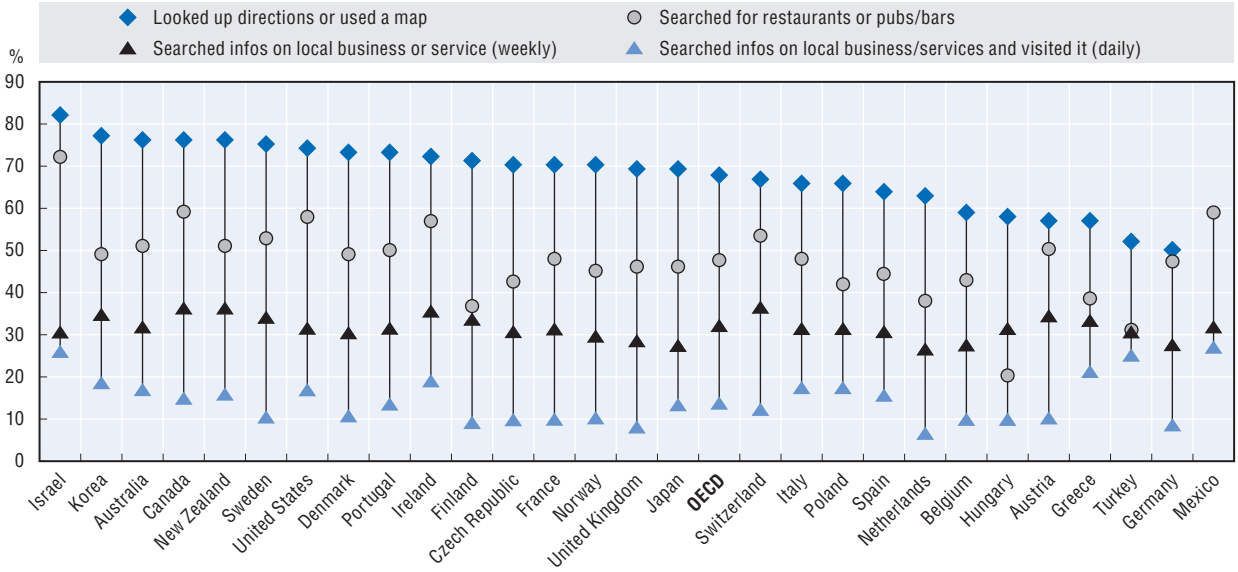
Note: No data available for Chile, Estonia, Iceland, Luxembourg, the Slovak Republic, or Slovenia. Sample covers private smartphone users who use the Internet in general. "Share" refers to daily visits.

Source: Our Mobile Planet, 2013.

StatLink http://dx.doi.org/10.1787/888933224968

Figure 3.16. **Use of location-based services on smartphones, 2013**

Percentage of smartphone users who use the Internet



Note: No data available for Chile, Estonia, Iceland, Luxembourg, Slovak Republic, or Slovenia. The sample covers private smartphone users who use the Internet in general.

Source: Our Mobile Planet, 2013.

StatLink http://dx.doi.org/10.1787/888933224978

New and evolving businesses models and markets

The growing penetration of mobile Internet and the variety of frequently used mobile applications are influencing incumbent business models in established markets and enabling the emergence of new business models. Transformative effects of digitisation and the Internet in markets such as advertising, content, health and e-commerce have been discussed in earlier OECD publications (OECD, 2012).

In the meantime, the Internet, and the use of data and mobile applications in particular, is driving ongoing market transformations (see the following sections on retail and banking). New sharing economy business models that enable collective consumption are being examined in markets previously less concerned with the Internet (mobility and accommodation), alongside evolving business models that solicit the public for research and development, or for funding. Many of these business models rely on data-driven platforms that provide services based on data collection and analysis. The providers of such platforms can yield substantial profit margins by exploiting network effects and multi-sided markets (see Box 3.2). Some of the firms that rely on Internet-enabled and data-driven business models, discussed below, have overcome substantial entry barriers and, in many countries, are operating within legal and regulatory frameworks not adapted to their new business models. The resulting issues for policy makers are discussed here, where appropriate.

Box 3.2. **Data favours the creation of multi-sided markets**

Two or multi-sided markets are "roughly defined as markets in which one or several platforms enable interactions between end-users and try to get the two or multiple sides 'on board' by appropriately charging each side" (Rochet and Tirole, 2005). Established and emerging service platforms such as Amazon, eBay, Google, Facebook, Apple's iOS, Microsoft and TomTom are active in multi-sided markets. eBay provides an online marketplace for sellers and buyers; Amazon constitutes another type of marketplace, albeit closer to the retail model; Facebook and Google provide services to consumers and advertisers; Apple's iOS provides a platform that links application developers and consumers ("the app economy") and musicians and consumers (iTunes); Microsoft's Xbox platform is positioned in between consumers and game developers; and TomTom's navigation services are provided to users and to traffic management providers. Although these are very different examples, one commonality is that data about user behaviour are crucial for managing the service platform and to provide attractive services in multi-sided markets.

The general notion is that success on one side of the market reinforces success on the other. For example, consumers that appreciate customised search results and ads provided by Google's search and webmail platform will spend more time on the platform. This allows Google to gather even more valuable data about consumer behaviour, and to further improve services for consumers as well as advertisers. These self-reinforcing effects may increase with the number of applications provided on a platform (e.g. bundling email, messaging, video, music and telephony). Data gathered while providing one application can be used for improving other applications, thereby increasing the number of markets that interact. The commercial relationship between service platforms and consumers can become two-way, when users are explicitly rewarded for sharing data about their behaviour, preferences and social networks. Service platforms need not rely on consumer data only. Service platforms may procure (raw) data, information and intelligence from third parties. Conversely, service platforms can sell their own data, information and intelligence (partly, aggregated, with a delay, etc.) to third parties.

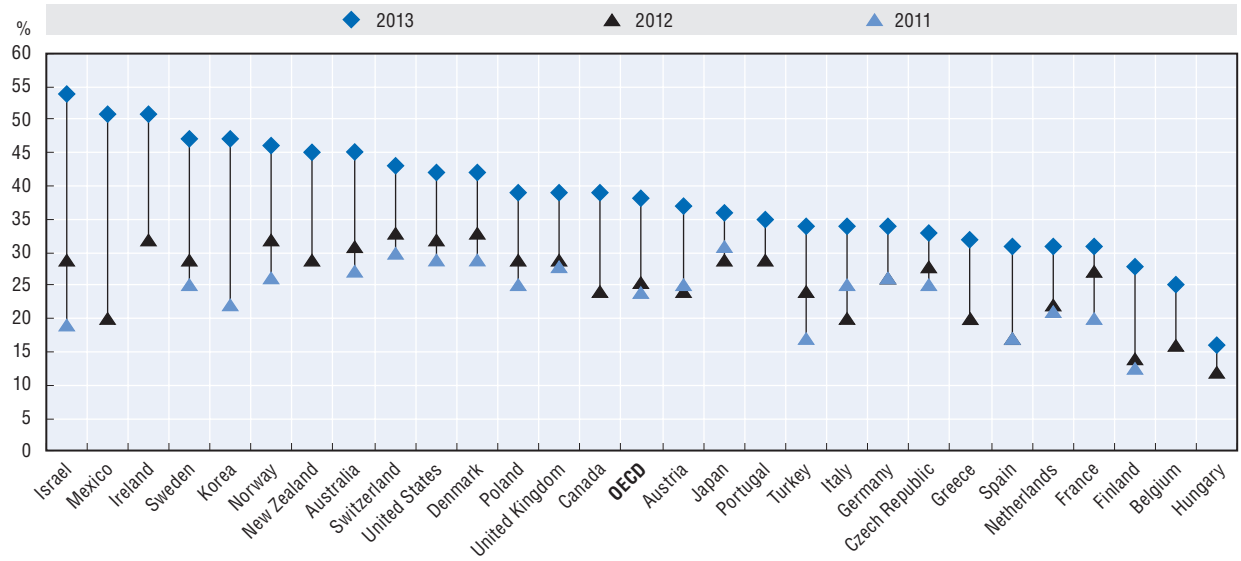
Source: OECD, 2015a.

Ongoing transformations in retail

A growing number of smartphone users across the OECD purchase goods and service on their phones. The share of smartphone users who ordered a good or a service on their mobile device has grown from 24% in 2001 to 38% in 2013 (Figure 3.17). Product information gathered on smartphones also influences purchasing decisions both online and offline. According to Our Mobile Planet (2013), 26% of OECD smartphone users who researched a product chose to buy it on their smartphone, 32% purchased it offline and 40% used a computer. Large firms are responding to these trends through multichannel retailing (i.e. increasing their presence in stores, social media and online retailers). From the consumer perspective, m-commerce and mobile product information gathering translate largely into greater choice, convenience and reduced transaction costs, notably in product search.

Figure 3.17. **Purchasing of goods or services on smartphones**

Percentage of smartphone users who use the Internet



Note: No data available for Chile, Estonia, Iceland, Luxembourg, the Slovak Republic, or Slovenia. The sample covers private smartphone users who use the Internet in general.

Source: Our Mobile Planet, 2013.

StatLink http://dx.doi.org/10.1787/888933224989

For firms, in particular small and medium-sized enterprises (SMEs), the implications of these trends are mixed. SMEs tend to lack sufficient resources to develop effective marketing and sales strategies for multiple channels and in different countries. These developments occur in a context where cross-border e-commerce is significantly lower among SMEs than large firms. In EU28 countries, for example, 12% of large firms (above 250 employees) sell online across borders, but the same is true for only 6% of medium-sized firms (50-249 employees) and 3% of small firms (10-49 employees) (Eurostat, 2013).

Several barriers may explain the moderate uptake of e-commerce among SMEs, in particular across borders. One third of Internet users in the EU cite security concerns as the main reason (OECD, 2014c), while consumer mistrust often stands in the way of cross-border purchases. In addition, several supply-side obstacles need to be addressed, notably trade and regulatory barriers. The latter have been identified by 12% of SMEs in the Euro area as the most pressing problem for accessing foreign markets in 2012, up from

7% in 2009. Some of the most common barriers to foreign market access, including via e-commerce, are (OECD, 2009, 2013b):

1. high customs administration and shipping costs, which obstruct in particular long-tail economic transactions, and thus SMEs
2. high tariffs, such as excessive taxes applied to imported goods; arbitrary tariff classifications,[2] or competitors with preferential tariffs via regional trade agreements, unfavourable quotas and embargoes
3. inadequate property right protection, including copyrights, patents and trademarks
4. shortage of working capital to finance exports, information to locate and analyse markets, and managerial time, skills and knowledge.

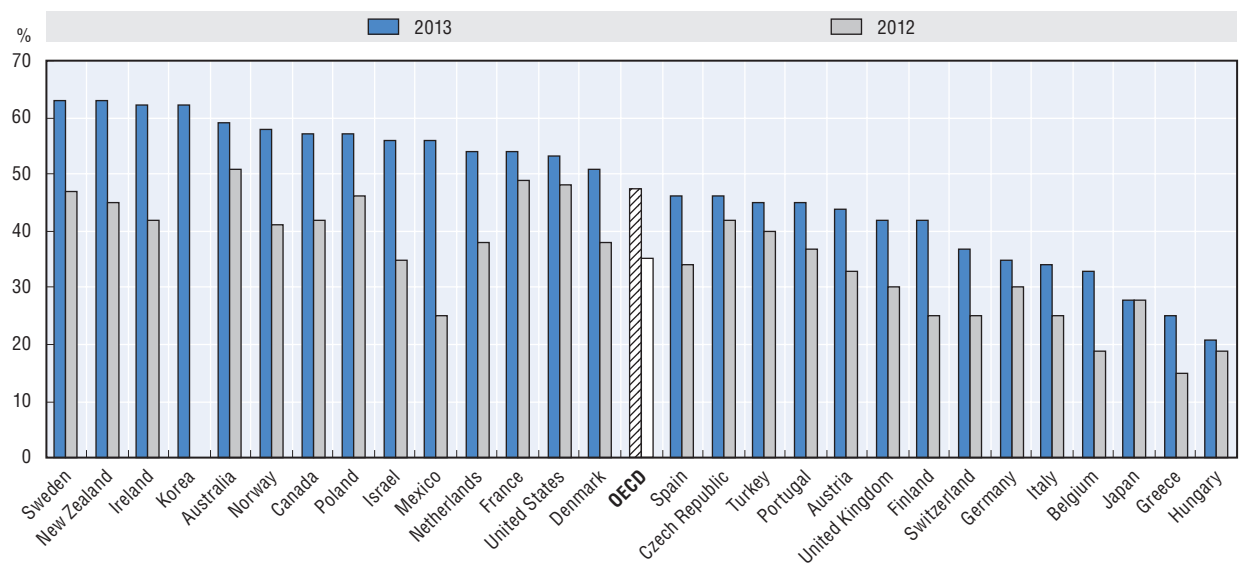
Policy measures to reduce these barriers will benefit especially SMEs, which tend to have limited resources and skills to tackle obstacles. At present, SMEs rely increasingly on e-commerce intermediaries and marketplaces such as Amazon or eBay. While these intermediaries make it easier for SMEs to access foreign markets and benefit from large network effects and economies of scale, the key role of online intermediaries in online and mobile markets may result in SMEs becoming dependent on such players.

New competition in banking

Retail banks are facing continuous shifts in demand through online and mobile banking, as well as new competition from online peer-to-peer (P2P) lending platforms. More than half of Internet users in OECD countries use online banking, and mobile banking is catching up. In 2013, 60% of Internet users in OECD countries used online banking, up from 42% in 2011 and 31% in 2007 (OECD, 2012, 2014c). Uptake of mobile banking and other finance-related activities on smartphones have also increased at a similar rate, from 35% of smartphone users in 2012 to 47% in 2013 (Figure 3.18).

Figure 3.18. **Mobile banking uptake**

Percentage of smartphone users who use the Internet and perform online banking or other finance-related activities on their smartphone



Notes: No data available for Chile, Estonia, Iceland, Luxembourg, the Slovak Republic, or Slovenia. The sample covers private smartphone users who use the Internet in general.

Source: Our Mobile Planet, 2013.

StatLink http://dx.doi.org/10.1787/888933224998

The rise of online and mobile banking is changing market boundaries and the parameters for competition in traditional retail banking. While a network of local branches represents a key competitive asset for traditional banks, physical proximity to customers is not an issue for online banks. Instead, their boundaries are defined not by geography but by technology, regulation and marketing budgets (PwC, 2014a). In reaction to higher competition from online banks, offline banks can either specialise in place-based business (e.g. farmers) or step up their response to online competition, an option that involves significant costs. The expected trend is towards a reduction in local bank branches. In heavily banked markets such as the United States, 20% of local branches are expected to disappear by 2020, mostly to the detriment of smaller regional and community banks (PwC, 2014a).

New competition for retail banks also comes from P2P lending. With an environment of low interest rates and tighter credit conditions, P2P lending has grown quickly into a substantial market. P2P lending platforms match borrowers and lenders, mostly via online auctions, and offer better conditions to both parties than most banks. Lenders apply for a loan and, if accepted, are categorised within respective risk profiles. Borrowers can choose the risk profile of the loans they buy, mostly in slices to diversify risk. So far, P2P lending platforms have targeted primarily the consumer credit market, with business loans representing a small share of the two largest P2P lending platforms – Prosper and Lending Club. Recently, however, platforms such as Funding Circle have started to focus on small business lending. Other more specialised platforms target markets as diverse as real estate (Relendex, Realtymugol, Fundrise) or student loans (Prodigy Finance).

Box 3.3. **P2P lending platforms**

The largest P2P lending market is based in the United States and is currently dominated by two platforms, Prosper and Lending Club, which combined hold 98% of issued P2P loans to date. These successful P2P lending platforms attract not only individual lenders, but also institutional investors. For example, only one third of participants in Lending Club are retail investors, the rest are institutional investors and rich individuals (*Economist*, 2014).

From its inception in 2007 to the end of 2014, the Lending Club has issued USD 7.6 billion in loans. While this represents only a small share of the USD 3 trillion consumer lending market in the United States, the amount of loans issued by the platform doubled steadily each year (Lending Club, 2014). In August 2014, Lending Club was the first P2P lending platform to file for an initial public offering at a USD 5 billion valuation, although some consider this to be overrated (Cinelli, 2014).

Loans issued on P2P lending platforms are mostly consumer loans. Data from Lending Club show that 61% of loans are used for refinancing, including 22% to pay off credit card debt, 9% for other consumption purposes and 6% for home improvements. Business loans account for only 2%, and are generally found to be significantly more expensive on P2P lending platforms than from traditional lenders (Mach, Carter and Slattery, 2014).

Sources: Cinelli, 2014; *Economist*, 2014; Lending Club, 2014, Mach, Carter and Slattery, 2014.

P2P lending platforms have not yet come under serious stress and it is unclear whether they would survive, for example, a financial crisis. If their strong growth continues, and if they prove able to deal with economic uncertainties, they may become a potentially disruptive competitive force in consumer credit markets in the near future.

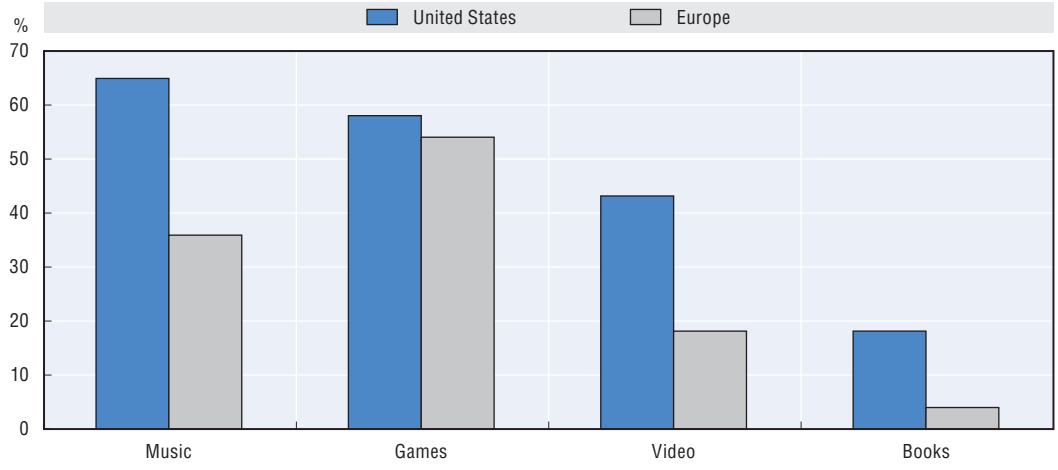
P2P lending has attracted little attention from regulators to date. The United Kingdom is among the few countries to have taken a pro-active stance on regulating P2P lending platforms. The "Financial Conduct Authority's regulatory approach to crowdfunding over the Internet, and the promotion of non-readily realisable securities by other media" (FCA, 2014) provides clear rules and regulation, addressing industry-specific risks and operational features. Important issues covered in this framework include:

- *Minimum capital requirements*. Platforms are required to hold a minimum amount of regulatory capital to be able to withstand potential financial shocks.
- *Successor loan servicing arrangements*. Platforms must undertake steps to ensure that loans continue to be administered if the platform goes out of business.
- *Dispute resolution rules*. Investors have the right to complain to the platform and, as a second step, to the Financial Ombudsman Service. Disputes follow a standards-based process.
- *Client money protection rules*. Platforms are subject to client money rules that require all firms holding client money in relation to investment business to ensure its adequate protection.
- *Disclosure rules*. Platforms are required to communicate to investors all information they require to make informed investment decisions, in a manner that is fair, clear and not misleading.
- *Ongoing reporting*. Platforms are obliged to report regularly on their financial position, client money held, complaints and details of loans arranged each quarter.

Content and creative industries

The availability of digital online content and consumption continues to rise. For example, Spotify, an online music streaming service, offers over 20 million tracks licensed globally, and adds on average over 20 000 songs per day.[3] The iTunes Store, one of the most popular online music stores, available in 119 countries, offers a selection of over 26 million songs (Apple, 2013). However, despite the transformations experienced by major content markets, there remains room for dematerialisation (Figure 3.19).

Figure 3.19. **Dematerialisation of major content markets, 2013**



Source: IDATE, 2014.

StatLink http://dx.doi.org/10.1787/888933225006

User-created content, notably images and video, continues to grow strongly. In 2013, the photo-sharing site Flickr reached an average of 1.6 million photos uploaded daily to its platform.[4] In September 2013, Facebook announced that its users had uploaded a total of 250 billion pictures to the platform (Wagner, 2013); and Instagram recently announced that its members had published 20 billion photos, translating into an average of 70 million uploads per day.[5] YouTube, one of the most popular online video-sharing platforms reported in mid-2014 that users watch (stream) over 6 billion hours of video each month on their platform and upload 100 hours of video to YouTube every minute.[6]

Digital content is increasingly consumed and shared on mobile devices. In 2013, 70% of smartphone users in the OECD accessed a social network and 24% shared information about themselves on a daily basis (Our Mobile Planet, 2014). Mobile social networking also seems to be a driver for other types of mobile content consumption, such as watching videos or reading news on smartphones.

The above-mentioned trend adds to the ongoing migration of newspaper from print to digital. Over the past five years, printed newspaper circulation declined by 10% in North America and by 30% in Europe. Accordingly, print advertising declined by 23% and 18% in both regions. Today, around 2.5 billion people read newspapers in print and 800 million on digital platforms worldwide (WAN-IFRA, 2014).

Television is also undergoing a transformation, with delivery over the Internet targeted to individuals and increased flexibility. As opposed to analogue linear broadcasting delivered to a fixed television within a household, audio-visual content delivered over the Internet allows users to view films and programmes of their choice on any device at any time. Netflix, for example, claims to offer over 10 000 movies and TV titles streaming-on-demand via its platform in the United States.[7] These offers are increasingly being picked up on mobile devices. In November 2014, for the first time, Americans spent more time on mobile devices (177 minutes per day on average) than in front of a TV (168 minutes) (Flurry, 2014).

Advertising, a main revenue source in several of the above markets, is following suit. In 2013, revenues from online advertisement amounted to USD 117 billion and are expected to increase to over USD 190 billion by 2018, closing the gap with total TV advertisement revenues. Search accounts for the largest proportion of online advertising (USD 48 billion in 2013), followed by video and mobile advertising, which are expected to see the strongest growth up to 2018, with compound annual growth rates of 23.8% and 21.5% respectively (PwC, 2014b). Google currently dominates the market for online advertising, while Facebook and Google command the mobile segment (Figure 3.20).

The rise of mHealth

The convergence between wireless communication technologies and healthcare devices has started to reshape the health sector. The new opportunities for healthcare delivery brought forward by ICTs and the continued trend of ageing populations are opening new markets with large growth potential. Developments in ICTs are not only changing the way healthcare is delivered, but also offer patients a more active role in the prevention and monitoring of diseases.

Smartphones, in particular, offer the potential to broadly and cheaply diffuse more intensive self-monitoring, feedback, self-management and clinical support than has been possible previously. Such devices support a diverse set of data streams and monitoring activities, including automated tracking of body movement, location and other data that

can infer physical activities, sleep and environment; automated and manually entered physiological measures (e.g. readings from a glucose meter); and prompted and user-initiated self-reports of the user's symptoms or behaviours.

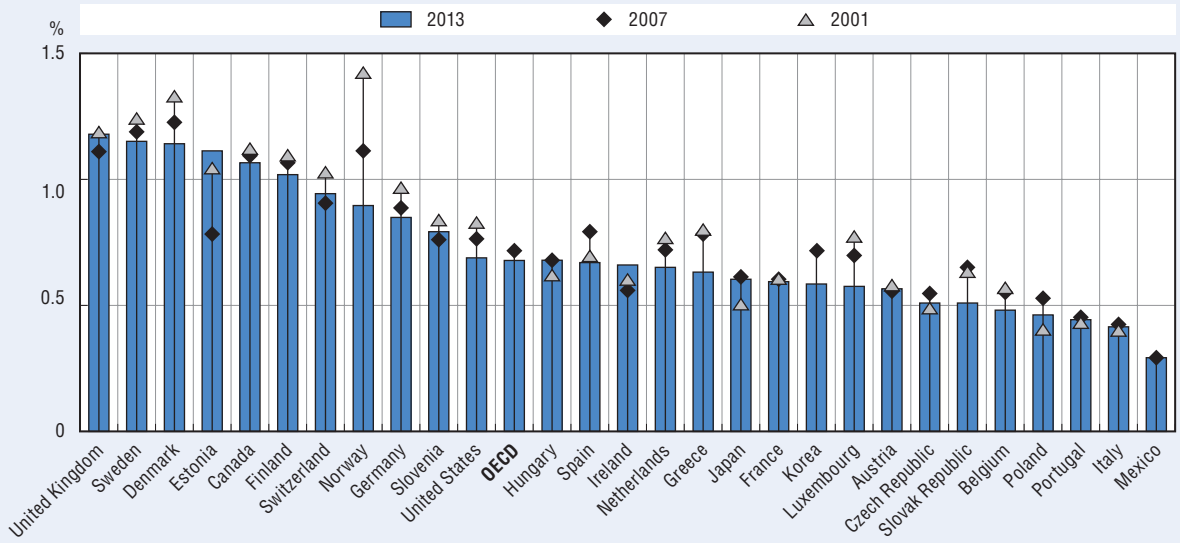
This information, properly managed, can be leveraged to trigger highly personalised interventions, and thus significantly improve an individual's ability to understand and manage his or her own behaviours. Moreover, such data (e.g. of measurements, medical images, symptom descriptions) can be stored in large databases with the potential to boost healthcare research and innovation.

Box 3.4. **Content and media sector: An overview**

Media and content industries are engaged in the production, publishing and/or electronic distribution of content products (OECD, 2011). In 2013, the sector employed almost 3.5 million people, accounting for 0.7% of total employment in 29 OECD countries for which data are available. The United Kingdom and Sweden have the largest shares, followed by Denmark, Estonia, Canada and Finland (all over 1% of total employment). In 2001-13, employment shares in this sector fell in most countries, particularly in Norway (-0.5 percentage points), but also in Denmark, Greece, Luxembourg and the United States (-0.2). Japan and Hungary are among the few exceptions to this trend, where the employment share of the media and content sector increased since 2001.

Evolution of the employment in the media and content sector, 2001, 2007 and 2013

As a percentage of total employment



Notes: Data for France, Germany, Ireland, Japan and Switzerland refer to 2012. Data for Mexico, Portugal and Sweden refer to 2011. Data for Switzerland refer to 2008, instead of 2007. The media and content sector is defined here as the sum of industries 58-60 Publishing, motion picture, video, television programme production; sound recording, programming and broadcasting activities excluding 582 Software publishing. Exceptions are Canada, Ireland, Japan, Mexico, the Netherlands, Portugal, Switzerland and Sweden, where industry 582 was not excluded.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4; Eurostat, National Accounts Statistics and national sources, April 2015.

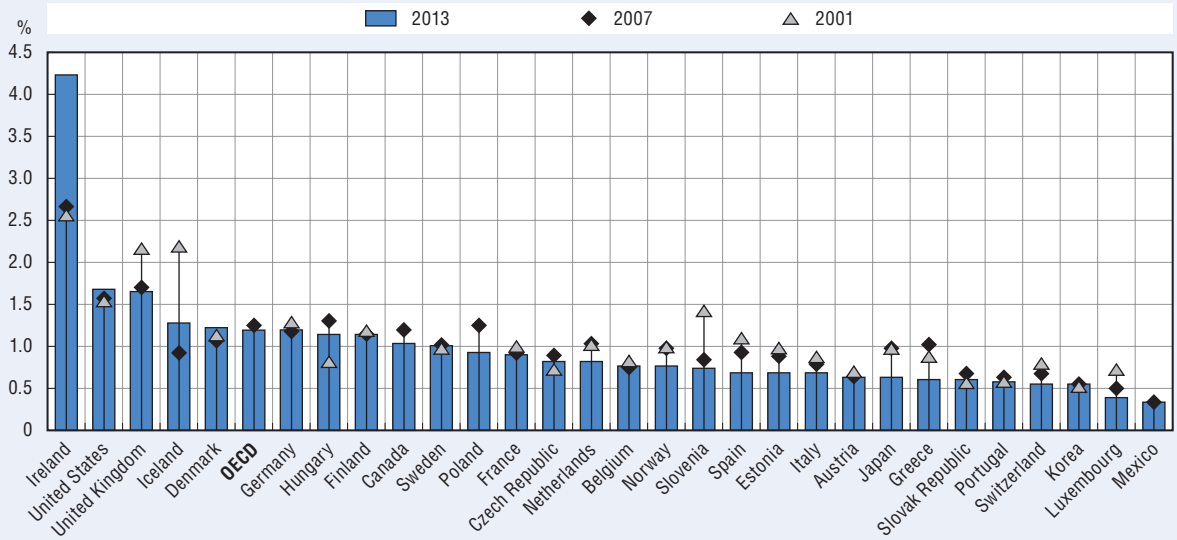
StatLink http://dx.doi.org/10.1787/888933225018

In 2013, the content and media sector accounted for 1.2% of total value added in the OECD area. The share of this sector was significantly higher in Ireland (4.2%), the United Kingdom and the United States (1.7%). As for employment, the shares in value added have fallen in most countries over 2001-13, the main exception being Ireland (+1.65 percentage points), Hungary (0.31), the Czech Republic (0.12) and the United States (0.09).

Box 3.4. **Content and media sector: An overview** *(cont.)*

Evolution of value added in the media and content sector, 2001, 2007 and 2013

As a percentage of total value added

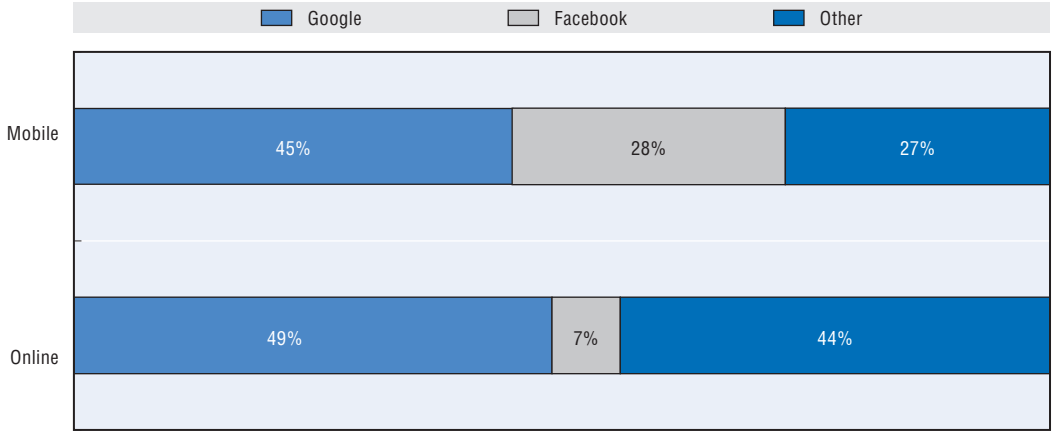


Notes: Data for Germany, Iceland, Ireland, Japan, Mexico, Poland, Sweden, Switzerland and the United Kingdom, refer to 2012. Data for Canada and Portugal, refer to 2011. Data for Switzerland refer to 2008, instead of 2007. The media and content sector is defined here as the sum of industries 58-60 Publishing, motion picture, video, television programme production; sound recording, programming and broadcasting activities excluding 582 Software publishing. Exceptions are Canada, Iceland, Ireland, Japan, Mexico and Switzerland, where industry 582 was not excluded.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4; Eurostat, National Accounts Statistics and national sources, April 2015.

StatLink http://dx.doi.org/10.1787/888933225029

Figure 3.20. **Major players in online and mobile advertisement**



Source: IDATE, 2014.

StatLink http://dx.doi.org/10.1787/888933225034

The market for mobile health and wellness apps (*mHealth*) has developed rapidly in recent years. The number of mHealth apps published on the two leading platforms, iOS and Android, has more than doubled in only 2.5 years to reach more than 100 000 apps (Q1 2014). In 2012, 69% of US smartphone owners reported tracking at least one health indicator such as weight, diet, exercise or symptoms using a mHealth app (Fox and Duggan, 2013).

According to some estimates, the global mHealth market may reach USD 23 billion in 2017, with Europe accounting for USD 6.9 billion and Asia-Pacific for USD 6.8 billion, ahead of the North American market of USD 6.5 billion. Remote monitoring treatment solutions would constitute almost 60% of total mHealth deployments in Europe. Solutions that increase the efficiency of the healthcare workforce and systems make up nearly 15% of overall deployments, alongside health and wellbeing apps.

By 2017, mHealth could potentially save a total of EUR 99 billion in healthcare costs in the European Union. The largest savings would be in the areas of wellness/prevention (EUR 69 billion) and treatment/monitoring (EUR 32 billion), while increasing the wage bill for workers in mHealth by EUR 6.2 billion (GSMA, 2013).

Increasing use of ICTs in healthcare has led to rapid growth in the amount of digitised data available. Over the past decade, in particular, there has been a rising interest in electronic health records (EHRs) in OECD countries.

While all countries are investing in data infrastructure, a 2013 OECD survey found that most countries had a national plan or policy to implement EHRs (22 of 25 countries) in 2011-12, and the majority had already begun to implement that plan (20 countries). EHR systems in some countries include data on key patient characteristics and health problems, as well as patient histories of encounters with the healthcare system and treatments received from a variety of healthcare providers. The greatest contribution of these systems as they develop is the potential for secondary analysis of data to monitor and conduct research, with a view to improving the health of the population and the quality, safety and efficiency of healthcare.

Of the 25 countries studied, 18 had included some form of secondary analysis of EHRs within their national plan (Figure 3.21). The most commonly included secondary uses reported were public health and health system performance monitoring. Fourteen countries also indicated that they intended for physicians to be able to query data to support treatment decisions. The least commonly reported planned data use (ten countries) was for facilitating or contributing to clinical trials.

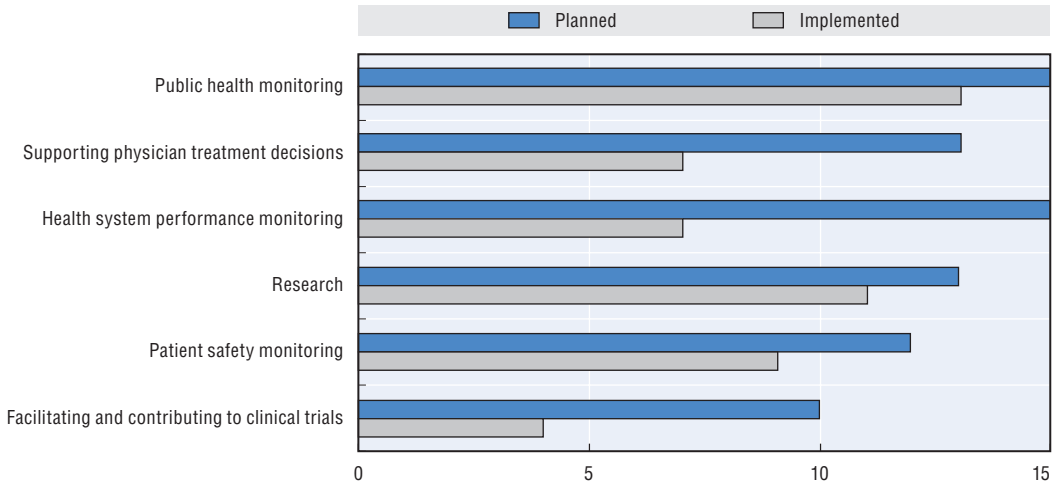
Collective consumption

Over the past few years, several innovative business models have emerged under the heading of the "sharing economy". These models enable collective consumption of private durable goods by providing access to excess capacity of these goods. Several factors seem to have created the conditions for the emergence of these business models:

- increasingly ubiquitous mobile Internet penetration and growing smartphone adoption and use
- social networks that normalised the sharing of information while online and mobile, and which gave individuals an online identity that facilitates trust among Internet users
- real-time and geo-locational data that enables direct matching of demand and supply for rides, cars or bikes
- online ratings and peer-reviews as a key tool for quality control of sellers and buyers by mutual evaluation
- constrained economic conditions since the 2008 financial crisis, which may have encouraged owners to welcome additional opportunities to monetise assets, and consumers to welcome cheaper offers (the largest home-sharing platform, Airbnb, launched in 2008, and the largest ride-sharing application, Uber, launched one year later).

Figure 3.21. **Planned and implemented uses of data from electronic health record systems**

Number of countries



Note: Twenty-five countries responded to the survey.

Source: OECD Health Care Quality Indicators Country Survey, 2012.

StatLink http://dx.doi.org/10.1787/888933225043

Prominent "sharing economy" businesses are platforms that offer short-term space rentals, mostly homes. Although home exchanges or short-term rentals are not new, the speed and scale at which platforms such as Airbnb have made commercial home sharing a common practice is unprecedented. While the growth of some home-sharing platforms has been spectacular in recent years, their overall economic impacts are not yet fully understood (Box 3.5).

Sharing economy business models have also emerged rapidly in the urban mobility market. Based on real-time geo-locational and (in most cases) mobile applications, shared mobility options range from the rental of private cars (Zipcar), rides (Uber, Lyft, blablacar) and parking spaces (justpark) to the rental of free floating (Car2go, DriveNow) and station-based cars (Autolib') and bikes (Velib'). These services are enjoying strong success among users, although their impact on urban mobility remains to be assessed (Box 3.6).

Many sharing economy business models currently rely on self-regulation, notably via ratings and reviews. Reputation is a key guide for both consumers and suppliers in the sharing economy. While ratings and reviews provide incentives for both sides to deliver on their promises, they suffer from several shortcomings (e.g. low response rates, incomplete information, etc.).

While the sharing economy brings to consumers the potential for a high variety of services and lower prices, its business model is not always consistent with existing regulations and laws, established at a time when the underlying technology was unavailable. This situation has raised strong reactions from incumbent business associations, who regard it as unfair competition; trade unions, who are concerned by the undefined status of the people working in these new businesses; and policy makers, who want to ensure the protection of consumers and workers, to the point that these activities have been forbidden in some countries or cities. The challenge for regulations and laws is to ensure effective protection of consumers and workers in this new economic environment, while fostering the potential benefits from the sharing economy.

Box 3.5. **Potential economic effects of home sharing**

There is no comprehensive assessment yet of the economic effects of home sharing. However, anecdotal evidence provides some insights. For example, in the case of New York, Airbnb claims that its guests are likely to generate more income for the city than hotel guests, and that Airbnb guests tend to spend their money in areas that have traditionally not profited overmuch from hotel guests and tourism.

The Airbnb study claims that in 2013, 416 000 visitors booked accommodation through Airbnb in New York, generating economic activity worth USD 632 million. An Airbnb guest stayed 6.4 nights on average (compared to 3.9 for hotel guests) and spent USD 880 at NYC businesses (compared to USD 690 for average New York visitors). Most Airbnb listings in New York (82%) are situated outside of the main tourist area of midtown Manhattan, compared to 30% of hotels; and 57% of Airbnb visitor spending occurs in the neighbourhood where they stay.

While these figures give an indication of the behaviour of Airbnb users, they do not provide a complete picture of the economic effects of Airbnb and other home-sharing services on a city. For example, the study does not consider how home sharing affects the market share of hotels and the potentially negative effects this could have on the local tax base and employment (Zervas et al., 2015). It also fails to consider local spending by hotel employees versus spending by Airbnb apartment owners, who are likely to be absent from the city while renting their property.

A more comprehensive assessment of the economic effects of home sharing and other sharing economy businesses is needed to better understand the overall economic implications of such services at local and national levels.

Sources: Airbnb, 2014; Zervas et al., 2015.

Collaborative production

While the sharing economy concerns "collective consumption", crowdsourcing and crowdfunding provide two interesting examples of "collaborative production".

Crowdsourcing can be applied to a large range of activities, tasks or challenges, the most common of which include idea creation, product design, problem solving, product development, marketing and advertising (Simula and Ahola, 2014). Large firms and organisations such as IBM, General Electric, NASA, DARPA or USAID tend to organise crowdsourcing within their internal networks. Smaller firms that have neither the scale nor the resources to undertake internal crowdsourcing tend to address communities external to the firm, mostly via a crowdsourcing platform. These platforms invite specific communities of interest or expertise to fulfil a well-defined task for the firm or to propose a solution to some challenge the firm is facing. Typically, crowdsourcing is organised as a contest in which a prize rewards the winning idea, solution or design. Contests seem to work well in many cases; however, instead of providing incentives for collaboration, they tend to put individuals in competition (Majchrzak and Malhotra, 2013). Platforms that enable online collaboration, such as Wikipedia, or co-creation, such as Quirky, are still rare.

Crowdsourcing for product development is not a widely spread practice, but some firms are using it intensively and with success. The most common practice is to involve customers via social media and through feedback. In the EU (28) countries, 25% of

enterprises use social media with their customers and almost 10% involve customers in the development or innovation of goods and services (Figure 3.22). A good example for such a practice is the Chinese smartphone producer Xiaomi, which releases a new version of its MIUI software each week, based on customer feedback. Customers make suggestions and vote on modifications via Weibo, the Chinese equivalent to Twitter (*Economist*, 2013).

Box 3.6. **Potential effects of shared mobility in urban transport**

Cars are an abundant asset and among the most expensive items in household budgets. In cities, vehicles are parked for 95% of the time, and a US household spends on average USD 8 776 per year on its car including gas, insurance, depreciation, vehicle payments and other expenses (ITF, 2012; *Time*, 2012).

Sharing cars, rides and bikes increases transport options in cities, reduces resource consumption and has the potential to change the overall face of urban mobility. Ratti and Claudel (2014) find that on-road mobility demand in Singapore could be met with 30% of the vehicles currently in use in the city. A calculation by the International Transport Forum (ITF) estimates that car sharing could reduce the fleet size in cities by half and presents a scenario that combines high-capacity public transport with self-driving "TaxiBots" (self-driving shared vehicles) in which only 10% of cars would be needed (ITF, 2014).

These optimistic scenarios are not likely to be realised in the near future. In the first place, shared mobility services could actually increase the number of cars in cities, as early evaluations of car sharing systems have found. A main reason for this is that car-sharing users do not necessarily give up their private car and many users that sign up for car-sharing offers do not own a car (*Le Monde*, 2013).

Given that these sharing systems are still in the early stages, more time, experience and evidence is needed to judge their overall effect on urban mobility. However, their success and economic potential indicate that their impacts will need to be considered. Free-floating car-sharing systems are projected to generate annual revenues of EUR 1.4 billion in OECD cities above 500 000 inhabitants by 2020 (Civity, 2014).

Sources: Civity, 2014; ITF, 2012, 2014; *Le Monde*, 2013; Ratti and Claudel, 2014; Time, 2012.

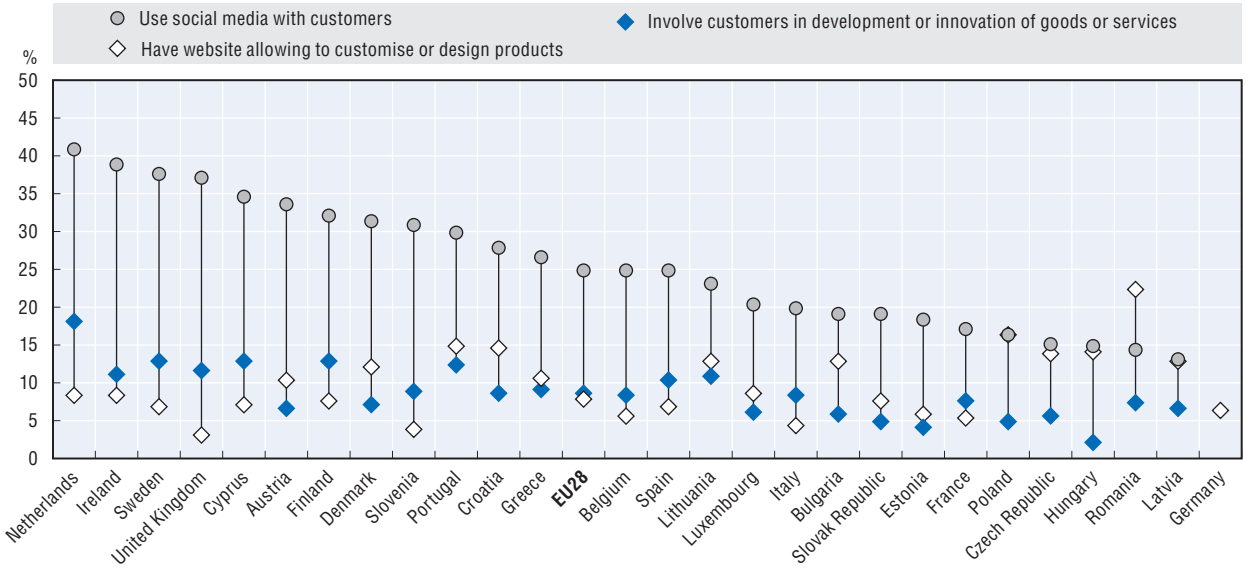
Other companies such as Tesla or Adidas allow customers to individualise their products online. Quirky, a start-up company, goes one step further: it offers a platform on which everyone can provide product ideas and designs, lets the community vote on which product to produce, and allows designers to influence the final development process. Ideas, designs and influence are in turn remunerated with royalties on each product sold by Quirky. Since 2009, Quirky has developed 417 products with its community, which currently includes over 1 million inventors (Quirky, 2015).

While there is virtually no regulation of crowdsourcing in OECD countries, a number of important issues may need to be addressed:

- There is a need for rules for employing and remunerating people online, potentially from abroad, on short-term contracts. Contests are unlikely to be an equitable model and might not be the most effective.

- There is a risk of potential abuse of extrinsic (e.g. monetary, increasing knowledge and skill-level, reputation building) or intrinsic (e.g. community sentiments, enjoyment, intellectual stimulation) motives of crowd members (Simula and Ahola, 2014).
- Not all intellectual property systems currently handle collaborative invention efforts well. This is an issue for both patents and copyrights.

Figure 3.22. **Enterprises engaging with customers in product development, 2013**



Note: Unless otherwise stated, sector coverage consists of all activities in manufacturing and non-financial market services. Only enterprises with ten or more persons employed are considered.

Source: Eurostat, Information Society Statistics, January 2015.

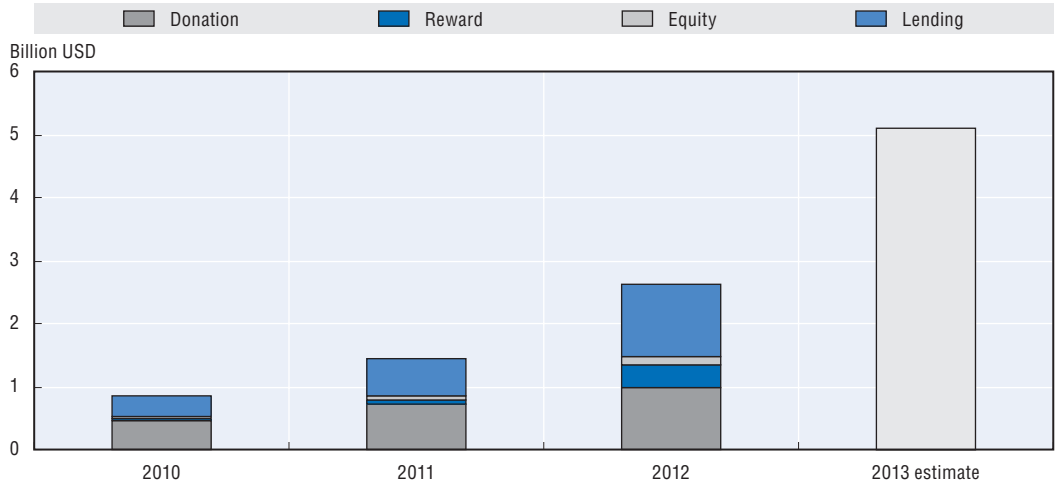
StatLink http://dx.doi.org/10.1787/888933225054

The term *crowdfunding* is used for different types of platforms. It may refer to: (i) lending (P2P); (ii) donations or reward-based funding; or (iii) equity crowdfunding (investment). Crowdfunding platforms first appeared within creative industries (e.g. music, film, games, performing arts, fashion and design), but have since diversified into a wide variety of activities.

The crowdfunding market has grown strongly over the past years, driven mainly by non-equity crowdfunding (Figure 3.23). Crowdfunding is most developed in the United States and Europe, which accounted for 60% and 35%, respectively, of the market in 2012 (Massolution, 2013).

Non-equity crowdfunding (donation and reward-based) platforms create opportunities for innovators while creating little risks for backers, which have no financial interests attached to their contribution, but rather care for the (future) product or "community benefits" (Belleflamme and Lambert, 2014). Opportunities created by equity crowdfunding platforms for both entrepreneurs and investors should be examined together with risks, notably for investors (Agrawal, Catalini and Goldfarb, 2013). Given the potential to provide additional sources for early stage funding of start-ups, a clear regulatory framework is necessary to minimise such risks and foster the potential of crowdfunding (Wilson and Testoni, 2014).

Figure 3.23. **Global crowdfunding volumes**



Source: Massolution (2013).

StatLink http://dx.doi.org/10.1787/888933225069

Few countries have addressed these challenges so far. In particular, in Europe, the second largest crowdfunding market, a variety of national regulations remain to be addressed (see the Annex). The United States has adopted a comprehensive legal framework for crowdfunding, the Jumpstart Our Business Startups (JOBS) Act, which is currently being implemented.

3.3 Measuring the impact of the digital economy: Growth, productivity and jobs

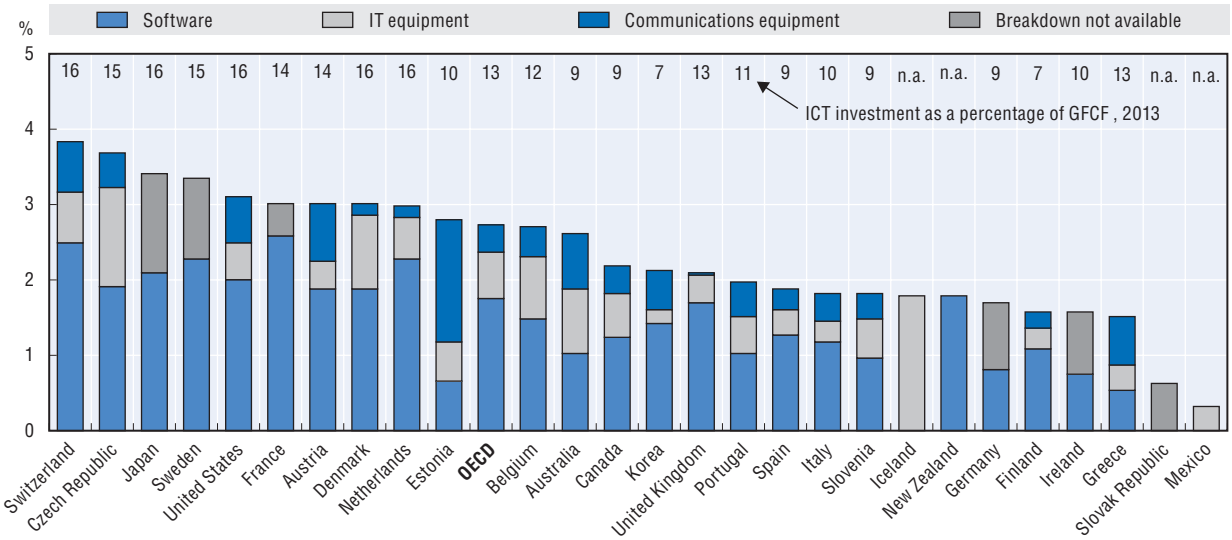
Investment in ICT goods and services is an important driver of growth. In 2013, ICT investment in the OECD area represented 13.5% of total fixed investment[8] and 2.7% of GDP. Over two thirds of ICT investment is devoted to computer software and databases. ICT investment across OECD countries varied from just below 4% of GDP in Switzerland and the Czech Republic to less than 2% in Greece and Ireland. These differences tend to reflect differences in the specialisation of each country and its position in the business cycle (Figure 3.24).

Over 2001-13, ICT investment dropped from 3.4% to 2.7% of GDP, and from 14.8% to 13.5% of total fixed investment (Figure 3.25). This decrease was the result of two opposite changes: a decrease in IT and communication equipment and an increase in software. The latter increased to 69% of total ICT investment in 2013, from 51% in 2000. The decrease in total ICT investment relative to GDP was particularly large in Korea (-1.4 percentage points), Slovenia and Sweden (-1.2).

The generalised slowdown in ICT investment is due partly to a rapid decrease in prices, particularly for IT and communication equipment, and partly to the fact that an increasing proportion of business ICT expenditures might not be capitalised. Indeed, detailed information available for the United States reveals that about one third of total business expenditure in ICTs is non-capitalised and that the ICT sector itself is responsible for 40% of capitalised expenditure (OECD, 2014c).

Figure 3.24. **ICT investment by capital asset, 2013**

As a percentage of GDP and Gross Fixed Capital Formation



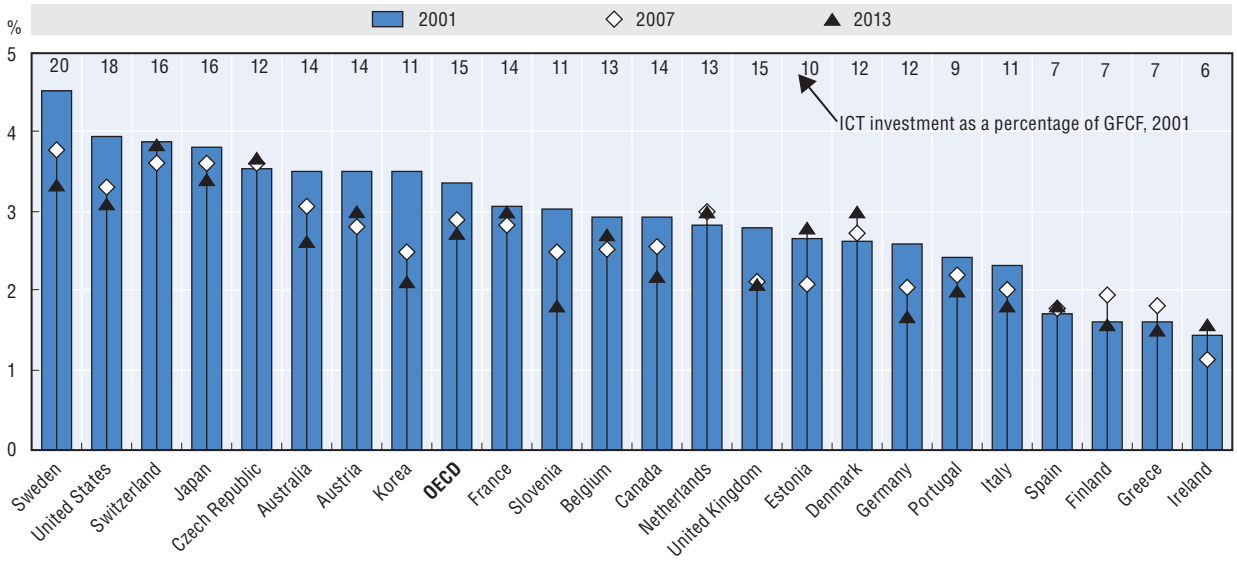
Notes: Data for Australia, Spain and Sweden are 2012 instead of 2013, and data for Portugal are 2011. Data for Iceland, Mexico, New Zealand and the Slovak Republic were incomplete and only represent the asset for which data were available. The series "breakdown not available" represents in all cases the combination of IT and communication equipment.

Source: OECD, Annual National Accounts (SNA) Database; Eurostat, National Accounts Statistics and national sources, February 2015.

StatLink *http://dx.doi.org/10.1787/888933225071*

Figure 3.25. **The dynamics of ICT investment, 2001, 2007 and 2013**

As a percentage of GDP and Gross Fixed Capital Formation



Note: Data for Australia, Spain and Sweden are 2012 instead of 2013, and data for Portugal are 2011.

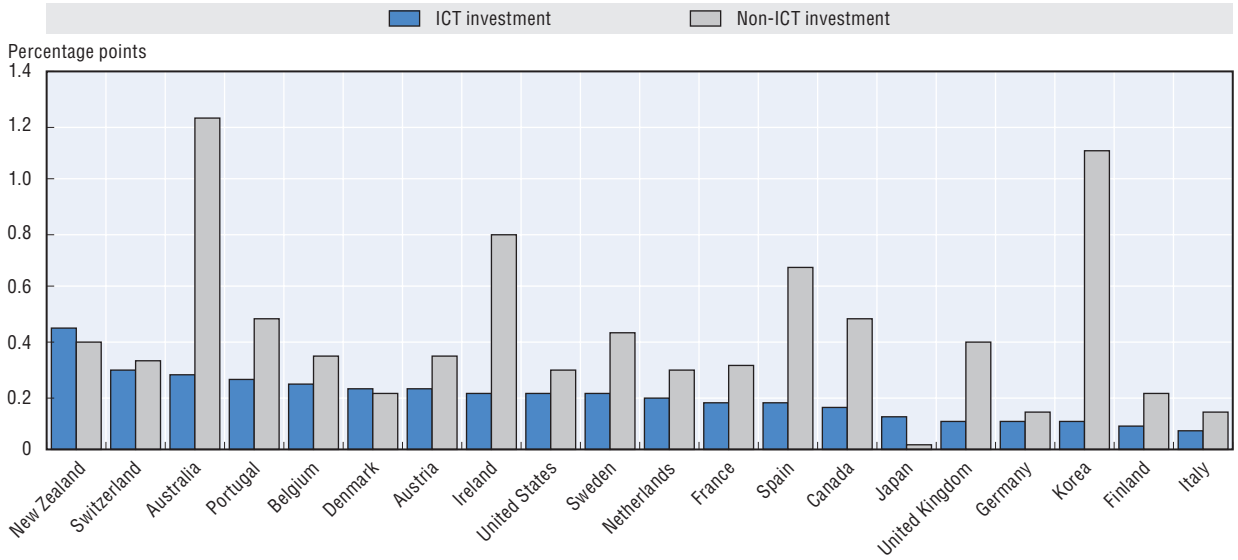
Source: OECD, Annual National Accounts (SNA) Database; Eurostat, National Accounts Statistics and national sources, February 2015.

StatLink *http://dx.doi.org/10.1787/888933225087*

Between 2001 and 2013, ICT investment contributed between 0.15 and 0.52 percentage points to annual growth in GDP. However, the contribution of ICT investment to growth has slowed since the onset of the financial crisis in 2007. ICT investment accounted for between 0.07 and 0.45 percentage points of annual growth in GDP (Figure 3.26), compared to 0.22-0.59 for the 2001-07 period (Figure 3.27).[9]

Figure 3.26. **Contribution of ICT and non-ICT investments to GDP growth, 2008-13**

Percentage points, annual average



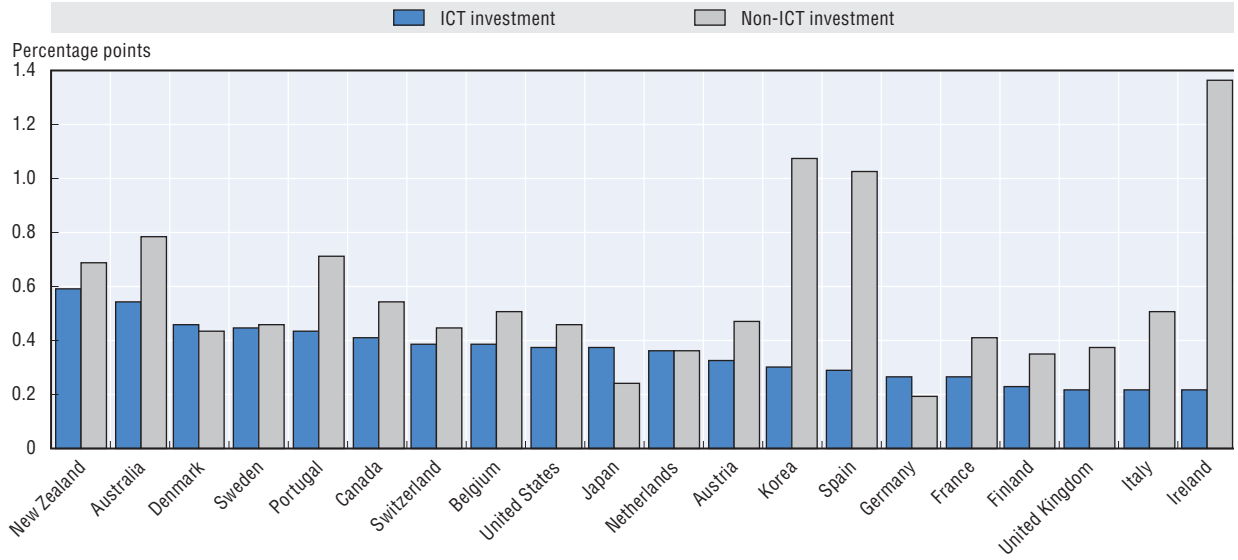
Note: Data for Australia and Japan correspond to the period 2008-12. For Portugal, the period corresponds to 2008-11.

Source: OECD, Productivity Database, February 2015.

StatLink http://dx.doi.org/10.1787/888933225096

Figure 3.27. **Contribution of ICT and non-ICT investments to GDP growth, 2001-07**

Percentage points, annual average



Source: OECD, Productivity Database, February 2015.

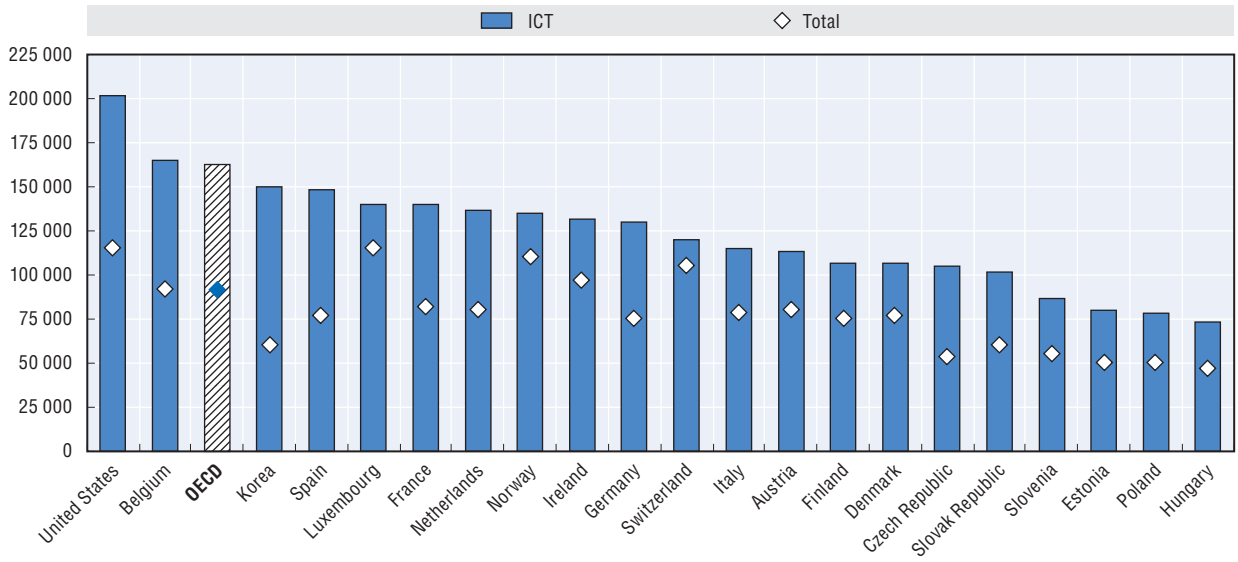
StatLink http://dx.doi.org/10.1787/888933225109

In 2013, OECD labour productivity (i.e. value added per person employed) in the ICT sector was USD 162 000 PPP (i.e. 79% higher than the rest of the economy). The labour productivity edge was particularly large in Telecommunication services (160% higher than the total economy) and in Computer manufacturing (138%), while it was smaller, but still considerable, in Software publishing (103%) and IT services (21%).

These data show large variation across countries. Labour productivity in the ICT industries relative to the total economy, range from over USD 200 000 PPP in the United States, to over USD 74 000 PPP in Hungary (Figure 3.28).

Figure 3.28. **Labour productivity of the ICT sector and total economy, 2013**

USD current PPP per person employed



Note: Data for France, Germany, Ireland, Poland, Spain and Switzerland refer to 2012.

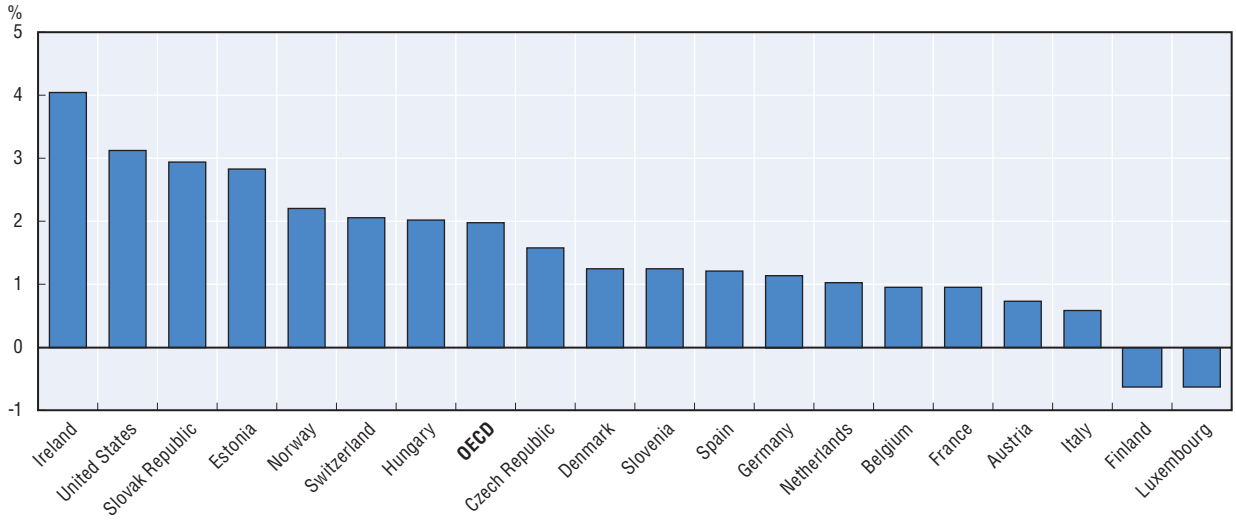
Sources: Based on OECD, National Accounts Database, ISIC Rev.4, and national sources, May 2015.

StatLink http://dx.doi.org/10.1787/888933225113

Over the period 2001-13, ICT industries made a significant contribution to total labour productivity growth in a majority of OECD countries (Figure 3.29). The ICT sector raised total labour productivity by 4% in Ireland, about 3% in Estonia, the Slovak Republic and the United States, over 2% in Hungary, Norway and Switzerland. The slowdown in productivity growth in the ICT sector seems also to have resulted into a large decrease in total labour productivity in Finland and Luxembourg (-0.6%).

The contribution of the ICT sector to total employment growth over the last decade has been uneven (Figure 3.30). About 23% of the drop in total employment in 2001 and 46% in 2002 – the years of the dot-com bubble – was due to employment losses in the information and communication industries. Their contribution was positive but limited (5% a year on average) in 2005-08. In the aftermath of the recent crisis (2009-10), the contribution of information and communication became negative again, accounting for 6% per year of the decrease in total employment. However, the ICT sector accounted for 4% of total employment growth in 2011 and 2012 and for 22% in 2013. These latest figures suggest that ICTs are playing a significant role in the upcoming recovery.

Figure 3.29. **Growth in total labour productivity growth accounted for by the ICT sector, 2001-13**

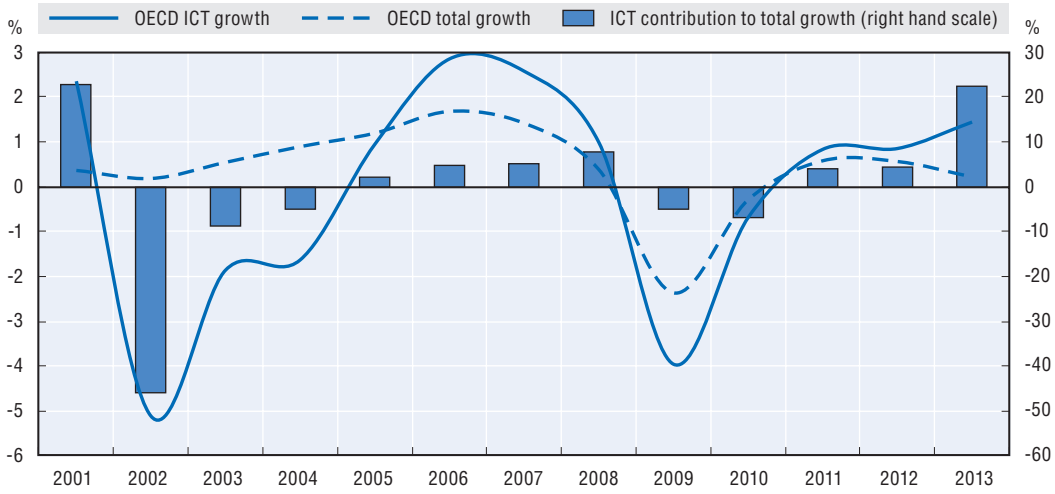


Notes: Data for France, Germany, Ireland and Spain correspond to the period 2001-12. For the Netherlands, the period corresponds to 2002-13. For Switzerland, the period corresponds to 2002-12.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4, and national sources, May 2015.

StatLink *http://dx.doi.org/10.1787/888933225121*

Figure 3.30. **Contribution of the ICT sector to total employment growth in the OECD, 2001-13**



Notes: The aggregate for the OECD area includes 27 OECD countries for which data series were fully available. Data for 2013 are estimates.

Sources: Based on OECD, National Accounts Database, ISIC Rev.4 and national sources, March 2015.

StatLink *http://dx.doi.org/10.1787/888933225139*

Box 3.7. **Stimulating demand for ICT development in Colombia**

The Republic of Colombia has experienced a trend towards higher living standards and political development in recent years (OECD, 2015b), and has adopted new strategies with the aim of making Colombia an attractive country for investments. Despite these accomplishments, however, over 29% of people are still living in poverty. ICTs are regarded as an essential tool not only to raise Colombia's competitiveness in the global environment, but also to improve the quality of life and upgrade the skills of its citizens.

In many countries, ICT policies have focused mainly on the supply side. While good ICT infrastructure and services are a prerequisite to fostering ICT use, Colombia has adopted a holistic approach to fostering the entire digital ecosystem. Through its ICT policy programme "Plan Vive Digital" (2010–2014), the government has developed the country's digital ecosystem by working simultaneously in four areas: infrastructure and services (supply), and applications and users (demand). This plan is expected to significantly increase Internet adoption as a means to reduce poverty, create jobs, and improve competitiveness and productivity.

Colombia has deployed four new submarine cables across the Pacific and Atlantic Oceans, and has significantly improved its international connectivity capability, to meet the increasing demand of applications and services in the country. A national broadband strategy has been complemented by nationwide deployment of 4G, with a move from three operators (3G) in 2010, to six operators (3G and 4G) and four MVNOs (mobile virtual network operators).

Deployment of backbone infrastructure is not enough, however. A key component of the "Vive Digital" strategy is reaching users at the bottom of the income pyramid and in rural areas of Colombia. To connect rural and remote areas, Colombia has established Community Internet Centres to provide citizens with access to training, Internet connectivity, telephony, entertainment and other technological services. To date, 449 "Puntos Vive Digital" have been established in less favoured urban areas and 6 548 "Kioscos Vive Digital" have been set up in rural centres with more than 100 inhabitants.

Examples of a Punto Vive Digital (left) and a Kiosco Vive Digital (right)

Source: MinTIC, Colombian Ministry of ICT.

The digital strategy also subsidises Internet services for low-income populations, covered by contributions made by operators to the National Telecommunications Fund (FONTIC). Subsidies are granted to users through Internet service providers, which subsequently deduct the amount from the contribution made to FONTIC. Citizens can choose whether the subsidy covers part of the monthly value of the broadband plan or part of the value of a computer/terminal.

In terms of taxation policy, the VAT exemption on computers was extended to mobile devices with a price threshold below USD 900 for PCs and laptops and USD 470 for smart mobile devices. In addition, import tariffs on computers, tablets, smartphones and related parts were eliminated in 2011. As a result of these measures, growth rates in computer sales are among the highest in Latin America (+16% growth).

Box 3.7. **Stimulating demand for ICT development in Colombia** *(cont.)*

In addition, computers prices are among the lowest on the continent. In the third quarter of 2014, the government reached a penetration rate of 41.44 terminals (computers and tablets) per 100 inhabitants.

Several programmes of the "Vive Digital" strategy aim to increase ICT adoption by SMEs. These include Internet training courses, trade shows for SMEs and the IT industry, and promotion of e-commerce. Some programmes targeted to SMEs are run by large enterprises and co-financed by the government. The aim is to provide SMEs with training and incentives to use ICTs to improve the efficiency of the entire value chain of which they are a part.

To foster content creation, Viva Labs (digital content centres) have been installed to reinforce the digital content industry in areas such as video games, animation and audio-visual. Apps.co, the digital entrepreneurship programme, is training more than 70 000 entrepreneurs in issues such as business model development, start-up management and acquisition of ICT skills.

Through the "Computadores para Educar" (Computers for education) initiative, the Colombian Ministry of Information Technology and Communications (MINTIC) has delivered 2 million computers and tablets to public schools and libraries. The initiative also provides extensive training for teachers and children and raises awareness among parents.

The awareness raising programme "En TIC Confío" (In ICT I Trust) promotes responsible and secure use of the Internet, as well as avoidance of online risks for children, youth and adults.

During the last four years, Colombia has earned significant recognition for the ambitious "Vive Digital" strategy. In 2012, it received the GSMA Government Leadership Award for the establishment of sound telecommunications regulatory policies and practices.

Several important achievements can be reported. The "Vive Digital" plan has increased the number of broadband connections from 2.2 million in 2010 to 9.7 million in 2014. The number of municipalities connected to the Internet has risen from 17% in 2010 to 96% in 2014. The share of connected SMEs increased from 7% in 2010 to almost 61% in 2014. Finally, the proportion of households connected to the Internet rose from 17% in 2010 to 44% in 2014, and is expected to reach 50% by the end of 2015.

The next stage of the strategy, "Vive Digital 2014–2018", aims to strengthen the demand side of the digital ecosystem (i.e. applications and users). It has three main goals: (i) to become a world leader in the development of social applications for lower income families and populations in rural or remote areas; (ii) to increase government efficiency and transparency through ICTs; and (iii) to promote and develop digital talent.

Efforts in the area of connectivity, however, will continue into 2018. Colombia is aiming to reach 27 million broadband connections, and to increase household connectivity penetration from 50% in 2014 to 63% by 2018. Colombia also intends to increase Internet penetration among SMEs from 60% to 70% by 2018.

Colombia faces a major challenge, however: talent is necessary to foster a local innovation ecosystem. While the annual growth rate for system engineering graduates in China and Brazil is 26% and 10% respectively, Colombia has a negative growth rate of -5%. Another goal of the plan is therefore to increase the IT-related workforce.

MINTIC is working on a talent roadmap to promote IT careers among students and to implement substantial improvements in quality of education. Colombia has already organised several "hackathons", which gather a wide range of software and apps developers, user interface designers, data analysts and experts to collaborate on developing services, products or solutions to a given challenge. The hackathons have focused on developing social apps that will help to solve problems facing low-income populations and help to fight poverty.

Stimulating demand is not purely an ICT sectoral issue, since ICTs now penetrate almost every sector and transform economies into digital economies. A whole-of-government approach is essential to grasp the benefits of ICTs. In Colombia, the Ministries of Defence, Justice, Education, Health and Trade, Industry and Tourism have all been key allies in fostering demand in each of these sectors.

Sources: Alcaldía de Mutatá, 2014; MinTIC, 2013.

Notes

1. Small firms are defined as companies with between 10 and 49 employees.
2. Such as the case when customs administrations classify goods in disaccord with internationally accepted rules and principles of tariff classification.
3. For more information, see *http://press.spotify.com/fr/information/*.
4. See *www.flickr.com/photos/franckmichel/6855169886/*.
5. See *http://instagram.com/press/*.
6. For more information, see *www.youtube.com/yt/press/statistics.html*.
7. See OECD based on Instantwatcher (*http://instantwatcher.com/titles/all*).
8. Gross Fixed Capital Formation (GFKF).
9. The contribution of non-ICT investment has increased in general for all countries due to the implementation of the new system of National Accounts (SNA 2008), which has introduced some important changes including the capitalisation of expenditures in R&D and military equipment. It has been relatively higher in Australia, Canada, Ireland, Korea, Portugal and Spain.

References

Agrawal K., C. Catalini and A. Goldfarb (2013), "Some simple economics of crowdfunding", NBER working paper series, Cambridge, MA, *www.nber.org/papers/w19133* (accessed 14 October 2014).

Airbnb (2014), "The Airbnb community's economic effect on New York City", *Airbnb* blog, *http://blog.airbnb.com/wp-content/uploads/Airbnb-economic-impact-study-New-York-City.pdf*.

Alcaldía de Mutatá (2014), "Punto Vive Digital Municipio de Mutatá", Press release, 12 November 2014, Mutatá en Antioquia, *www.mutata-antioquia.gov.co/noticias.shtml?apc=ccx-1-&x=2785213* (accessed 15 April 2015).

Androsoff, R. and A. Mickoleit (2015), "Measuring government impact in a social media world", *OECD Insights* blog, 18 February 2015, *http://oecdinsights.org/2015/02/18/measuring-government-impact-in-a-social-media-world* (accessed 15 April 2015).

Apple (2013), "iTunes store sets new record with 25 billion songs sold", *Apple Press Info*, 6 February 2013, Cupertino, *www.apple.com/pr/library/2013/02/06iTunes-Store-Sets-New-Record-with-25-Billion-Songs-Sold.html* (accessed 15 April 2015).

Bakhshi, H., A. Freeman and P. Higgs (2013), *A dynamic mapping of the UK's creative industries*, NESTA, *www.nesta.org.uk/sites/default/files/a_dynamic_mapping_of_the_creative_industries.pdf*.

Belleflamme, P. and T. Lambert (2014), "Crowdfunding: some empirical findings and microeconomic underpinnings", prepared for a special issue of the *Revue Bancaire et Financière*, July 2014.

Cinelli, S. (2014), "Lending Club's IPO and the next phase of Crowdfunding", crowdfundingbeat, *http://crowdfundbeat.com/lending-clubs-ipo-and-the-next-phase-of-crowdfunding/* (accessed 22 October 2014).

Civity (2014), "Urban mobility in transition?", *matters no. 1*, Civity Management Consultants, Berlin.

ECN (2013), *Review of Crowdfunding Regulation*, European Crowdfunding Network, Brussels, *www.europecrowdfunding.org/wp-content/blogs.dir/12/files/2013/12/ECN-Review-of-Crowdfunding-Regulation-2013.pdf*.

Economist (2014), "Banking without banks", *The Economist*, 1 March 2014, *www.economist.com/news/finance-and-economics/21597932-offering-both-borrowers-and-lenders-better-deal-websites-put-two* (accessed 22 October 2014).

Economist (2013), "Taking a bite out of Apple", *The Economist*, 12 September 2013, *www.economist.com/news/business/21586344-xiaomi-often-described-chinas-answer-apple-actually-quite-different-taking-bite-out* (accessed 14 October 2014).

Eurostat (2013), Information Society Databases, Eurostat website, *http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/comprehensive_databases* (accessed 4 November 2014).

FCA (2014), "The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media", *Feedback to CP13/13 and final rules*, Financial Conduct Authority, London, *www.fca.org.uk/static/documents/policy-statements/ps14-04.pdf*.

Flurry (2014), "Mobile to television", *Flurry Insights*, *www.flurry.com/blog/flurry-insights/mobile-television-we-interrupt-broadcast-again#.VG-PgPnF9HX* (accessed 21 November 2014).

Fox, S. and Duggan, M. (2013), "Tracking for health", *Pew Research Center*, 28 January 2013, Pew Research Center, Washington DC, *www.pewinternet.org/2013/01/28/tracking-for-health/*.

GSMA (2013), *Socio-economic Impact of mHealth: An Assessment Report for the European Union*, London, Groupe Speciale Mobile Association and PricewaterhouseCoopers, *www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic_impact-of-mHealth_EU_14062013V2.pdf*.

GSMA and PwC (2012), *Touching Lives through Mobile Health: Assessment of the Global Market Opportunity*, London, Groupe Speciale Mobile Association and PricewaterhouseCoopers, *www.gsma.com/connectedliving/gsma-pwc-report-touching-lives-through-mobile-health-assessment-of-the-global-market-opportunity/* (accessed 21 November 2014).

IDATE (2014), *Digiworld Yearbook 2014*, IDATE, Montpellier, France.

ITF (2014), *Urban Mobility: System Upgrade*, International Transport Forum and Corporate Partnership Board, Paris, *http://internationaltransportforum.org/cpb/pdf/urban-mobility.pdf*.

ITF (2012), "Smart Grids and Electric Vehicles: Made for Each Other?", *Discussion Paper 2012* No. 2, International Transport Forum, Paris.

Le Monde (2013), "On a raté l'objectif. Autolib' ne supprime pas de voitures", *Le Monde Blogs*, 26 March 2013, *http://transports.blog.lemonde.fr/2013/03/26/on-a-rate-lobjectif-autolib-ne-supprime-pas-de-voitures/* (accessed 19 September 2014).

Lending Club (2014), "Lending Club – what we do", Lending Club, San Francisco, CA, *www.lendingclub.com/public/about-us.action* (accessed 22 October 2014).

Mach, T.L, C.M. Carter and C.R. Slattery (2014), "Peer-to-peer lending to small businesses", *Finance and Economics Discussion Series*, Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board, Washington DC, *www.federalreserve.gov/pubs/feds/2014/201410/201410pap.pdf*.

Majchrzak, A. and A. Malhotra (2013), "Towards an information systems perspective and research agenda on crowdsourcing for innovation", *Journal of Strategic Information Systems*, No. 22, pp. 257-268, *http://dx.doi.org/10.1016/j.jsis.2013.07.004*.

Massolution (2013), *2013CF: The Crowdfunding Industry Report*, Massolution, Los Angeles, CA, *www.crowdsourcing.org/editorial/2013cf-the-crowdfunding-industry-report/25107* (accessed 14 April 2015).

MinTIC (2013), "Más de 2.800 nuevas localidades de zonas rurales o apartadas tendrán Kioscos Vive Digital" (More than 2,800 new locations in rural and remote areas will have Vive Digital Kiosks), *MinTIC* website, 18 September 2013, Ministry of Information Technologies and Communications, Bogota, *www.mintic.gov.co/portal/604/w3-article-4372.html* (accessed 14 October 2014).

OECD (2015a), *Data-driven Innovation for Growth and Well-being*, OECD Publishing, Paris (forthcoming).

OECD (2015b), *OECD Economic Surveys: Colombia 2015*, OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/eco_surveys-col-2015-en*.

OECD (2014a), "Cloud computing: The concept, impacts and the role of government policy", *OECD Digital Economy Papers*, No. 240, OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/5jxzf4lcc7f5-en*.

OECD (2014b), "Government use of social media. A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Maker", *OECD Public Governance Working Papers No. 26*, OECD, Paris, *http://dx.doi.org/10.1787/5jxrcmghmk0s-en*.

OECD (2014c), *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, DOI: 10.1787/9789264221796-en.

OECD (2014d), *Recommendation of the Council on Digital Government Strategies*, OECD Publishing, Paris, *www.oecd.org/gov/public-innovation/recommendation-on-digital-government-strategies.htm* (accessed 14 April 2015).

OECD (2013a), "Open government data: Towards empirical analysis of open government data initiatives", *OECD Public Governance Working Papers*, No. 22, OECD, Paris, *http://dx.doi.org/10.1787/5k46bj4f03s7-en*.

OECD (2013b), *New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments*, Draft Report for the 44th Session of the Working Party for SMEs and Entrepreneurship, OECD, Paris.

OECD (2012), *OECD Internet Economy Outlook 2012*, OECD Publishing, Paris, *www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm*.

OECD (2011), *OECD Guide to Measuring the Information Society 2011*, OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/9789264113541-en*.

OECD (2009), *Top Barriers and Drivers to SME Internationalisation*, Report by the OECD Working Party on SMEs and Entrepreneurship, OECD, Paris, *www.oecd.org/cfe/smes/43357832.pdf*.

Our Mobile Planet (2013), *Our Mobile Planet – Full Data Sets and Country Reports*, *http://think.withgoogle.com/mobileplanet/en-gb/downloads/* (accessed 13 April 2015).

PwC (2014a), *Retail Banking 2020: Evolution or Revolution?* PricewaterhouseCoopers, London, *www.pwc.com/et_EE/EE/publications/assets/pub/pwc-retail-banking-2020-evolution-or-revolution.pdf*.

PwC (2014b), *Internet Advertising – Key Insights at a Glance*, PricewaterhouseCoopers, London, *www.pwc.com/gx/en/global-entertainment-media-outlook/segment-insights/internet-advertising.jhtml* (accessed 20 November 2014).

Quirky (2015), "About", Quirky website, *www.quirky.com/about* (accessed 17 April 2015).

Ratti, C. and M. Claudel (2014), *The Driverless City*, *www.project-syndicate.org/commentary/carlo-ratti-and-matthew-claudel-foresee-a-world-in-which-self-driving-cars-reconfigure-urban-life* (accessed 15 May 2014).

research2guidance (2014), *mHealth App Developer Economics 2014: The State of the Art of mHealth App Publishing*, research2guidance, Berlin, *http://research2guidance.com/r2g/research2guidance-mHealth-App-Developer-Economics-2014.pdf*.

Rochet J.-C. and J. Tirole (2006), "Two-sided markets: a progress report", *RAND Journal of Economics*, Vol. 37/3, pp. 645-667, *http://ideas.repec.org/a/bla/randje/v37y2006i3p645-667.html*.

Simula, H. and T. Ahola (2014), "A network perspective on idea and innovation crowdsourcing in industrial firms, *Industrial Marketing Management*, No. 43, pp. 400-408, *http://dx.doi.org/10.1016/j.indmarman.2013.12.008*.

TechCrunch (2014), "Travel, retail and media are 3 industries taking over the App Store", *TechCrunch*, 18 October 2014, *http://techcrunch.com/2014/10/18/travel-retail-and-media-are-3-industries-taking-over-the-app-store/* (accessed 22 October 2014).

Time (2012), "What's Car Sharing Really Like?", *Time Business*, April 2012, *http://business.time.com/2012/04/16/whats-car-sharing-really-like/* (accessed 19 September 2014).

Wagner, K. (2013), "Facebook has a quarter of a trillion user photos", *Mashable*, 17 September 2013, *http://mashable.com/2013/09/16/facebook-photo-uploads/* (accessed 15 April 2015).

WAN-IFRA (2014), "World press trends", Press release, World Association of Newspapers and News Publishers, Franffurt/Paris, *www.wan-ifra.org/press-releases/2014/06/09/world-press-trends-print-and-digital-together-increasing-newspaper-audienc* (accessed 21 November 2014).

Wilson, K. and M. Testoni (2014), "Improving the role of equity crowdfunding in Europe's capital markets", *Bruegel Policy Contribution Issue*, 2014/09.

Zervas et al. (2015), *The Rise of the Sharing Economy: Estimating the Impact of Airbnb on the Hotel Industry*, *http://people.bu.edu/zg/publications/airbnb.pdf*.

ANNEX

Crowdfunding regulation in OECD countries, 2013

Equity:		Equity and funding:	
Funding:		Equity and lending:	
Lending:		All types:	

Exemptions: * Equity ** Funding *** Lending **** All types

Country/ Regulation	General (financial)	Prospectus / threshold	Payment service	Consumer credit	Crowdfunding Act/ legislation
Austria		250k/issuer/y			
Belgium		100k/issuer/y			
Canada	*		****		
Czech Republic		1 mio/issuer/y			
Denmark	***	1 mio/issuer/y			
Estonia	***	5 mio/issuer/y			
Finland		1.5 mio/issuer/y	Unclear		
France		* 100k/issuer/y	**		Under consideration
Germany	*	* 100k/issuer/y			
Greece		100k/issuer/y		Lending only by banks	
Hungary	* ***	100k/issuer/y			
Ireland	*	unclear	Unclear		
Israel	Unclear		Unclear	Unclear	
Italy		5 mio/issuer/y			
Luxembourg	Unclear			Unclear	
Netherlands	Unclear	2.5 mio/issuer/y			
Portugal					
Slovak Republic		100k/issuer/y			
Slovenia		* 100k/issuer/y			
Spain		2 mio/issue/y			Under consideration
Sweden		2.5 mio/issuer/y	Unclear		
Switzerland	Unclear				
United Kingdom	*	5 mio/issuer/y	****		

Note: no information is available for Australia, Chile, Iceland, Japan, Korea, Mexico, New Zealand, Norway or Poland.

Source: ECN, 2013.

© OECD 2015

Chapter 4

Main trends in communication policy and regulation

The digital economy is based on efficient and reliable communication networks and services that need to be accessed ubiquitously, at competitive prices and at sufficient speeds. Communication policy and regulation are therefore increasingly important for achieving a vibrant digital economy. This chapter examines communication policy and regulatory developments in fixed and mobile networks, paying special attention to the emergence of over-the-top providers of traditional and new services. Policy responses to industry consolidation and the network neutrality debate take a prominent role, as does spectrum policy, international mobile roaming, public funding of communication networks and IPv6 initiatives. In particular, the chapter discusses convergence trends, the emergence of connected televisions and bundles of communication services to ascertain how they can best serve the interests of consumers.

Communication policy and regulation are crucial for the promotion of efficient and reliable communication networks and services, which will in turn realize the full potential of the digital economy. Fixed and mobile networks are increasingly converged, as are certain services that used to be provided by distinct networks. Television, video services, fixed and mobile telephony services are now increasingly provided through IP technology over the Internet. As a result, over-the-top providers are playing a more prominent role in the provision of communication services, which raises important questions in areas such as network neutrality and traffic prioritisation.

Increased consolidation in certain parts of the communications industry, such as mobile networks, has raised concerns over the level of effective competition. In some countries, authorities have acted to open opportunities for new entrants, such as through spectrum auctions, or by blocking mergers where there is limited opportunity for new entry. At the same time, convergence increasingly means that players with disruptive business models can enter the market from other parts of the communication ecosystem, as long as policy settings are pro-competitive.

In mobile markets, for the most part, consumers have benefitted from lower unit prices driven by reduced termination rates, enhanced technologies such as Long Term Evolution (LTE) (i.e. 4G) and more vibrant competition. For example, specific operators in some countries have started to include international mobile roaming services in baseline plans at no incremental cost. Moreover, handset manufacturers have introduced the first reprogrammable SIM cards that enable consumers to swap service providers in both domestic and some foreign markets.

Regulators and competition authorities in OECD countries have assessed the pros and cons of industry consolidation in mobile markets, especially with regard to merger cases and entry proceedings. Few feel that more consolidation would improve competition, but in some cases authorities have obtained commitments from merging parties aimed at facilitating the presence of mobile virtual network operators (MVNO) or a more equitable distribution of spectrum resources among operators. These initiatives aim to mitigate the loss of competition, but may not be as effective given possible uncertainties surrounding deals between mobile network operators (MNOs) and MVNOs (e.g. prices, roaming, 4G capabilities, long-term business plans).

Recent years have seen consolidation of MNOs in Australia, Austria, Germany and Ireland with consolidation forthcoming in the United Kingdom. However, market entry has occurred in Canada, France, Israel, Luxembourg and the Netherlands, and is planned in Hungary. In some cases, consolidation has been a reaction to financial demands on all infrastructure providers and the capital-intensive nature of the sector, which is responding to welcome increases in demand, even if these bring new challenges. Other players have made increasing use of network sharing. While network sharing has the potential to lower infrastructure competition, it may increase retail competition in otherwise underserved locations and regions. Countries introducing such policies include France, Israel and the

United Kingdom, while Japan has long used such tools to improve service in areas that might otherwise have poor coverage (e.g. tunnels, shopping malls).

It is beneficial to discuss demands for consolidation together with convergence. Fixed-mobile convergence, or the joint provision of fixed and mobile services, has become an important driving force in communications markets, as witnessed by recent high-profile mergers between cable operators and mobile providers. While consumers benefit from unified billing or seamless hand-offs between one network and another, fixed-only or mobile-only operators may be excluded from offering a full range of services.

Connected televisions or devices with screens for watching video content transmitted over the Internet (e.g. tablets, laptops, smartphones) are central to convergence between telecommunication and television providers. Some traditional pay television providers see new online video providers as a major threat to their business models. In certain cases, these developments may also challenge existing policy and regulatory frameworks. In addition to increasing choice and competition, and providing innovative services, the recent surge in online video providers represents an opportunity to advance regulatory reform for the Internet era. As these services involve substantial amounts of traffic exchanged between networks, they have also elicited discussion about issues relating to network neutrality, such as traffic prioritisation or zero-rating, among others.

In addition, some over-the-top players are partnering with traditional telecommunication and cable operators to form mutually beneficial relationships. These arrangements focus around the use of bundled communication services, composed initially of fixed telephony and Internet services, pay television and mobile services, but now encompassing other services. For example, in the United Kingdom telecommunication and cable providers such as BT and Virgin Media offer Netflix, a provider of on-demand Internet streaming media, as an optional part of a bundle. Regardless of the competition implications of service bundling, again both potentially positive or negative, adding new services like home monitoring systems for services such as security to communication bundles may open up new opportunities for communication operators.

Spectrum remains a key element of the digital economy, as any wireless transaction needs to be supported by reliable and fast wireless communications. Policy makers are seeking ways to allocate more spectrum resources to mobile communications and to increase the efficiency of bands already in use. New licensing frameworks such as Licensed Shared Access (LSA), whether currently used by government users or other licensees, target spectrum bands with the potential for shared access at certain points in time or for certain areas, thus opening up the band to more users. While the bulk of spectrum used by communication providers remains licensed on an exclusive basis, LSA and in particular unlicensed bands are gaining prominence. The success of Wi-Fi and RFID technologies proves that unlicensed bands, subject to device power limitations, a sustainable degree of reutilisation and constant monitoring of congestion, may bring substantial benefits for consumers.

Notwithstanding the increasing relevance of mobile connectivity at the network access level, networks at the backhaul and backbone segment use mostly fixed technologies, regardless of the service provided through them, whether mobile or fixed. As a result, backhaul Internet connectivity markets play a critical role in guaranteeing competitive prices for users. While most OECD countries are relatively well served, with the presence of multiple international routes and intense competition, other regions, especially those

outside major international routes, sometimes need public support for the deployment of backhaul and international connectivity infrastructure. Once infrastructure is in place, countries must implement and monitor open access policies to ensure that international connectivity routes, which often require significant investment, are provided by a sufficient number of market players.

4.1 Industry consolidation and policy responses

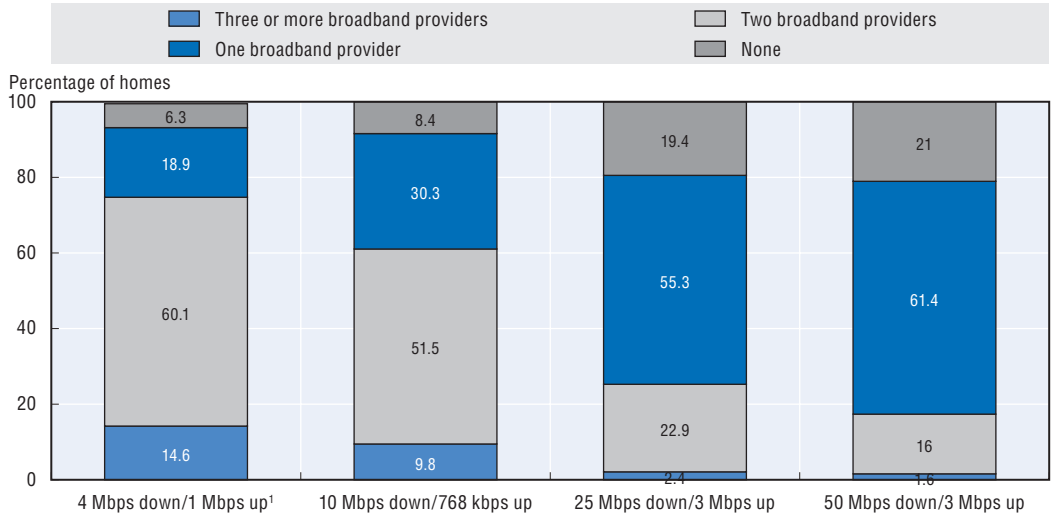
Consolidation in communication and media industries is not a new phenomenon. In the United States, for example, AT&T broke-up the Bell System in 1984, relinquishing control of the Bell Operating Companies; this subsequently resulted in mergers among the seven created "Baby Bells" following the passing of the Telecommunications Act in 1996. In the United States and other countries in the OECD area, there has also been a considerable amount of merger activity between regional cable companies. While many small companies exist in regional areas, in countries that had regional rather than nation monopolies prior to liberalisation, there has been a trend towards consolidation of some of these smaller incumbents.

At present, infrastructure competition exists in most countries between players that grew out of traditional public switched telephone networks (PSTN, which later evolved into DSL) and cable networks (upgraded to provide Internet access services). There is however only limited geographical competition between the same networks (i.e. between DSL infrastructure providers or between cable providers in the same area). In some of these markets, additional players may be present, either because of new private sector entry using fibre or fixed wireless, or municipal networks using the same technologies. In countries that employ unbundling, additional competition is provided by ISPs using the local access facilities of infrastructure-based operators.

Some observers also point to the potential for competition from mobile operators. While these networks certainly provide strong competition for traditional services such as telephony, they are still perceived as largely complementary to fixed networks. Aside from the fact that some mobile operators do not provide a full range of quadruple-play services, or are owned by the incumbent fixed players, wireless networks cannot compete at scale with fixed networks. This is the result of many factors including spectrum limitations and pricing strategies that promote radically different usage patterns for fixed and wireless services. This is best exemplified by the fact that in most countries 70% to 80% of data downloaded by smartphone users is downloaded at private access points (i.e. via Wi-Fi in residences or offices).

The degree of competition in many markets is therefore a function of network performance. In September 2014, the Chair of the Federal Communications Commission (FCC) noted that 75% of households in the United States can choose between two (60%) or three (15%) ISPs to deliver download speeds of 4 Mbit/s (FCC, 2014). This figure reduced to 25% of households for 25 Mbit/s, while 20% had no service option available to them at that level. In other words, a considerable proportion of households can choose from only one (55%) or at best two (23%) providers offering speeds of 25 Mbit/s, a situation which the FCC Chair regarded as insufficiently competitive (Figure 4.1). The situation may have improved as a result of network upgrades by operators, such as AT&T's recent increase in maximum speeds from 24 Mbps to 45 Mbps for certain areas.

Figure 4.1. **Wired broadband speed tiers, number of broadband providers**



Sources: FCC, 2014; National Telecommunications and Information Administration (NTIA), State Broadband Initiative Data (December 2013). These data reflect 3 Mbps up speeds/768 kbps down speeds, which the FCC uses as the best proxy for 4 Mbps/1 Mbps. See FCC, 2010a, for example.

StatLink http://dx.doi.org/10.1787/888933225147

Challenges for policy makers and regulators: increasing choice and meeting growing demand

The challenge of ensuring sufficient competition in fixed markets is not restricted to the United States. Other countries with large geographical territories and even lower population densities, such as Australia and Canada, face similar obstacles in providing choice and innovation to meet consumer requirements. Most OECD countries have addressed this situation either through the use of regulatory tools such as unbundling of local facilities, or through measures such as functional or structural separation. In some cases, countries have opted for public investment in networks, usually linked with open access requirements, although these approaches may lead to a monopoly in wholesale provision. In other cases, new players have entered the market, having identified a business opportunity or a particular location neglected by the incumbents. Typically, this involves municipal networks in part because an existing player may respond to a new entrant by providing investment and improved services in the same location, so as to reduce the attractiveness of investment by the new entrant.

In mobile markets the situation is far more propitious across the OECD area, although there are challenges. The frenetic pace of innovation in the wireless sector compared to fixed markets is the result of greater facilities-based competition. Whereas in fixed networks consumers have at best one or two independent facilities-based competitors, all OECD countries have at least three MNOs and the majority have four. In both fixed and mobile networks ISPs use unbundled networks that provide substantial competition and, for wireless networks, MVNOs that exert competitive pressure on established providers. Nonetheless, the extraordinary innovation around wireless networks compared to fixed networks is undoubtedly due to competition, among other factors, as witnessed by the increases in mobile calling patterns or the extraordinary development of apps. The take-off of mobile broadband services was also assisted by agreements between certain mobile operators and handset device manufacturers, with a view to gaining a competitive advantage.

Going forward, the challenge for policy makers and regulators is to preserve and promote competition, especially where it remains insufficient. Mobile markets have witnessed a spate of recent mergers, but also substantial market entry (see Table 4.1 and 4.2). In a recent report, *Wireless Market Structures and Network Sharing* (OECD, 2014a), the OECD examined the implications of an increase or decrease in the number of players in mobile markets. While stating that market forces should ideally determine the number of players, the report noted that scarcity of spectrum resources and the need for significant network deployment investments, suggest that policy makers may have to take a stance and determine, or at least influence, the number of players in mobile by promoting or preventing consolidation according to circumstances.

Box 4.1. **Mobile mergers in the European Union**

Sector regulators and general competition authorities have long recognised the potential of smaller players to dramatically change competition dynamics in mobile markets. In 2006, the European Commission reviewed a number of mergers in mobile markets, and cleared the merger of T-Mobile Austria and Telering, decreasing the number of operators in the Austrian market from five to four. The resulting firm had a 30% to 40% market share and became the second largest operator in the market. T-Mobile Austria/Telering was the first "gap case" to be examined in Europe. The European Commission recognised that Telering had behaved as a "maverick", thus driving competition, innovation and price reductions. The merger was authorised subject to a number of commitments agreed by T-Mobile Austria, which enabled Austria to retain lower mobile prices (for the OECD area) in the period following the merger (EC, 2006). Since 2010, planned concentrations, whether successful or not, have been more frequent in OECD countries. In view of these concerns, some mergers were blocked, while others were cleared subject to conditions.

In 2013, again in Austria, the European Commission used an innovative approach to assess the Hutchinson/Orange Austria mergers, which was again cleared subject to conditions (EC, 2013). For the first time, the European Commission applied the Upward Pricing Pressure (UPP) analysis to demonstrate that the merging parties (with a joint market of some 25%) exerted considerable pressure on each other, despite their relatively low joint market share, and that the merger would significantly reduce competition.[1] As a consequence, the merging parties would have an incentive to increase prices after the merger. This approach was inspired by the Staff Document of the FCC in the United States, in the analysis of the proposed AT&T/T-Mobile merger (FCC, 2011), which was in the end abandoned.

Over the course of 2014, the Commission also approved mobile mergers in Ireland (O2 Ireland/H3G) and Germany (Teléfonica Deutschland/E-Plus), in both cases resulting in a decrease in the number of independent network operators from four to three and based on commitments offered by the parties (EC, 2014a, 2014b). These conditions surrounded access to the network by MVNOs and, in the Irish and German cases, a commercial relationship between the MNO and the MVNO on capacity-based terms, as opposed to traffic-based charging, which should enhance the incentive of the MVNO to acquire customers. These conditions also involved divesture of spectrum and certain assets. Unfortunately, in the Austrian case, the authorities were not successful in attracting a fourth operator, despite spectrum set-asides, which highlights the challenges for new entrants in relatively mature mobile markets.

Table 4.1. **Mobile mergers in OECD countries**

Year	Country	Operators
2005	The Netherlands	KPN purchased Telfort
2005	Austria	T-Mobile purchased tele.ring
2005	Chile	Telefonica Movistar purchased Bellsouth
2007	Netherlands	T-Mobile purchased Orange
2009	Australia	Vodafone purchased Hutchison-3
2010	United Kingdom	Orange and T-Mobile merged to form EE.
2010	Switzerland	Orange intended to acquire Sunrise, but did not obtain regulatory approval.
2011	United States	AT&T intended to purchase T-Mobile, but did not obtain regulatory approval
2012	Austria	Hutchison 3G purchased Orange
2012	Japan	Softbank purchased eAccess
2012	Greece	Vodafone intended to purchase Wind Hellas, reducing the number of operators to two, but regulators blocked the purchase
2013	United States	T-Mobile purchased MetroPCS SoftBank purchased Sprint and Clearwire AT&T purchased Allied Wireless
2013	Germany	Telefonica purchased E-Plus
2013	Ireland	Hutchison 3G UK purchased Telefonica Ireland
2014	Japan	eAccess merged with Willcom and became Ymobile
2014	Colombia	Tigo (mobile) merged with UNE (fixed and mobile). Regulators required them to divest spectrum.
2014	United States	AT&T purchased Leap
2015	Mexico	AT&T made an offer to acquire Iusacell and Nextel
2015	Japan	Softbank acquired all Ymobile shares

Source: OECD (2014a).

Since 2005, there has also been significant entry into mobile markets, especially as a result of 4G spectrum auctions. Chile, France, Israel, Poland and New Zealand, among other countries, have experienced substantial changes in market dynamics as a result of market entry, with Hungary also planning new market entry in 2015 (see Table 4.2). Nevertheless, if the total number of subscribers in all markets in the OECD area is taken into account, consolidation tends to prevail over new entry, although the overall situation for entry and exit is more balanced than sometimes presented.

Table 4.2. **Recent entry into mobile markets in the OECD area**

Year	Country	Operators
2006	Spain	3 to 4 (Yoigo)
2007	Slovak Republic	2 to 3 (O2)
2008	Slovenia	3 to 4 (T-2)
2009	New Zealand	2 to 3 (2Degrees)
2009	Poland	4 to 6 (Aero2, Centernet)
2012	France	3 to 4 (Iliad/Free Mobile)
2012	Israel	4 to 5 (Golan Telecom (Iliad)
2012	Luxembourg	3 to 4 (Join Experience)
2013	Chile	3 to 7 (Nextel, VTR)
2014	Hungary	3 to 4 (4th license awarded in 2014)
2010-13	Canada	3 to 4
2014	The Netherlands	3 to 4

Source: Based on OECD (2014a).

Policy implications of network sharing and mobile virtual network operators (MVNOs)

Recent years have seen growing use of network sharing between MNOs in OECD countries. Network sharing can decrease costs to a single operator of network deployment and extend coverage to locations that might otherwise be underserved, especially in rural areas. Proponents of the use of network sharing suggest it may avoid a reduction in retail competition while going some way to meeting the objectives of MNOs that may otherwise look to merge.

Network sharing encompasses at least four forms of sharing: (i) passive sharing (e.g. sites, masts and antennae), (ii) active sharing (radio access network sharing), (iii) core network sharing, and (iv) network roaming. Active sharing may include spectrum sharing – the simultaneous use of a specific radio frequency band in a specific geographical area by a number of independent entities (BEREC/RSPG, 2011). It should be noted that, in this case, the term "spectrum sharing" refers to the joint use by two (generally private) entities, as opposed to Licensed Shared Access (LSA), discussed below, where the focus is on the eventual use of spectrum resources already licensed to an "incumbent" user.

Japan provides one example of an approach to network sharing. The Japan Mobile Communications Infrastructure Association (JMCIA), which includes all Japanese MNOs, major facility vendors and developers as members, shares facilities in locations such as tunnels. While base transceiver stations (BTS) are run separately by the MNOs, the JMCIA provides transmission facilities from BTS to antennae.

Network sharing can raise competition issues which should be addressed prior to its introduction. These include: (i) unilateral effects, (ii) potential coordination, and (iii) information sharing. By way of example, a market with four MNOs and two sharing agreements may facilitate co-ordination and effectively result in a wholesale duopoly. This is why regulators and competition authorities need to remain vigilant and monitor sharing agreements. A further aspect of network sharing, which needs to be considered, is the competitive role of MVNOs and whether they exert sufficient pressure on MNOs. The FCC in the United States has stated that MVNOs do not play a substantial role in all the industry's competition dimensions (e.g. some forms of non-price rivalry), whereas many European markets have a significant MVNO presence (e.g. 16.8% in Belgium, 19.5% in the Netherlands, 13.2% in Spain, as of end-2013).[2] This suggests that MVNOs play a more important role in competition dynamics in these countries.

Fixed-mobile convergence trends

A notable trend in the OECD area is growing cross-ownership between fixed network and mobile operators. While incumbent fixed telecommunication networks have long owned MNOs, there have been recent moves by cable and mobile network operators to merge or purchase one another. In 2013-14, Vodafone purchased ONO and Kabel Deutschland (the leading cable operators in Spain and Germany) and Numericable launched a successful takeover of SFR in France. Meanwhile, in 2012, Foxtel (cable) merged with Austar (satellite) in Australia to complete a nationwide pay television service. Foxtel is half-owned by Telstra, which has the largest MNO in that country.

The cable industry has also experienced consolidation in many OECD countries, both at the national and international level. In the United States, Comcast's bid for TimeWarner Cable (the largest and second largest cable operators in the country) is being analysed

by authorities. Some believe that a merged Time Warner-Comcast entity would have implications for the pay television industry in the United States, including at the levels of content aggregation and rights acquisition. Comcast already has substantial interests in television content companies (e.g. Universal studios, NBC). In addition, any merged entity would constitute a large player in the areas of peering and transit, given their control over a substantial proportion of customer access networks. A further notable development is the bid by AT&T for DirecTV, the largest satellite multichannel video-programming distributor (MVPD) – a market where AT&T is also present. The new entity would be able to provide a full range of voice, broadband and video services, including through mobile technology.

In 2014, Telefónica announced its intention to buy the largest pay television provider in Spain (Digital Plus) for a reported USD 913 million. Digital Plus holds a 63% market share in revenue terms. If the transaction goes through, Telefónica would control nearly 80% of Spain's pay television market (60% in terms of subscribers). Drivers for market concentration in Spain are believed to include raising content costs, especially live football, and a decrease in pay television subscribers as a result of the economic crisis. Similar transactions have already taken place in Australia where the largest telecommunication network also owns the largest pay television provider, and Canada where telecommunication companies are major owners of television. Liberty Global, headquartered in the United States, is also pursuing a series of acquisitions of cable operators in many OECD countries. The company runs cable operations in Chile, Czech Republic, Germany, the Netherlands, Poland and other countries in Central and Eastern Europe. In 2013, Liberty Global acquired the largest cable operator in the United Kingdom (Virgin Media) for USD 24 billion.

Box 4.2. **Consolidation and competitiveness in the European market**

A truly European internal market is one of the high-level goals of the European Union.[3] Industry consolidation is playing a key role in the debate on industrial policy and the promotion of the European Union's internal market. Successive European Union Commissioners responsible for the Digital Agenda have repeatedly voiced the need to overcome national borders and have been supportive of consolidation that leads to a Digital Single Market. The European Telecommunication Network Operators' Association (ETNO) has also argued that a larger scale market would allow European operators to compete more effectively and position themselves in value chains, where Internet content providers also play a major role.

In telecommunication markets, policy debates seem to focus on whether domestic consolidation within countries (e.g. Austria, Germany and Ireland) should be allowed, rather than on transnational mergers (e.g. Vodafone/ONO, Liberty Global/Virgin Media). Notably, mobile market consolidation in Europe seems to be taking place more markedly within countries, than as a result of European operators expanding their footprint to cover more countries. Indeed, in some cases transactions between different MNOs reduce cross-border ownership within Europe of affiliated companies (e.g. SFR was sold by Vodafone and subsequently purchased by a cable company).

In this respect, there is a perceived misalignment between calls for the creation of pan-European operators to compete with their largest peers in the United States or China, although the largest players from both markets do not have extensive overseas operations, and the industry's preference for domestic consolidation. The European Union's intervention on international mobile roaming, which has regulated retail and wholesale prices since 2007, is one example of a case where regulators found it necessary to act in the absence of pan-European firms offering competitive outcomes for consumers.

From a public policy perspective, it is important to make sure that such concentrations do not affect competition in the coming years, as was the case with pay television mergers in Europe in the early 2000s – also in a scenario of rising content costs.[4] These transactions demonstrate that market players are positioning themselves to take advantage of the economies of scale and scope of fixed and mobile operations, such as joint backhaul and backbone networks. If bundling of fixed and mobile services becomes dominant in the near future, these operators would also benefit from unified offers and early positioning from the customer's perspective.

The transactions mentioned here relate to trends in convergence in OECD countries. They point to convergence between fixed and mobile networks, as well as between infrastructure and content or television companies. Some of the services these companies provide are also converging with the Internet and the mergers should be viewed in this light, as they seek to limit adjacent competition or better place themselves to compete with other such merged players.

4.2 Convergence: Service bundles and the rise of over-the-top operators

Competition and service bundles

Consumers can benefit from bundles through discounts over the sum of the price of standalone prices, unified billing and, potentially, innovative services at low incremental prices. Unified billing may render bills less complex and more understandable, but it can also raise challenges to price comparison if service bundles cannot be easily compared. This section highlights some of the challenges involved in comparing bundle prices. According to the January 2014 Special Barometer of the European Union, 46% of households in the area covered purchased a bundle of communication services, which translates to an increase of 3% since December 2011.[5] Some policy makers have sought to increase billing and price transparency by requiring operators to disaggregate the prices of each service component (e.g. Finland, the Netherlands for handsets, Slovenia), while in other countries, operators do so voluntarily.

A good example of bundling practices is the sale of smartphones at a significant upfront discount, when purchased together with a mobile communication plan. This practice has played a substantial role in users acquiring or upgrading their smartphone devices. Nevertheless, as the OECD report *Mobile Handset Acquisition Models* highlights, the practice may render consumer switching more difficult and, in most cases, represents a higher cost for consumers if the total cost of ownership (mobile communication plan and device) is considered (OECD, 2013). Between 2012 and 2014, SIM-only offers have become more important and some countries have promoted transparency measures, such as requiring operators to disaggregate the handset costs in monthly bills (e.g. Finland, France, the Netherlands, Slovenia). In November 2014, the Ministry of Internal Affairs and Communications of Japan mandated operators to unlock mobile handsets sold from May 2015, if users so request, and at no cost, to enable consumers to switch operators more easily. This will increase user choice and facilitate the use of other operators' SIM cards – previously impossible with a locked device. In the European Union, a proposal is being discussed to give consumers the right to terminate a contract six months or longer after signature, at no compensation other than the value due for the "subsidised" bundled handset device.[6] In the United States, unbundling of handsets from mobile services is now taking place, largely driven by competition and customer demand.

Some service bundles may lead consumers to purchase elements they would otherwise not buy as a stand-alone service. For example, a consumer might want broadband Internet access but receive a basic television service as part of the bundle. Alternatively, a user wanting telephony and television may value less Internet access capability. A potential benefit of this approach may be increased service penetration (i.e. consumer surplus from one service may help subsidise another less-valued element) (OECD, 2011). This phenomenon is generally welcomed as the increase in uptake is thought to bring wider economic and social benefits, such as in the case of broadband access. Conversely, bundling and tying may have negative effects on competition.

Firms may choose to bundle a good or service from a competitive market with a good or service where they have some degree of market power, with a view to engaging in horizontal foreclosure (Rey and Tirole, 2006). In this case, the good could be premium television content. For example, the Board of European Regulators of Electronic Communications (BEREC) recognised that the most important source of competition concerned the inability of operators to offer pay television services (especially premium content) and by extension triple-play packages (BEREC, 2010). Indeed, access to premium television content has been addressed through ex-ante regulation, competition law and merger decisions in most OECD countries. In 2010, the Office of Communications (OFCOM) in the United Kingdom imposed (based on ex-ante broadcasting regulation) a wholesale obligation on the leading pay television provider (Sky) to offer its wholesale sports channels at regulated prices to third-party providers.

In the United States, in view of similar concerns (access to content, though unrelated to bundling issues), the 1992 Cable Act introduced the Programme Access Rules (PAR) to facilitate access to popular content by non-affiliated retail pay television providers. In 2012, the FCC phased out the PAR in view of increasing competition from satellite providers. With the advent of online video distributors (OVDs) such as Hulu and Netflix, competition authorities in France (Autorité de la Concurrence) and the United States (DoJ and FCC) have taken due care to ensure that OVDs have the ability to purchase content under fair and reasonable terms. Most of these measures have been linked to mergers. In October 2014, for the first time, the FCC Chairman announced that the definition of "multichannel video programming distributors" (MVPDs) would be reviewed, to allow OVDs to avail themselves of protections granted to traditional cable or satellite pay television providers in the United States, such as the possibility to seek arbitration in negotiations with programmers. This effort to accommodate Internet players under traditional rules represents a step towards regulatory reform.

Communication regulators may also need to monitor competition for bundles, as they do for stand-alone services, to ensure that competition is not diminished by the use of bundling. In 2014, the Portuguese Competition Authority cleared a merger of the two major telecommunication operators in Portugal – Zon and Optimus (Sonaecom) – by defining a relevant market consisting of a triple-play bundle (PCA, 2013; Pereira et al., 2013). In a number of countries, dominant fixed operators or those with significant market power (SMP) are precluded from bundling unreasonably, or are required to offer stand-alone services (e.g. incumbent operators in Austria, Belgium, Germany, Greece, Ireland, Italy, Korea, Slovak Republic, Slovenia and Switzerland). That being said, service bundling, especially mixed bundling, makes economic sense in some cases, for example, by allowing the allocation of fixed costs across a number of different services. It also creates opportunities to launch innovative services and provides customer benefits such as unified billing, and in some cases simpler offers for consumers.

An arguably less problematic issue raised by service bundles is fixed-mobile convergence. If competition shifts to quadruple-play bundles (with a mobile element), market players that lack mobile operations could be excluded from competition, even though fixed-only operators could well become MVNOs, if allowed by regulatory frameworks, in order to replicate these bundles. In 2014, the OECD undertook data collection to ascertain how widespread fixed-mobile offers were in each of the 34 OECD countries (OECD, 2015). According to the results, 61 out of 104 fixed broadband operators surveyed (in most cases three operators in each of the 34 OECD countries) had an MNO subsidiary and an additional 17 had MVNO operations. Nevertheless, in only five countries did all three fixed broadband operators, included in that country, have a fixed-mobile integrated offer. These three operators were the three largest fixed broadband providers in every OECD country, covering on average over two thirds of fixed broadband subscribers. Some small fixed broadband operators not included in the dataset may be less likely to have mobile operations.

Triple-play bundles (fixed broadband, voice and pay-tv) are among the most popular in most OECD countries after double play (fixed broadband and telephony or fixed broadband and pay television). Quadruple-play, where offered, usually consists of fixed broadband, fixed telephony, pay-tv and mobile services, which in turn include mobile voice, broadband and SMS. A few exceptions exist in countries where mobile services are sold in bundles without a pay television component. In 2012 in Spain, Telefónica launched "Fusión", a set of plans that combine fixed and mobile services. These bundles including fixed broadband and telephony and mobile services – not pay television – accumulated 46% of fixed broadband subscribers by the end of 2013 (CNMC, 2014), due partly to replication by competitors. As of May 2014, the "Fusión" bundle no longer offers the option to exclude pay television from the bundle. These developments represent a significant change in the Spanish communication market and raised possible competition concerns, in particular with regard to access to mobile services and television content by competitors.

Convergence: Access any service over the Internet

In addition to independent provision of over-the-top (OTT) services, 2012-14 saw a dramatic increase in partnerships between traditional telecommunication operators and OTT providers. For example, traditional telecommunication operators in Finland, France, Ireland, the Netherlands, New Zealand, Slovenia, Slovak Republic, Spain and Sweden are now offering online music services such as Spotify or Deezer as part of bundles. Other operators such as TDC Play (Denmark), Vodafone, NOS and Portugal Telecom (Portugal) and TTNet (Turkey) have chosen to develop online music stores.

Arguably, some deals between OTTs and traditional telecommunication operators may have major implications for markets and the full value chain. For example, this is the case for deals involving video service providers such as YouTube, Dailymotion and Netflix. Cable operators offering the TiVo Box (e.g. Virgin Media in the United Kingdom, UPC and Comhem in Sweden) have advertised the inclusion of the Netflix app as part of the TiVo interface.[7] This list has recently expanded with France Télécom, SFR and Bouygues Télécom in France due to include the Netflix app in their set-top boxes. This is also the case for three small cable operators in the United States (Atlantic Broadband, Grande Communications and RCN). While these services can be accessed via other pathways (e.g. smart-televisions or the World Wide Web), they may be provided at a discount if bundled with telecommunication operators. Virgin Media in the United Kingdom, for example, was arguably the first major

operator in the OECD area to actively advertise Netflix, offering in Q2 2014 to bear the costs of the first six months of Netflix subscription (Figure 4.2). In Mexico, the online video service Clarovideo is being provided at no additional cost with some Telmex bundles.

Figure 4.2. **Virgin Media's VIP Collection, United Kingdom**

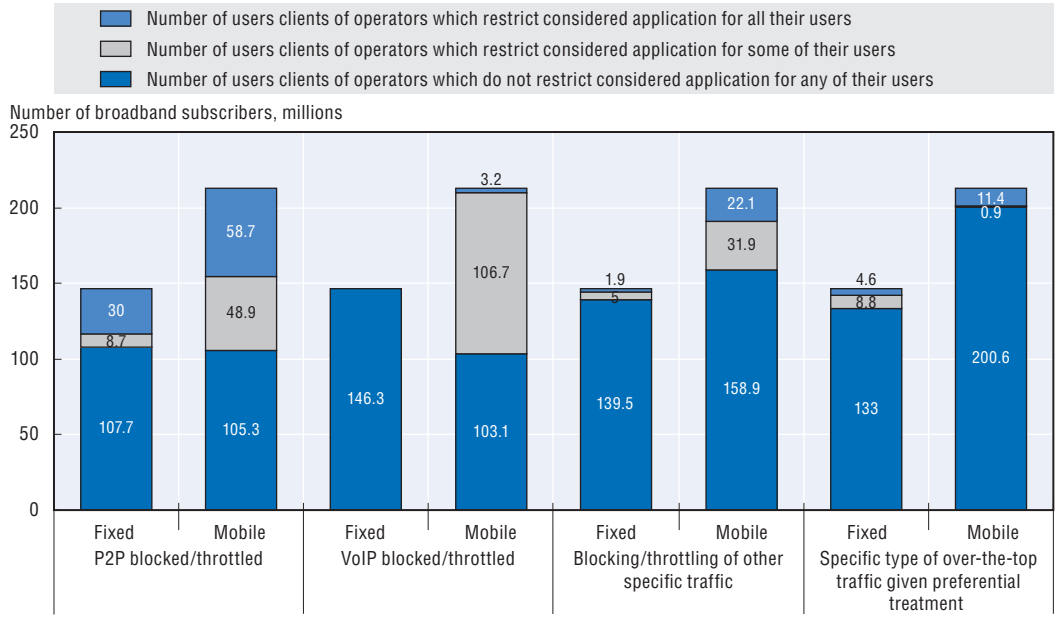
Source: Virgin Media, United Kingdom. *www.virginmedia.com/*.

Broadband providers are also opting for the inclusion of other services as a means to strengthen their customer relationships and reduce turnover. These services include home management systems, banking/payment services and enhanced connectivity features such as cloud services or Wi-Fi hotspots. Home management services are a good example of how a telecommunication infrastructure provider can leverage its physical presence (networks to the premises of consumers and businesses) to work with providers of security services. In Canada, Rogers Communications is advertising home monitoring services as part of its bundles, at the same level as Internet, television and telephony, highlighting the major role they play in the company's marketing strategy. International VoIP calling through Wi-Fi networks is another additional service provided by mobile providers, such as Fastweb in Italy or AT&T in the United States. While OTT services such as Skype or Viber, to name two, provide a similar service, the inclusion of an app by the customer's operators may provide savings and could arguably involve a better consumer experience. The introduction of Voice over LTE (VoLTE) has pushed the market even further. Instead of requiring a separate application to call via Wi-Fi, telephones that support Wi-Fi calling using VoLTE IP telephony will set up the call using any available Wi-Fi connection, even if located in a different country. This service is now available from operators such as Sprint.

Adjusting policy and regulatory frameworks to the new convergence paradigm is not without its challenges. The principle of technological neutrality would suggest that similar services should operate under the same rules and conditions, but this principle may pose a fundamental challenge to most regulatory frameworks, where the Internet and traditional voice telephony and television broadcasting services stem from radically different environments. Advancing regulatory reform towards technology-neutral frameworks will help to provide a clearer set of rules to improve market efficiency. One challenge to updating the regulatory framework is approaches to measuring Internet content production and distribution, including monetary flows and associated business models, for which a demand-side rather than a supply-side approach is advisable.

A further challenge may arise if network operators block an OTT service, on the basis that it "cannibalises" their revenues for particular services. While customers pay for data to use a VoIP service, for example, this may undercut traditional pricing for telephony. Some regulators have conducted surveys to assess the extent of these practices. For example, a joint investigation by BEREC and the European Commission revealed that over 50% of mobile operators, weighted according to their total number of users, had blocked or throttled VoIP applications for all or some of their users (BEREC, 2012) (Figure 4.3). An increasing number of operators avoid such issues simply by charging for data and including voice and text as an integral part of a bundle. A number of countries have introduced legislation to ensure network neutrality and prohibit blocking and unreasonable discrimination of services (see below).

Figure 4.3. **Operators applying some level of restriction, weighted according to their total number of users**



Source: BEREC (2012).

StatLink http://dx.doi.org/10.1787/888933225155

Connected televisions

Many communication infrastructure providers have raised concerns that new video services provided by OTT video providers (e.g. Netflix or Hulu) may cause a "data tsunami", threatening the overall functioning of the Internet. According to some estimates, Netflix traffic accounts for 30% of peak load in the United States, yet the sustainability of networks and investment does not seem to be at risk. It is unlikely that increasing data traffic will become unsustainable, if networks continue to invest, because its relative growth rate from a higher base is at a historical low for both peak and average rate and continuing to decline (OECD, 2014b). Any bottlenecks are more likely to occur between two specific networks, or autonomous systems to use the precise term, rather than presenting a problem for the general Internet.

Over-the-top video services have witnessed considerable technical and business innovation. In response, traditional television broadcasters and pay television providers are increasingly migrating content to the Internet. For example, Swedish company Magine offers online television and cloud-based digital video recorder (DVR) services in Sweden, Germany and Spain. Networked and cloud DVR services have been launched in several countries including Australia (Optus), France, Switzerland (FilmOn) and the United States (Cablevision). In some cases, they have been subject to court challenges, which underline the inadequacy of current regulatory frameworks to address video services provided over the Internet.

This is in contrast to relatively rigid traditional pay television markets, where in many cases content licensing is subject to strict rules and markets are relatively concentrated. In 2014, the European Commission opened a market investigation into cross-country content licensing (called "absolute territorial exclusivity"), which currently grants full territorial exclusivity for certain content rights. For example, a subscriber to the German association football league "Bundesliga", through the leading pay television broadcaster, could not watch games if resident in France. In turn, there may or may not be a television provider interested in buying those rights in France.

Online video distributors have the potential to augment competition significantly in video markets, provided that the whole value chain benefits from increased competition and transparency, and that regulatory frameworks evolve towards the principle of technological neutrality. For their part some of the largest players are beginning to offer IP services, independent of whether a user has cable or satellite or a transitional pay television subscription. In the United States, for example, Time Warner's HBO and CBS announced stand-alone streaming offers in 2014 similar to those offered by Hulu Plus and Netflix. Such offers, already common in Nordic countries, may spread to other parts of the OECD area, allowing consumers to access television services *à la carte*.

4.3 The network neutrality debate

The network neutrality debate concerns complex issues surrounding traffic prioritisation and consists of two main points. The first relates to factors that affect the ability of users to access content and services, such as differentiation through pricing, quality of service or blocking of access (e.g. blocking VoIP services). The second relates to commercial arrangements that enable traffic exchange between networks (i.e. peering and transit). Both issues concern the relationship between a user and their ISP, whom they have paid for access to the Internet, and the terms and conditions to which networks agree in order to exchange traffic. In the United States, most policy discussions on network neutrality have so far focused on last mile issues (i.e. the last leg of delivery up to the home or business),[8] even though the FCC has sought comments on the effects of business arrangements between third-party providers and ISPs on Internet openness.

The economic literature on issues relating to network neutrality is relatively recent, but is evolving rapidly. It examines issues such as network management practices, the two-sidedness of Internet interconnection markets, innovation aspects, terminating monopoly issues and so forth, without reaching definitive conclusions or being strongly dependent on the assumptions made. Krämer et al. (2013) have provided a survey of economic literature on network neutrality.

Network neutrality in Internet access service

Changes in access to content, services or networks terms, including quality, may alter outcomes for users of the network and affect the capacity of users on other networks to communicate with them. Any unreasonable limitation on such communication, without the consent of the user and beyond necessary network management, could lead to different quality levels for alternative network paths, which – while all using IP technology (e.g. an ISP's own video service) – do not treat traffic in the same manner. Apart from the potential "fragmentation" that could result from any impairment to the user's ability to access the Internet – as opposed to independent, third-party service provision – limitations on access could have implications for the Internet as a platform for innovation.

A number of OECD countries have introduced legislation to ensure network neutrality and have prohibited blocking and unreasonable discrimination of services. In 2010, Chile was the first OECD country to legislate in favour of network neutrality, followed by the Netherlands (2011) and Slovenia (2012). Meanwhile, in April 2014, in the lead up to NET Mundial, an international summit on Internet Governance held in São Paulo, Brazil's Congress passed the bill "Marco Civil da Internet" (the Internet Civil Framework Act), which affirms that network neutrality should be the rule on the Internet (although the implementing regulations still need to be developed by Presidential Decree; see Chapter 1, Box 1.3). Italy is following a similar process with a public consultation launched in October 2014 on a statement of principles on Internet rights. Among other things, the statement proposes a "fundamental right to Internet access" and network neutrality.

There is no unified approach towards network neutrality in the OECD area and policy frameworks vary from country to country. In some countries, provisions on network neutrality are established jointly with the industry, such as the Norwegian model of co-regulation, or the Korean "Guidelines on Net Neutrality and Internet Traffic Management", published in December 2011. For its part, the United Kingdom focuses on transparency and sufficient competition, favouring self-regulation, with a view to providing consumers with adequate information to make an informed decision. European countries follow different approaches on network neutrality, ranging from self-regulation to binding legislation. To avoid fragmentation of the EU single market, the European Commission has set an objective of establishing clear EU-wide rules to safeguard the open Internet. .A legislative proposal is being discussed in the European Union that would ensure that end users are free to access and distribute information and content, run applications and use services of their choice on the Internet. The proposal protects the non-discriminatory open Internet, while allowing for innovative services with specific quality requirements. The European Parliament adopted its position on the proposal on 3 April 2014 and the Council gave a negotiation mandate to the Latvian Presidency on 4 March 2015. Dialogues between the institutions started in March 2015.

On 12 March 2015, the FCC of the United States released the Order "*Protecting and Promoting the Open Internet*", which established three "bright line" rules applicable to both fixed and mobile broadband Internet access service, prohibiting blocking, throttling and paid prioritisation (FCC, 2015). Under the new rules, broadband Internet access providers are prohibited from blocking lawful content, applications, services or non-harmful devices, subject to reasonable network management. For throttling, the rule states that ISPs shall not impair or degrade lawful Internet traffic on the basis of Internet content, application or service, or use of a non-harmful device, subject to reasonable network management. ISPs

also shall not engage in paid prioritisation. "Paid prioritisation" refers to the management of a broadband provider's network to directly or indirectly favour some traffic over other traffic, including through use of techniques such as traffic shaping, prioritisation, resource reservation or other forms of preferential traffic management, either in exchange for consideration (monetary or otherwise) from a third party, or to benefit an affiliated entity. To address any future concerns that may arise with new practices, the Order includes a standard for future conduct rule that prohibits ISPs from unreasonably interfering with or unreasonably disadvantaging the ability of consumers to select, access and use the lawful content, applications, services or devices of their choosing; or of edge providers to make lawful content, applications, services or devices available to consumers. Reasonable network management is not considered a violation of this rule. The Commission will have authority to address questionable practices on a case-by-case basis, and to provide guidance in the form of factors on how the standard will be applied in practice. The Order also enhances the transparency rule adopted in 2010 for both end users and edge providers, including by adopting a requirement that broadband providers must always disclose promotional rates, all fees and/or surcharges, and all data caps or data allowances; adding packet loss as a measure of network performance that must be disclosed; and requiring specific notification to consumers that a "network practice" is likely to significantly affect their use of the service (FCC, 2010b).

In addition, the Order establishes that the Commission can hear complaints and take appropriate enforcement action if it determines that the interconnection activities of ISPs are not just and reasonable. The Order reclassified broadband Internet access as a telecommunications service under Title II of the Communications Act, but decided to forbear this service from major provisions of the Title II including rate regulations, tariff filing and unbundling.

In Canada, the Canadian Radio-television and Telecommunications Commission (CRTC) released a network neutrality framework in 2009. The framework guides the telecommunication industry in the use of acceptable traffic management practices. Should these practices be necessary, the policy emphasises that economic measures (e.g. monthly usage caps, overage charges) should be used wherever possible; technical measures (e.g. traffic prioritisation) should be applied only as a last resort, and outright blocking or degrading time-sensitive traffic is prohibited unless prior CRTC approval is obtained. The policy emphasizes that ISPs must be transparent in the management of traffic on their networks.

Traffic exchange between networks: Peering and transit

The Internet's model for traffic exchange works extremely well and has been a major ingredient in enabling it to scale so rapidly and pervasively. At its heart, every user of the Internet pays for his or her own access. In turn, their ISP undertakes to provide connectivity to the rest of the Internet either through peering (direct interconnection) or transit. The purchase of transit enables an ISP to reach all networks around the world. Peering enables two ISPs to directly exchange traffic while bypassing the transit providers. Through the use of peering, ISPs can reduce their costs, as they do not need to purchase transit for that traffic. To save costs, ISPs establish or make use of Internet Exchange Points (IXPs), where they can peer with multiple networks at the same time. The largest IXPs can have over 600 connected networks and over 3 Terabit/s of traffic. Meanwhile, the purchase of transit enables them to more economically reach networks where they do not have their own facilities.

A survey undertaken for an OECD report of 4 300 networks, representing 140 000 direct exchanges of traffic on the Internet, found that 99.5% of "peering agreements" were made on a handshake basis, with no written contracts, and exchange of data occurring with no money changing hands. Moreover, on many IXPs multilateral agreements are in place, using a so-called route server where hundreds of networks accept to exchange traffic for free with any network that joins the agreement. The parties to these agreements include Internet backbone, access and content distribution networks, as well as universities, non-governmental organisations, branches of government, businesses and enterprises of all sorts.

Under the current voluntary system, operators have an incentive to invest and expand their network to reach new peers, and to co-operate with other networks to establish new IXPs in areas where there are none, because they save on transit costs. Indeed, peering locations have been established in every corner of the world and large content providers and Content Distribution Networks (CDNs) have expanded their networks into these locations – in both developed and developing countries. This has saved them and their customers – including the ISPs they peer with and their customers – billions of dollars each year, while greatly increasing quality of service. Expanding the number of IXPs helps to keep local traffic local, unburdens interregional links and stimulates investment in local networks. For this reason the OECD continues to encourage countries to develop and use IXPs.

Content Distribution Networks have evolved during the last decade to become important players in reducing traffic costs for both content providers and ISPs, and achieving overall quality and performance improvements. Akamai is the largest CDN in the world with at least 50 global and regional competitors, some of which are part of transit networks, such as Level 3. Some traditional telecommunication operators, such as TDC in Denmark, have developed their own CDNs. The possibility of contracting with several CDNs provides ISPs and telecommunication operators with a range of options. Typically, CDNs have servers, peering agreements and network connectivity in a large number of countries, which alleviates possible congestion problems and increases network performance in terms of latency, interconnection capacity and so forth.

Some commentators have argued that CDNs constitute a special class of networks, distinct from content providers and telecommunication operators. They suggest that CDNs provide non-neutral high-speed lanes to consumers, but only for sites large enough to pay the cost. This view does not appear correct from a number of perspectives. At the technical level, networks cannot distinguish between CDNs, content providers or telecom operators. For the routing protocol BGP, all AS numbers are the same and can provide the same services. At the business level, a CDN saves its customers the need to deploy and manage servers globally and negotiate with hundreds of networks over peering and transit costs. Most customers do not have the scale necessary to make investments in servers, IXP memberships and peering negotiations worthwhile, and for them a CDN is a way of receiving the benefits, without the level of investment needed. However, some of the largest Internet players, such as Google, Microsoft and Netflix, have developed their own CDN-type solutions, and Apple and Facebook are reportedly working on similar solutions. Netflix, for example, estimated a 20% saving in the efficiency of equipment and network resources use for its OpenConnect CDN, which is optimised for its traffic over commercial, non-optimised CDN services. This can result in a better performance and cost savings on equipment and IP transit, not just for Netflix, but also for the ISPs with which it interconnects. Many smaller

and local sites will not use CDN services because the costs outweigh the benefits they receive, or they can achieve the same benefits by peering directly with local networks or placing their servers in multiple collocation facilities.

The Internet has thus enabled the development of an efficient market for connectivity based on voluntary contractual agreements. Operating in a highly competitive environment, largely without regulation or central organisation, the Internet model of traffic exchange has produced lower prices, promoted efficiency and innovation, and attracted the investment necessary to keep pace with demand. Nonetheless, where commercial negotiations do take place and in the absence of sufficient competition, one player may leverage their position to extract higher rents from others. In such instances, ISPs have the option to bypass each other. This is a key reason behind the success of the Internet in competitive markets.

In the absence of sufficient retail competition the question arises as to whether consumers are receiving the service for which they pay. This can be a challenging area to address given that the Internet is a network of networks with each network responsible for delivering connectivity and traffic to their own customers. Nevertheless, computer scientists are developing tools to investigate and inform stakeholders about questions such as whether congestion exists and, if it does, where it originates. One example is a project being undertaken by the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory jointly with the Centre for Applied Internet Data Analysis (CAIDA/UCSD) for the United States. In 2014, the findings of the preliminary report did not reveal widespread congestion among ISPs in the United States, with most congestion attributed to specific business uses, and interconnection disputes seemingly being resolved through commercial negotiations. Similar projects in other parts of the world would contribute greatly to informing policy makers and regulators.

Network neutrality and zero-rating

If the traffic sent and received by consumers over the Internet is metered and some specific traffic is unmetered, the industry applies the term "zero rated" to the latter. Although the term is used mostly in the context of mobile data, it has been applied to both fixed and mobile broadband services. Historically, only in a minority of OECD countries, such as Australia, Belgium, Canada, Iceland, Ireland and New Zealand, are explicit data caps common in fixed broadband plans. In others, fair use policies may exist with a different degree of enforcement. In mobile markets, which are generally subject to much lower data caps, zero-rating may have significant implications in competition dynamics.

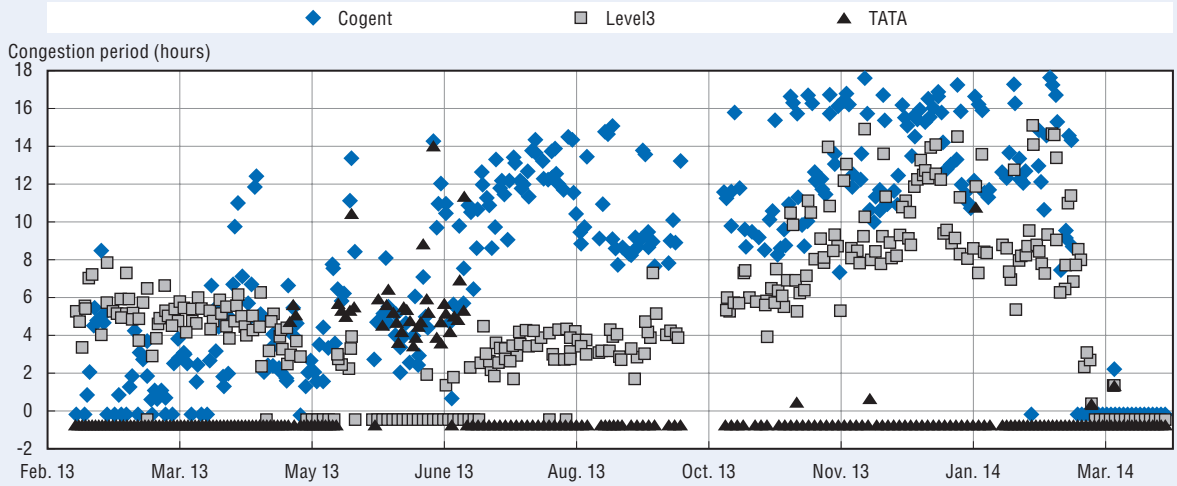
Zero-rating can take a number of forms. One is where zero-rating is applied by ISPs to their own content or that of pre-selected partners. This can range from the content of the home screen viewed by an ISP's customer, through to proprietary content such as video or music services, which are paid for by consumers in their bundle. In Australia, for example, some ISPs purchase the rights to major sports. When one of their customers accesses this content it does not count against their data cap. Alternatively, if the customer of another ISP accesses that content over the Internet, they would pay both a subscription charge to the service and have this data counted against their allowance by their own ISP. It is common, therefore, for ISPs to offer services such as games or other content, with it not being counted against a consumer's data allowance.

Some mobile operators partner explicitly with a video or music service. Other operators, such as T-Mobile in the United States, whitelist a number of music services and exclude them from counting against a customer's data cap. In Hungary, T-Mobile takes a

Box 4.3. **Interconnection disputes between Comcast and Netflix**

In the second half of 2013, an interconnection dispute arose related to congestion between Comcast and Netflix. Metrics tracked by MIT and USCD indicated congestion leading up to early 2014. In February 2014, to resolve this issue both companies reportedly came to an agreement to directly exchange traffic. At that time, congestion on those links, largely recorded in transit networks selected by Netflix, disappeared (Clark et al., 2014a).

Estimated congestion duration for links connecting three major networks to Comcast



Sources: Clark et al., 2014a, 2014b.

StatLink http://dx.doi.org/10.1787/888933225165

While interconnection disputes can be an outcome of business negotiations, with quality degradation used as a bargaining tool, they rarely represent a concern for regulators because both parties can still buy transit to reach each other. Disputes only represent a concern for regulators where assessment highlights insufficient competition and transparency for consumers and networks to make informed choices. If as seems likely Netflix paid Comcast to directly interconnect between the two networks, Comcast would receive revenue both from its own customers to deliver services such as Netflix in addition to the fees they receive from Netflix (i.e. Netflix passes these costs on to its customers). Some economists perceive this as a two-sided market; however, this leaves out the option for competitive transit for Netflix. The key question is whether consumers have sufficient choice to reach a service such as Netflix via an alternative ISP or (given that the video services of both Netflix and Comcast can to an extent be viewed as substitutes) does Netflix have sufficient competitive transit providers to reach its customers. From Comcast's perspective the aim is to maximise its return on investment in networks and services.

The traffic congestion situation between Netflix and Comcast was resolved through direct interconnection. However, instead of using peering or transit to facilitate the interconnection, the parties used a model sometimes referred to as "paid peering". In such cases, one network agrees to pay another to exchange traffic, but not for that network to carry this traffic to a third network (i.e. the latter would be transit). Netflix said it reluctantly paid for direct peering because it could not locate a transit provider offer that was not either congested or simply required it to pay for peering via the third party. Some large ISPs propose to adopt interconnection charging based on the "Sending Party Network Pays" principle because they believe this situation is similar to the terminating access payments common for telephony. Unlike telephony markets however, peering markets are generally regarded as competitive. In the telephony market, almost all OECD regulators have found a terminating monopoly on the side of the access network. At heart the issue is the same, with both networks exchanging traffic contending they bring greater value to the exchange and that

Box 4.3. **Interconnection disputes between Comcast and Netflix** *(cont.)*

this should be the basis for the relationship. Historically, this was resolved in the market for peering and transit, precisely because no network was large enough not to need transit to reach the rest of the world. This would, therefore, leave an alternative path via transit open, if both could not peer either because of location or because of commercial differences.

Ensuring sufficient local access competition, while not eliminating monopoly power over termination, disciplines behaviour because it empowers consumers. In addition, as discussed below, Australia and New Zealand's experience following the turn of the century, in an uncompetitive market for peering and transit, demonstrated that the so-called, "zero-rating" access for Internet content can be used as a competitive tool by ISPs and content providers agreeing to peer directly.

different approach by charging an extra fee for zero-rating certain types of use, such as video or social networks. To date, regulators have taken different positions on this practice. In Canada, Chile, Norway, the Netherlands and Slovenia, regulators have made explicit statements against zero-rating, which they have assessed as anti-competitive, or imposed fines as a result of a violation of that country's net neutrality regulation. In other countries the practice exists among various operators in different forms and regulators have not taken action.

Another type of zero-rating may occur when there is a large difference in price between on-net and off-net traffic (i.e. either traffic supplied by the ISP itself and its unpaid peers or content obtained via an IP transit network is treated for billing purposes as "off-net"). In countries with little competition in transit or backhaul markets, entering into direct peering relationships can be a win-win for the ISP and the content provider. It enables those ISPs and content providers to exchange traffic without payment and pass the benefit onto their customers. This would not be possible in the absence of peering or where transit is expensive. These kinds of arrangements tend to be popular in countries that have low bit caps included in monthly allocations as a result of high transit prices. As the size of bit caps increase due to factors such as increased competition and a decrease in transit prices, zero-rating becomes less important for attracting end users. This is because there is little difference from the consumer's perspective between zero-rated content and using data in a large cap or for a wholly unmetered service.

In Australia, lower bit caps due to high IP transit rates resulted in the use of zero-rating as a competitive tool. Smaller ISPs and content providers, such as radio stations, directly exchanged traffic and ISPs passed on the lower costs to their customers through zero-rating. This enabled consumers with low bit caps to stream audio from these stations – an option that would not have been attractive at metered pricing. If regulation had required these ISPs to treat this traffic in the same manner as that of any other content provider not directly interconnecting with them, it would have distorted the incentives for peering and transit. In other words, the ability to reduce costs by peering, and then pass these reductions onto their customers, enabled the ISPs and a radio station to benefit along with users. On the other hand, even if ISPs average costs in their retail prices, between content coming from direct peering and from transit, Australian consumers would not have had the benefit of streaming such a radio service without using their data allowance.

Insufficient market competition may remove the incentive for major transit providers with a large base of end users to enter into peering relationships. .They may believe that content providers such as radio stations should enter into a paid peering and transit

relationship with them in order to reach both their own customers and those of other ISPs. A company in this position would tend not to zero-rate the services of content providers, aside from those offered by its own network. Precluding zero-rating would therefore favour such a dominant player because both their competitor ISPs and the content provider would not be able to offer an unmetered service.

In markets with large bit caps or unmetered service, such as fixed Internet access in most OECD countries, the issue of zero-rating is not overly emphasized. In mobile networks where relatively low bit caps are common, the practice is much more prevalent than for fixed networks. The incentives may also be different from fixed networks where there are generally many more ISPs, particularly in markets with unbundled local loops.

An additional form of zero-rating occurs in developing countries where the practice is increasing. Popular Internet services, such as Facebook, WhatsApp, Twitter, Wikipedia and Google, have been partnering with telecommunication operators to offer zero-rated access to these services. However, it should be noted that these products do not provide access to the Internet, but only to a limited number of sites. The goal is to use a limited number of sites as a teaser to encourage wider Internet use among consumers. This approach can also help achieve social objectives by including unmetered access to sites such as Wikipedia or health and government information. In some cases the practice of zero-rating certain services explains why users report not using the Internet, while confirming that they access Facebook or Wikipedia.

The rapid take up of such offers in developing countries is undoubtedly due to several factors. The first is that some of these countries have extremely competitive mobile markets with up to six national MNOs. A second factor is that consumers in these markets are both very conscious of costs and, in many cases, have not previously experienced Internet access due to low fixed network penetration. In such cases, it is in both the ISP's and content provider's interest to stimulate usage, which may have economic and social spill-over effects for development as a whole.

While zero-rating can clearly be pro-competitive and may have beneficial aspects for economic and social development, regulators need to be vigilant. Previous experience in OECD countries has shown that zero-rating becomes less of an issue with increased competition and higher or unlimited data allowances. Indeed, it can be a tool to increase competition. Prohibiting zero-rating may have implications for a market where there is lower competition for transit and may reduce the effectiveness of peering. Nevertheless, in any market with limited competition for access, zero-rating could be an issue of concern. For example, a situation where a dominant content provider is zero-rated and its competitors are not (and the provider's position enables them to opt for paid-peering rather than peering) may impede new or innovative firms from entering the market. Likewise, a situation where an ISP offers a high-volume service while setting a low data cap could also stifle competition.

Zero-rating needs to be considered on a case-by-case or market-by-market basis. While there is potential to enhance and increase competition in certain instances, there is also a risk of abuse of dominant positions. An important safeguard in this regard is transparency. Some zero-rated websites, for example, do not charge users for content, but do count data downloaded as advertising – something that may not be obvious to a user. Moreover, while most consumers can readily understand zero-rating as an additional service to their

bundle, tariff schemes that offer unlimited access for a bundle of services, and charge for metered access beyond that bundle, may be complex. This is where competition can play a key role. Open markets will deliver competitively priced plans with access to the full Internet – the reason for today's mobile broadband boom – rather than a handful of popular Internet services that could effectively become a walled garden.

4.4 Advanced fixed networks and regulatory issues

Fixed network upgrading: Fibre, VDSL, vectoring and DOCSIS

Between 2012 and 2014, there was a substantial increase in the use of fibre-to-the-home (FTTH) broadband in a number of OECD countries. As of December 2013, Japan and Korea continue to lead with over 60% of broadband subscriptions using this technology. Growth in FTTH use is also increasing in other countries. In Spain, Turkey and the United Kingdom fibre penetration still remains below the OECD average of 16.6 fibre subscriptions per 100 fixed broadband subscriptions (respectively 5.2, 14.3 and 10.4), but has increased by more than 80% year-on-year. In Ireland, Eircom announced an FTTH service in October 2014 to connect 65 towns at speeds of up to 1 Gbit/s. The service will compete with the joint venture of Vodafone/ESB, which was cleared by the European Commission and involved USD 563 million in public funding to deliver fast broadband service to 50 towns, or 500 000 premises, over ESB's electricity network, providing access to third parties under open access.

Despite increasing coverage of FTTH networks, most broadband subscribers still rely on copper and coaxial cable. A fundamental question is how to maximise the utility of existing copper or coaxial cable networks until they are fully replaced by fibre. Regulatory and policy decisions in this area will have a significant impact on the evolution of competition and the transition towards a fibre-only environment. Deployment costs for FTTH are significant and a myriad of competing technologies such as fibre-to-the-node (FTTN) and hybrid fibre coaxial (HFC) offer broadband performance close to FTTH, provided that local loops are short enough. However, some of these technologies may pose challenges to competition remedies such as local loop unbundling, rendering the situation slightly more complex than pure cost-benefit analysis from the firm's perspective. For example, some technologies such as VDSL2 require technical adjustments to networks that render traditional remedies for third-party access (e.g. sub-loop unbundling) unfeasible or uneconomical. In such cases, regulators should carefully assess whether some of these technologies or their implementation and topologies, may result in foreclosure of the market to competitors.

Regardless of whether FTTH technology prevails in the coming years, FTTN technologies such as VDSL2 vectoring or G.fast may continue to coexist for some time. VDSL2 can provide up to 80-100 Mbps download speeds in short loops (400-800 metres), and may reduce investment needs over the short term from USD 1 500 down to USD 500 per subscriber, for a given scenario (WIK, 2014). In order to improve performance and increase download speeds, vectoring technology estimates the cross-talk effect of neighbouring copper pairs and subtracts in real time the estimated cross-talk signal of those pairs from the original signal. Unfortunately, vectoring, at least in its first generation version, can raise competition concerns, as it does not produce the desired results if more than one operator is present at the cabinet. Its use restricts or makes impractical the unbundling of sub-loops and requires that the same provider manage all sub-loops in a copper bundle.

These concerns may be alleviated in countries where sub-loop unbundling is not demanded (BEREC, 2014). More generally, the availability of wholesale products in FTTN networks is highly dependent on topology (e.g. point-to-point vs. point-to-multipoint). More recently, some regulators have approved virtual wholesale products that replicate the characteristics of physical remedies, such as Local Loop Unbundling (LLU). For example, Virtual Unbundled Local Access (VULA) is an active remedy that allows for substantial control of the characteristics of virtual connections, and could possibly replace LLU unbundling for fibre networks until fibre unbundling becomes available.

At least four European countries (Austria, Belgium, Denmark and Germany) have issued regulatory decisions that allow the incumbent operator to deploy vectoring, provided that certain conditions are in place to compensate for the loss of the sub-loop unbundling (SLU) as an unbundling remedy. Sub-loop unbundling is used in some countries for FTTN networks, and provides access to a partial local loop to alternative operators.[9] For example, Bundesnetzagentur, the regulatory authority in Germany, has allowed operators to deploy vectoring and refuse access to third parties in certain cabinets on a first-come, first-served basis, provided they offer access through virtual products equivalent to physical unbundling, and commit to implement vectoring within a year.

Cable broadband providers are keeping pace with technological developments, especially with regard to rising broadband speeds, in many cases offering superior products to those of DSL providers. Some DOCSIS 3.0 solutions offer broadband speeds comparable to those of FTTH providers. In the United States, Comcast offers 505/100 Mbps download/upload speeds in line with many FTTH operators. In the United Kingdom, leading cable providers such as Comcast or Virgin Media are testing DOCSIS 3.1, whose specifications were released by CableLabs at the end of 2013.[10] DOCSIS 3.1 may have the potential to deliver up to 10 Gbps in download speed.

Public initiatives to extend network coverage and speeds

The increasing use of mobile broadband for data services is encouraging further integration between fixed and mobile networks. Third-generation mobile networks and, in particular, LTE technology require mobile network upgrades with base stations connected to the operator's core network by fibre. In fact, bottlenecks that prevent support for a larger number of mobile broadband users for a given station may be located in the fixed backhaul network. As LTE coverage increases, operators are also investing in backhaul networks that feed LTE radio stations.

For the most part, backhaul markets between the largest cities in OECD countries are highly competitive. A high number of connectivity providers exert sufficient competition to ensure prices keep declining based on technological advances. Rural areas, however, are still a challenge in many OECD countries.

Developing countries may face significant challenges in extending backhaul broadband connectivity to areas outside the major cities. Key examples include countries with remote regions or challenging terrain conditions, such as the Amazon Basin in Brazil, Colombia, Ecuador and Peru, among other countries. In 2011 in Colombia, for example, the National Fibre Network tender was won by the Mexican joint venture Total Play/TV Azteca, with the aim of connecting 753 municipalities to backhaul fibre, with a total investment of USD 640 million (a third of which was provided by the government). TV Azteca was also awarded Peru's National Fibre Network, which will connect 180 of the

195 provincial capitals in that country. A second phase envisages reaching some 1 850 districts. In countries like Nicaragua and Peru, where river transport is prominent, fibre optic cables are being deployed along rivers to connect communities along those basins. The governments of Colombia, Ecuador and Peru are funding fibre networks, focusing on backhaul and backbone connectivity, which will allow ISPs to reach customers more easily and at lower rates, as they can access these networks at regulated prices. In other countries, publicly funded broadband infrastructure projects target different types of networks. In some cases, microwave links are used as backhaul infrastructure where fixed networks are deficient.

In Mexico, the Constitutional Reform adopted in 2013 included a national wholesale mobile network in the 700 MHz band which, together with fixed infrastructure owned by the Federal Electricity Utility (*Comisión Federal de Electricidad*), would allow independent providers to avoid existing bottlenecks, namely excessive backhaul and backbone connectivity prices set by the incumbent. Mexico's approach will devote the full digital dividend band (90 MHz in the 700 MHz band) to the national wholesale wireless network. This approach has not yet been explored in the OECD area, but Rwanda's LTE network is already being deployed through partnership between the government and operators in that country and Kenya plans to do so by 2015.[11] Mexico's network, which plans to launch by 2018, still needs to be tendered and will likely take the form of a public-private partnership (PPP). The Mexican Congress will also establish whether the 700 MHz band is exempted from paying spectrum fees. More critically, its success will depend on whether wholesale rates, which will be regulated in addition to quality and coverage conditions, are low enough to attract service providers including existing operators to use this network.

In Northern Europe, fibre networks are taking off largely due to municipal utilities leveraging their customer base to provide broadband services through fibre technology. Municipalities in other countries, such as Greece, Italy or the United States, have also launched similar initiatives, although those introduced in the Nordic countries, especially Sweden, have had the largest effect in terms of population covered. Large amounts of public money have translated into alternative networks, provided mainly through city urban networks. Swedish municipal networks have three main common points: (i) public ownership, (ii) limited geographical presence and, (iii) focus on fibre. According to one study, these networks have provided consumers with greater choice and thus reduced their dependence on incumbent operators (Sandgren and Molleryd, 2013).

In April 2009, the Australian government created NBN Co. to deploy a nationwide fibre broadband network, in partnership with the private sector. The aim was to connect over 90% of all Australian homes, schools and workplaces with speeds up to 100 Mbps using fibre-to-the-premises technology. At a later stage, the project included the purchase of the historical incumbent's copper assets. In 2014, the Australian government conducted a cost-benefit analysis to assess whether a technology mix of fibre-to-the-premises (FTTP) and FTTN would provide a better outcome, in addition to the use of fixed wireless and satellite technology for rural and remote areas in the country. Following the recommendations of this analysis, the Australian government is prioritising FTTN over FTTP technology, on the basis that it would save USD 16 billion and shorten deployment periods (Australian Government, 2014). In New Zealand, the government launched the Ultra-Fast Broadband initiative to expand and develop broadband services. The project aims to connect 75% of New Zealanders to ultra-fast broadband by 2020, and schools, hospitals and 90% of

businesses by 2015. The initiative will enable download speeds of up to 100 Mbit/s and upload speeds up to 50 Mbit/s. The government is contributing USD 1.05 billion (NZD 1.35 billion) to the programme.

In the European Union, the Digital Agenda for Europe set three main connectivity targets in terms of download speeds: *(i)* universal basic broadband for all Europeans by 2013; *(ii)* universal broadband at speeds of at least 30 Mbps by 2020; and *(iii)* 50% or more European households subscribing to Internet access above 100 Mbps. The European Union has fostered adoption of national broadband plans aimed at achieving these goals and member countries are working toward meeting the targets through a full range of measures, such as initiatives to reduce deployment costs and facilitate rollouts, public funding of broadband networks and so forth.

Other countries have also set targets in terms of very high-speed broadband connectivity (e.g. 100 Mbps or more). Iceland aims to provide 70% of households and workplaces with 100 Mbps broadband coverage by 2014 and 99% by 2022. In the United States, the 2010 National Broadband Plan aims to reach 100 million households with 100 Mbps/50 Mbps broadband coverage by 2020. The Plan's Action Agenda lists more than 60 key actions, proceedings and initiatives to implement its recommendations. These include "Connecting Rural America" (through a comprehensive reform of the Universal Service Fund), "Connecting Low Income Americans" and "Connecting Native American Communities", including the promotion of greater use of spectrum by these communities.

Initiatives to extend access to rural and remote areas, whether under a single initiative or through different programmes, are underway in most OECD and non-OECD countries, with different variations and goals depending on the initial situation in each country. In October 2014, the Indonesian government launched the "Indonesia Broadband Plan", which aims to provide fixed broadband access to all government offices, hotels, hospital, schools and public spaces by 2019 with speeds of at least 2 Mbit/s. A comprehensive list of broadband plans and targets in OECD countries is included in tables available online.[12]

International cables and gateways

International connectivity plays a major role in connecting businesses, citizens and governments to the Internet. Bottlenecks in international connectivity pose a serious threat to the expansion of Internet access, especially in developing countries (OECD, 2014c). Substantial progress has been made in recent years including new international undersea cables circling Africa, while in Latin America a number of announcements have been made regarding planned improvements to regional and international connectivity. Challenges in international bandwidth are being addressed by policy makers, in partnership with companies that have identified business opportunities in countries where large parts of their population are not yet online. An example of these developments is the expected growth in mobile communication infrastructure in Africa. In November 2014, the Nigerian phone tower group IHS announced that it had raised USD 2.6 billion in equity and debt to finance infrastructure spending. The mobile tower business in Africa is expected to grow significantly as pent-up demand for mobile broadband starts to be met.

An example of such partnership is the recent announcement by Google and telecommunication operators in Brazil (Algar Telecom), Uruguay (ANTEL) and Angola (Angola Cables) of a USD 400 million investment in a new submarine cable between Brazil and the United States. Telebras, a state-owned Brazilian operator is also investing USD 185 million in deployment of a new cable between Brazil and Portugal. The new cable is

one of several being deployed in the region to address international connectivity issues that have long hindered efforts to expand Internet access and reduce broadband connectivity prices. Telmex/AMX have also invested in a new cable linking Cancún in Mexico to the United States and other countries in the region, including Brazil, the Dominican Republic and Guatemala. In 2011, the Union of South American Nations (UNASUR) proposed the deployment of a South American fibre ring, which would link existing national fibre networks through agreed gateways. Some countries have held bilateral discussion to advance these initiatives, however the project is far from completion.

Notwithstanding broad commitments to expand connectivity and reduce prices, some countries are still applying policies that restrict connectivity, increase prices and reduce options for consumers. This is the case of certain Asian and African countries, such as Ghana or Pakistan. In Pakistan, for example, the government set up a cartel to set prices for incoming international calls, raising rates from USD 0.02 to USD 0.088. As result, traffic fell from over 2 billion minutes to 500 million. This in turn generated no increase in revenue, but rather resulted in a huge loss in consumer welfare. These policies contrast with those of other developing countries, such as India, where dramatic cuts in international termination rates, together with strong domestic competition, have seen traffic increase dramatically (Figure 4.4).

Policy developments in IPv6

The Internet Protocol (IP) defines the address space for the Internet. The number of addresses defined by Internet Protocol version 4 (IPv4), the version of IP used since commercialisation of the Internet began, is currently running out. A successor to IPv4 known as IPv6 has been available since 1998. However, diffusion of this new protocol has been slow, although it has increased markedly in the last two years. Data from APNIC show an increase in the IPv6 global user penetration ratio from around 0.71% in mid-2012 to 2.53% at the end of October 2014.

Governments and non-governmental institutions in the technical community, such as the Internet Society, have sought to facilitate the transition to IPv6 by diffusing best practices for implementing IPv6, and publishing information on IPv6 deployments. These efforts are valuable as they help inform adopters about the potential costs and benefits of adoption, although the availability of certain types of data to inform decision-makers could be improved. Successful efforts to coordinate the behaviours of large ISPs and content providers have included the publication of data on IPv6 penetration through sources such as World IPv6 Launch. While adoption remains very low, these policies have demonstrated some success at influencing the behaviour of lead users. One open question is the extent to which policies will be effective at encouraging adoption among other users on the IPv6 platform.

In 2012, the Belgian government launched a national plan for the introduction of IPv6. Among the initiatives included in the plan, the federal government requested federal, regional and local governments and universities to make their websites, online services and government networks and services accessible in both IPv4 and IPv6. The plan also included IPv6-related conditions for public procurement and requested ICT firms to include IPv6 in their development plans. As of October 2014, Belgium is the OECD leader in IPv6 adoption. Other OECD countries, such as Canada, Czech Republic, France, Korea, Sweden and the United States have adopted national initiatives to promote the deployment and adoption of IPv6 services.

Figure 4.4. **Average termination charges for outgoing traffic, United States to regions (top), outgoing minutes from United States carriers to regions (bottom)**

Source: Based on OECD (2014d).

StatLink http://dx.doi.org/10.1787/888933225177

4.5 Wireless developments

Radiofrequency spectrum remains one of the key inputs to the digital economy. Any wireless interaction has to be transmitted through electromagnetic waves, which whether using exclusive or shared resources need to transmit signals with a sufficiently low error rate to enable communication.

Numbering and M2M issues

Machine-to-machine (M2M) communications represent a turning point in the scale of the Internet, with billions of devices potentially connected in the coming years. Chapter 6 of this report covers M2M in depth, but the main policy implications of M2M communications can be highlighted here. In particular, numbering resource management is critical to enabling developments in this area. In some cases numbers are a scarce resource, as a result of the design of numbering plans, and need to be used efficiently. Traditionally,

numbering resources have been assigned to telecommunication operators, which in turn assigned them to end users of communication services. As liberalisation advanced in most OECD countries, new mechanisms, such as number portability, had to be found to accommodate number management to the new competitive situation. With the advent of M2M communications and the clear benefits arising from companies (e.g. automobile manufacturers, GPS device makers) managing their own numbering resources, new paradigms need to be found to improve flexibility.

Machine-to-machine communication is predicted to become one of the main sources of growth and innovation in the digital economy in the coming decade (see Chapter 6). In 2014, the Netherlands became the first country to reform numbering regulations to enable private networks to have access to mobile number or international mobile subscription identity (IMSI) ranges.[13] The main advantage of this regulatory setting is that allows businesses, especially large users of mobile services, greater flexibility in choosing how to offer M2M services across borders. This is a significant development for consideration by policy makers in all countries, with a view to ensuring the competitiveness of the mobile communication sector and its ability to meet rapidly evolving market demand. In a similar vein, Germany has launched a public consultation on the use of numbers/IMSI identifiers (Bundesnetzagentur, 2014). In most countries, companies would need to become an MVNO to be assigned numbers. Relaxing this requirement and allowing firms to be assigned IMSIs and numbers would render the market more flexible and allow switching between operators (as is the case with MVNOs do). At present, this is not practical for economic reasons, as thousands or millions of devices would need to be recalled to implement such a change.

Spectrum resources: Towards an efficient assignment framework

The remarkable growth in smartphones and tablet devices has led many governments and spectrum agencies to allocate new spectrum bands to mobile communication uses. The International Telecommunication Union's (ITU) World Radio communications Conference will take place in Geneva in November 2015 (WRC 2015). Spectrum issues are already being examined in preparatory meetings leading up to this conference. Previous WRC decisions facilitated the reallocation of the "digital dividend" band (700 MHz or 800 MHz, depending on the region). The ITU has developed a methodology to estimate the spectrum needs of countries, which takes into account technological evolution and communication uptake.

Most countries have engaged in important efforts to increase the amount of spectrum resources devoted to communications, as can be witnessed from the release of the digital dividend and other initiatives. These issues are priorities for decision makers in many countries. In 2010, for example, the President of the United States issued a Presidential Memorandum entitled "Unleashing the Wireless Broadband Revolution" requiring the Federal Government to make available 500 MHz of federal or non-federal spectrum for both mobile and fixed wireless broadband commercial use within a decade (United States White House, 2010).

A comprehensive approach to this task includes the production of spectrum inventories, outlooks and roadmaps. Spectrum inventories document every band, including its current use and occupation, while spectrum outlooks and roadmaps specify the needs of a given country and region. There are a broad range of circumstances to consider, such as possible harmful interference, current uses of spectrum such as civil

or defence use, and so forth. An example of spectrum outlook is Australia's "Five-Year Spectrum Outlook", released in September 2014, which sets out the regulator's (Australian Communication Markets Authority) strategy in response to spectrum demands, and decides on the work programme for the 2014-18 period (ACMA, 2014). The European Union's Radio Spectrum Policy Programme (RSPP) also placed significant emphasis on spectrum inventories and the basis for decision making in spectrum policy (European Parliament and European Council, 2012), provided that administrative burden, policy priorities and current uses of spectrum are also considered. Canada has also produced a "Commercial Mobile Spectrum Outlook", similar to Australia's, released in March 2013 and covering the period to the end of 2017.

Licensed spectrum

The traditional procedure for making spectrum available is through exclusive licences. More recently, unlicensed or license-exempt use of spectrum has proven a remarkable source of innovation and is used to complement exclusive licences in other bands. Wi-Fi and RFID technologies demonstrate that unlicensed spectrum allocation, in conjunction with low-emission devices and intensive spatial spectrum reutilisation, can greatly empower consumers and businesses and fulfil their wireless connectivity requirements.

An increasing number of OECD countries are considering the possibility of extending unlicensed/license exempt use to other spectrum bands. For example, France is currently consulting on other bands beyond the current 2.4 GHz and 5 GHz (5 150 to 5 350 MHz and 5 470 to 5 725 MHz). In particular, ongoing discussion relates to the use of additional segments of the 5 GHz band, taking into account the necessary protection of current users of the band (i.e. meteorological radars, satellite for earth observation, intelligent transport systems) (ARCEP, 2014). An eventual decision on this issue would need to be harmonised at the European level, including technical work by the European Conference of Posts and Telecommunication (CEPT). In Korea, the government plans to make more unlicensed spectrum available, including for inter-vehicle communications.

A relatively innovative and still nascent way of increasing efficiency in spectrum use is licensed shared access (LSA). This enables spectrum sharing by two or more entities in a given area or time interval for a particular band, and also includes licensing requirements for those potentially capable of using the incumbent's band (OECD, 2014e). In 2011, an industry consortium put forward a proposal to share spectrum based on licensed or authorised shared access. Existing spectrum users (the incumbent) would share spectrum with one or several licensed LSA users (licensees), in accordance with a set of conditions, which can be static (time allowed or exclusion zones) or dynamic. Dynamic use could utilise recent advances in dynamic spectrum techniques. Under LSA, the new users are authorised to use the spectrum in accordance with sharing rules included in their rights of use (license), while ensuring use by the long-term incumbent.

More recently, the FCC has put forward a notice for proposed rulemaking (NRPM) to adopt a licensed shared access approach in the 3.5 GHz band ("the Citizens Broadband Radio Service"). In Europe, the CEPT and the Radio Spectrum Policy Group (RSPG) have adopted LSA to foster spectrum sharing for IMT and other bands, in a harmonised manner (RSPG, 2013).[14] The first band where LSA could be implemented is 2.3-2.4 GHz, where it would enable shared use by the incumbent (the military) and new users (telecommunication operators).

Many OECD countries are looking actively at possibilities to increase efficiency in spectrum use under these types of frameworks. OFCOM, the regulator in the United Kingdom, issued a statement in April 2014 listing the areas where increased sharing, whether licensed or unlicensed, could be of most interest: *(i)* for indoor use, *(ii)* for outdoor use (e.g. through small mobile broadband cells), and *(iii)* for the Internet of Things (OFCOM, 2014). In France, the Minister of SMEs, Innovation and the Digital Economy requested that work be undertaken on dynamic spectrum management to promote innovation and growth (Toledano, 2014). A commissioned report put forward recommendations to implement a more flexible management of spectrum. The recommendations take into account key policy, economic, social and cultural goals to be met through increased availability of spectrum resources, and increased efficiency to be achieved largely through dynamic spectrum use. The recommendations are: *(i)* make available more unlicensed spectrum in the 900 MHz band or in the 5 GHz band, and *(ii)* facilitate the introduction of dynamic spectrum access techniques, such as a technical trial in the 2 300-2 400 MHz band or through a one-stop shop (at the National Spectrum Agency, the Agence National des Fréquences) for innovative projects exploiting television white space opportunities. The report also proposes the elaboration of a governmental strategy for spectrum issues, in cooperation with the private sector.

Television white space devices and femtocells

Trials on the use of television white space devices (TWSD) are being undertaken by a number of regulators in OECD countries. The licensing schemes for TWSDs can be considered less demanding than LSA, even though they have to abide by the requirement of registering in a database. The approach departs from the proposed LSA model in that it does not always oblige users of white spaces to register while operating in the band, although they do need to provide some information to the databases.

In March 2013, the FCC's Office of Engineering and Technology (OET) authorised television white space database systems to provide service to unlicensed radio devices that operate in these spectrum bands. The rules require TWSD to obtain a list of channels available for its operation. In the United Kingdom, OFCOM has tested this technology under various scenarios. Examples of these uses include joint work with Google and ZSL London Zoo, to use TWSD to stream live footage of animals on YouTube, as well as Internet connectivity for ships and boats around the Orkney Islands.[15] The potential use of white space to improve rural broadband availability is one of the areas under investigation. In October 2012, Canada released a framework for the use of television white spaces and is in the process of developing detailed technical rules that will allow implementation to proceed.[16]

Femtocells are low-power base stations that enable private GSM/3G/4G networks to achieve indoor and outdoor coverage. They provide additional coverage for a limited area, typically up to 50-100 metres, with a view to compensating for faulty macro network coverage. In the Netherlands, 5 MHz of spectrum in the 1 800 MHz band has been opened for low-power use by femtocell base stations, without licensing requirements. This was preceded by smaller scale testing, which proved extremely successful with over 3 000 organisations registering and deploying their own base stations.

Other countries, such as Brazil and Japan, have followed suit, although they have only allowed operators to register femtocells. In the case of Brazil, the regulator argued that allowing third-party users to use femtocells would increase the likelihood of harmful

interference. Nonetheless, the approach in the Netherlands may lead to more competition in the provision of devices, which can be expensive when tied to a specific operator that has, in effect, a monopoly. By way of example, in many rural regions of the OECD, there may be only a single network with coverage. If an operator has a monopoly over the provision of a femtocell there is no competitive discipline on the price it can charge, even though the consumer is contributing to network expansion to substitute for insufficient coverage. In such sparsely populated regions, without adequate wireless service, this raises the question of what type of service a femtocell may interfere with in practice, bearing in mind that the Netherlands has one of the highest population densities in the OECD area.

Spectrum auction developments

The question of how to distribute spectrum resources among market players remains a critical issue and one that has far-reaching implications. Between 2012 and 2014, most countries that have assigned spectrum have followed an auction procedure, subject to some conditions (e.g. coverage obligations, spectrum caps). An alternative procedure is comparative selection processes, sometimes called "beauty-contests", which take into account a set of criteria to allocate spectrum rather than allowing the market to set a price.

Austria, Belgium, Canada, Chile, Korea, Finland, Hungary, New Zealand, Slovak Republic, Slovenia and the United Kingdom conducted spectrum tenders in 2013-14, all using spectrum auctions, with the exception of Chile (where coverage obligations and investment commitments were used as criteria) and Estonia (where a prior beauty contest preceded the auction). Most auctions involve the "digital dividend" band (800 MHz band in Europe or 700 MHz in Regions 2 and 3) and the 2.5/2.6 GHz band, traditionally used to deploy LTE networks. These two bands can largely be seen as complementary, in that the 900 MHz/800 MHz bands provide good indoor coverage and carry signals over long distances, whereas higher frequency bands enable high download speeds over shorter distances.

It is noteworthy that spectrum agencies in the OECD area are devoting considerable attention to two outstanding policy challenges in their countries with regard to spectrum assignment procedures. The first is extending coverage at a reasonable pace while including, to the extent possible, rural areas. The second is providing a level playing field for competition through a balanced spectrum assignment. This can be achieved by balancing lower and higher bands and overall spectrum holdings while, in some cases, facilitating entry (see Table 4.3). As noted above, ongoing consolidation processes occurring in countries such as Austria (Hutchinson/Orange), Germany (Telefónica/EPlus) and Ireland (O2/Hutchinson) have resulted in the European Commission imposing conditions on spectrum holdings of the merging parties as a requirement to authorise the merger.

Table 4.3. **Examples of regulatory tools used to promote competition in spectrum auctions**

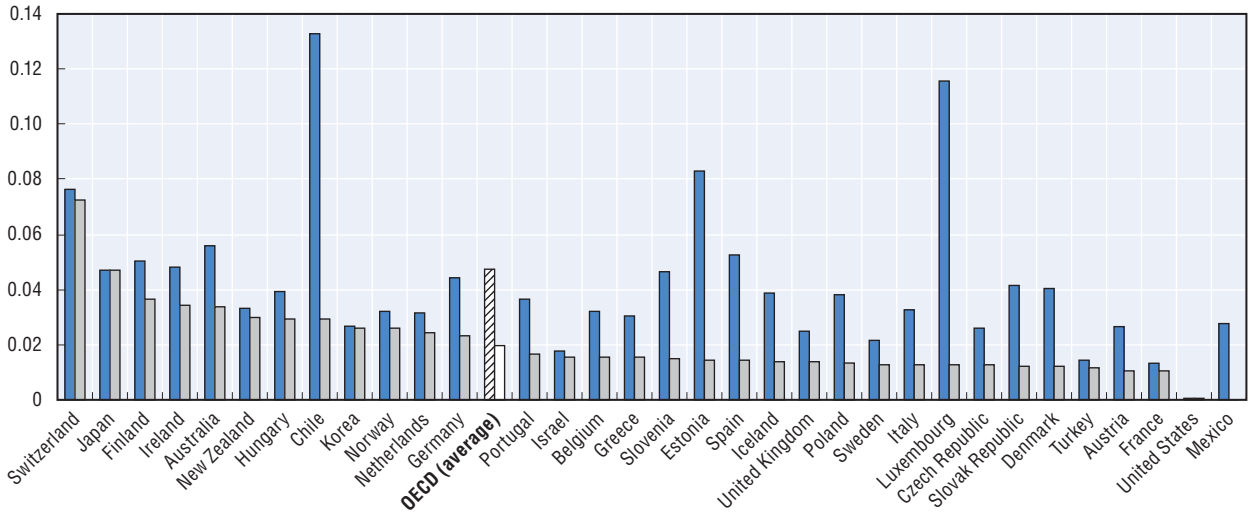
Tool	Countries
Spectrum caps	All
Spectrum caps for different bands	Canada, Czech Republic, Norway, Portugal, Slovenia
Set asides/discounts	Canada, Korea, Netherlands, Slovenia, United States
National roaming	Austria, Czech Republic,
Provision on MVNOs	France, Portugal

Decreasing mobile termination rates

In addition to ongoing policy debate over the number of wireless carriers and the implications for competition and innovation, mobile markets have generally benefitted from decreasing termination rates. From the middle of the last decade onwards and, in particular, following the Recommendation on Termination Rates issued by the European Commission, fixed and mobile termination rates reduced steadily in OECD countries.

Reduced termination rates generally lead to revenue and cost reductions for operators. In other words, a reduction from high to lower termination rates can be relatively neutral in terms of the bottom line for many operators, because although it reduces gross revenue it also reduces costs and may not have any significant effect on net revenue. That being said, revenues have fallen in some countries where high prices were adjusted in the face of increased competition and changing business models together with consumer preferences (e.g. lower prices for voice or SMS services with a shift to more use of data and over-the-top services). In October 2014, the average mobile termination rate (MTR) in the OECD area was USD 0.0197, representing a 51% decline from USD 0.0402 in October 2012 (see Figure 4.5 and 4.6). Amid the overall declining trend in MTRs, some OECD countries, such as Chile, Estonia or Luxembourg, have experienced dramatic reductions. In Mexico, following the adoption of the new Federal Law for Telecommunications and Broadcasting in August 2014, the MTR on the largest MNO (see Figure 4.5) was set at zero, while MTRs are still paid for calls terminating on other networks.

Figure 4.5. **MTRs in OECD countries, USD**

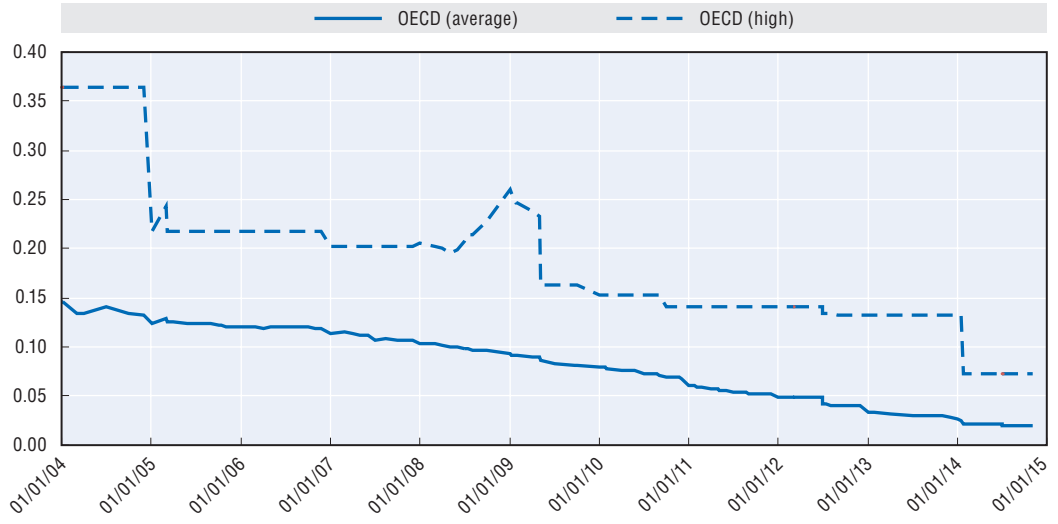


Note: The blue blocks indicate mobile termination rates (MTRs) for 28 October 2012, the grey blocks indicate MTRs for 5 November 2014.

StatLink http://dx.doi.org/10.1787/888933225188

In the past, these competition dynamics were limited by a de facto floor for retail prices (i.e. the mobile termination fee). In some cases, decreases in traditional revenue for voice and SMS have been offset by increased revenue from mobile broadband services. This is one reason why the industry has shifted its focus to superior technologies such as LTE, in search of additional revenue sources. Moreover, declining equipment prices may also have enabled price reductions driven by technology, with the benefits passed on to consumers in competitive markets.

Figure 4.6. **Average and maximum MTR in OECD countries, USD**



StatLink http://dx.doi.org/10.1787/888933225193

International mobile roaming

Since the OECD Council Recommendation on International Mobile Roaming Services in 2012, there has been a marked reduction in international roaming prices and a range of new service offers, in particular for mobile data roaming. Mobile network operators (MNOs) have thus aimed to respond to the demands of roaming customers. Mobile subscribers, to a large extent, have become more aware of high roaming prices and are more cautious when roaming, adjusting their consumption to limit expenditures and increasingly following procedures to limit mobile data consumption.

Despite the reduction in prices, roaming prices in many countries are still far from competitive. In many regions, the price reductions are viewed as insufficient, reinforced by the fact that domestic mobile (and fixed) telecommunication prices have fallen considerably in competitive markets. In several countries, a number of mobile network operators are offering domestic monthly packages, which include unlimited calls to fixed and mobile phones, unlimited SMS and generous mobile data packages. These price reductions in national mobile markets have led to considerable changes in consumption patterns for mobile phone services, which have not been replicated for roaming services.

Since 2013, initial offers from MNOs that include international mobile roaming as an integral part of their bundles have been made almost entirely in OECD countries with four or more operators (Denmark, France, Israel, Japan, Luxembourg, Sweden, United Kingdom, United States). Such offers have generally not yet emerged in countries with three operators. An exception is Portugal where one MNO offers roaming as an integrated part of a premium offer, with other offers subject to additional roaming charges. One country where cross-border investment has led to lower international mobile roaming charges is Japan, where Softbank recently introduced a roaming plan for the United States providing unlimited calling and data within the United States, but limited to customers using the iPhone 6 who have a domestic subscription providing flat rate calling and data. The offer was made available on Sprint, an MNO in the United States for which Softbank is the largest shareholder.

A significant commercial development with the potential to change the dynamics of the international mobile market was the introduction in October 2014 of a new range of iPads by Apple. These include a feature entitled "Apple SIM". This feature enables consumers to select the mobile network they prefer to use for data from the menu settings on their device. In other words, rather than inserting a SIM card provided by an MNO or MVNO, Apple's device comes with a reprogrammable SIM that can be used on unlocked iPads to select a carrier of their choice, together with the plans offered by the participating carriers. This approach, together with over-the-air IMSI delivery or a large pool of pre-installed IMSIs, introduces the flexibility to switch between mobile providers. If countries adopt this approach, it will make M2M services more dynamic and allow users with potentially billions of SIM cards, to switch mobile providers more easily.

Notes

1. For a detailed explanation of the UPP method, refer to the OECD Roundtable on Market Definition (2012). *www.oecd.org/daf/competition/Marketdefinition2012.pdf*.
2. FCC's 16th Annual CMRS Competition Report (page 39), *https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-34A1.pdf*.
3. The internal market is one of the pillars of the European Union. Completed in 1992, the single market is an area without internal frontiers in which persons, goods, services and capital can move freely, in accordance with the Treaty establishing the European Community. The internal market is essential for prosperity, growth and employment in the EU, contributing to the achievement of its objectives under the Lisbon strategy. As an integrated, open and competitive area, it in fact promotes mobility, competitiveness and innovation, interacting in particular with the EU sectoral policies. To ensure that everyone, citizen or business, can make the most of the advantages of the single market, the EU concentrates on dismantling barriers still impeding its operation. It seeks to harmonise legislation in order to improve its response to the challenges of globalisation and to adapt to advances, such as the new technologies. *http://europa.eu/legislation_summaries/internal_market/internal_market_general_framework/index_en.htm*
4. For example, the mergers of Newscorp/Telepiù (2003) in Italy, CanalPlus/TPS in France (2006).
5. *http://ec.europa.eu/public_opinion/archives/ebs/ebs_414_sum_en.pdf*. A bundle is a combined package offering more than one communication service from the same provider at an overall price. The sale of a smartphone device, with significant upfront discount, together with a mobile communication plan referred to in paragraph 69 is not included in this definition.
6. COM/2013/627/FINAL
7. TiVo is an advanced Digital Video Recorder (DVR), *www.tivo.com/*
8. For example, see the FCC's 2014 Open Internet Notice of Proposed Rule Making: *www.fcc.gov/document/protecting-and-promoting-open-internet-nprm*.
9. Sub Loop Unbundling (SLU) provides you with access to a partial local loop. It connects the network termination point at your customer's premises to a concentration point or a specified intermediate access point in the local network. We're responsible for the provision, maintenance and repair of the SLU circuit, which comes with Shared Metallic Path facility (SLU SMPF) and Metallic Path facility (SLU MPF) options. *www.openreach.co.uk/orpg/home/products/llu/subloopunbundling/subloopunbundling.do*.
10. See *www.lightreading.com/cable-video/docsis/docsis-31-whats-next/d/d-id/708425*, *www.ispreview.co.uk/index.php/2014/07/virgin-media-uk-lab-testing-10gbps-docsis-3-1-broadband-upgrade.html*.
11. See *www.bmi-t.co.za/content/open-access-wholesale-mobile-networks-not-necessarily-panacea*.
12. See Table 4.10. Broadband goals and funding, available online at *www.oecd.org/sti/DEO-tables-2015.htm*.
13. ITU-T Rec. E.212 (05/2008): 3.2 international mobile subscription identity (IMSI): The IMSI is a string of decimal digits, up to a maximum length of 15 digits, which identifies a unique subscription. The IMSI consists of three fields: the mobile country code (MCC), the mobile network code (MNC), and the mobile subscription identification number (MSIN). *www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.212-200805-I!!PDF-E&type=items*.

14. According to the RSPG definition, LSA is as "a regulatory approach aiming to facilitate the introduction of radio communication systems operated by a limited number of licensees under an individual licensing regime in a frequency band already assigned or expected to be assigned to one or more incumbent users. Under the LSA approach, the additional users are authorised to use the spectrum (or part of the spectrum) in accordance with sharing rules included in their rights of use of spectrum, thereby allowing all the authorised users, including incumbents, to provide a certain Quality of Service (QoS)", (RSPG, 2013).

15. *http://media.ofcom.org.uk/news/2014/white-spaces-trials-oct14/*.

16. Framework for the Use of Certain Non-broadcasting Applications in the Television Broadcasting Bands Below 698 MHz" see *www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10493.html*.

References

ACMA (2014), *Five-year Spectrum Outlook 2014–18: The ACMA's Spectrum Demand Analysis and Strategic Direction for the Next Five Years*, Australian Communications Markets Authority, Canberra, *www.acma.gov.au/~/media/Spectrum%20Outlook%20and%20Review/Report/FYSO%202014%20-%202018/ACMA_FYSO%202014-18%20pdf.pdf*.

ARCEP (2014), *Utilisation de fréquences sur des 'bandes libres' et projet de décision de l'ARCEP relatif aux dispositifs à courte portée: Consultation publique du 25 juillet au 15 octobre 2014* (*The use of frequencies on 'free bands' and draft decision of ARCEP on short-range devices: Public consultation from 25 July to 15 October 2014*), July 2014, Autorité de Régulation des Communications Électroniques et des Postes, Paris, *www.arcep.fr/uploads/tx_gspublication/consult-freqc-bande-libre-juil2014.pdf*.

Australian Government (2014), *Independent Cost-Benefit Analysis of the NBN*, Australian Government, Canberra, *www.communications.gov.au/__data/assets/pdf_file/0003/243039/Cost-Benefit_Analysis_-_FINAL_-_For_Publication.pdf*.

BEREC (2014), *Case Studies on Regulatory Decisions Regarding Vectoring in the European Union*, BoR(14)122, Body of Regulators for Electronic Communications, Riga, *http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/4587-berec-report-case-studies-on-regulatory-_0.pdf*.

BEREC (2012), *A View of Traffic Management and other Practices Resulting in Restrictions to the Open Internet in Europe*, BoR(12)30, Findings from BEREC's and the European Commission's joint investigation, Body of Regulators for Electronic Communications, Riga, *http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf*.

BEREC (2010), *BEREC Report on Impact of Bundled Offers in Retail and Wholesale Market Definition*, BoR(10)64, Body of Regulators for Electronic Communications, Riga.

BEREC/RSPG (2011), *BEREC-RSPG Report on Infrastructure and Spectrum Sharing in Mobile/Wireless Networks*, BoR(11)26, RSPG11-375, Body of Regulators for Electronic Communications/Radio Spectrum Policy Group, Riga/Brussels, *http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/224-berec-rspg-report-on-infrastructure-and-_0.pdf*.

Bundesnetzagentur (2014), *Marktbefragung zu einem zukünftigen Nummernplan für Internationale Kennungen für Mobile Teilnehmer (Market survey for a future plan for International identifiers for Mobile Users) (International Mobile Subscriber Identity, IMSI)*, Release No. 819/2014, Bonn, Bundesnetzagentur, *www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Technische%20Nummern/IMSI/Mitteilung819_2014.pdf?__blob=publicationFile&v=5* (accessed 15 April 2015).

Clark, D. et al. (2014a), *Measurement and Analysis of Internet Interconnection and Congestion*, 21st TRPC conference, 9 September 2014, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2417573* (accessed 15 April 2015).

Clark, D. et al. (2014b), *Challenges in Inferring Internet Interdomain Congestion*, IMC 14 Proceedings of the 2014 Conference on Internet Measurement Conference, 5-7 November 2014, Vancouver, BC, *http://dl.acm.org.libproxy.mit.edu/citation.cfm?id=2663741* (accessed 15 April 2015).

CNMC (2014), Informe anual de telecomunicaciones y servicios audiovisuales 2014 (Telecommunications and Audiovisual Services Annual Report 2014), Comisión Nacional de Mercados y de la Competencia, Madrid, *http://informetelecom.cnmc.es/docs/Informe%20economico%20sectorial/Informe%20Telecomunicaciones%20CNMC%202014.pdf*.

EC (2006), *T-Mobile Austria/Telering*, Case No. COMP/M.3916, European Commission, Brussels, *http://ec.europa.eu/competition/mergers/cases/decisions/m3916_20060426_20600_en.pdf*.

EC (2013), *H3G/Orange Austria*, Case No. COMP/M.6497, European Commission, Brussels, *http://ec.europa.eu/competition/mergers/cases/decisions/m6497_20121212_20600_3210969_EN.pdf*

EC (2014a), *Telefónica Deutschland/E-Plus*, Case No. COMP/M.7018 Telefonica Deutschland/E-Plus, European Commission, Brussels, *http://ec.europa.eu/competition/mergers/cases/decisions/m7018_20140702_20600_4149735_EN.pdf*

EC (2014b), *H3G/O2 Ireland*, Case No. COMP/M.6992 Hutchinson 3G UK/ Telefonica Ireland, European Commission, Brussels, *http://ec.europa.eu/competition/mergers/cases/decisions/m6992_20140528_20600_4004267_EN.pdf*

European Parliament and European Council (2012), "Decision No. 243/2012/Eu Of The European Parliament And Of The Council of 14 March 2012 establishing a multiannual radio spectrum policy programme", 21 March 2012, Brussels, *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012D0243&from=EN* (accessed 15 April 2015).

FCC (2015), *Report and Order on Remand, Declaratory Ruling, and Order, in the Matter of Protecting and Promoting the Open Internet*, 12 March 2015, Federal Communications Commission, Washington DC, *http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0403/FCC-15-24A1.pdf*.

FCC (2014), "FCC Chairman Tom Wheeler: More competition needed in high-speed broadband marketplace", Fact Sheet, *Daily Digest*, Vol. 33/167, 4 September 2014, Federal Communications Commission, Washington DC, *https://apps.fcc.gov/edocs_public/attachmatch/DOC-329160A1.pdf*.

FCC (2011), "Bureau Staff Analysis and Findings", WT Docket No. 11-65, 29 November 2011, *https://apps.fcc.gov/edocs_public/attachmatch/DA-11-1955A2.pdf*.

FCC (2010a), *Eighth Broadband Progress Report*, FCC 12-90, 29, Federal Communications Commission, Washington DC, *www.fcc.gov/reports/eighth-broadband-progress-report* (accessed 15 April 2015).

FCC (2010b), *Open Internet Order*, Federal Communications Commission, Washington DC, *http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf*.

Krämer, J., L. Wiewiorra and C. Weinhardt (2013), "Net neutrality: A progress report", *Telecommunications Policy*, Vol. 37/9, pp. 794-813.

OECD (2015), "Triple- and quadruple play bundles of communication services", *OECD Digital Economy Papers*, forthcoming, OECD Publishing, Paris.

OECD (2014a), "Wireless market structures and network sharing", *OECD Digital Economy Papers*, No. 243, OECD Publishing, Paris, DOI: 10.1787/20716826.

OECD (2014b), "Connected televisions: Convergence and emerging business models", *OECD Digital Economy Papers*, No. 231, OECD Publishing, Paris, DOI: 10.1787/5jzb36wjqkvg-en.

OECD (2014c), "International cables, gateways, backhaul and international exchange points", *OECD Digital Economy Papers*, No. 232, OECD Publishing, Paris, DOI: 10.1787/5jz8m9jf3wkl-en.

OECD (2014d), "International traffic termination", *OECD Digital Economy Papers*, No. 238, OECD Publishing, Paris, DOI: 10.1787/5jz2m5mnlvkc-en.

OECD (2014e), "New Approaches to Spectrum Management", *OECD Digital Economy Papers*, No. 235, OECD Publishing, Paris, DOI: 10.1787/20716826.

OECD (2013), "Mobile handset acquisition models", *OECD Digital Economy Papers*, No. 224, OECD Publishing, Paris, DOI: 10.1787/5k43n203mlbr-en.

OECD (2011), "Broadband bundling: Trends and policy implications", *OECD Digital Economy Papers*, No. 175, OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/5kghtc8znnbx-en*.

OFCOM (2014), *The Future Role of Spectrum Sharing for Mobile and Wireless Data Services*, Statement, 30 April 2014, *http://stakeholders.ofcom.org.uk/binaries/consultations/spectrum-sharing/statement/spectrum_sharing.pdf*.

PCA (2013), *AdC emite Decisão final de Não Oposição, acompanhado de condições e obrigações destinadas a garantir o cumprimento dos Compromissos assumidos pelas Notificantes, no processo envolvendo a fusão entre a Optimus e a ZON* (*Competition Authority issues Final decision of Não Oposição not accompanied by conditions and obligations intended to ensure compliance with the commitments made by Notifications in the case involving the merger between Optimus and ZON*), Comunication No. 18/2013, Portuguese Competition Authority, Lisbon, *www.concorrencia.pt/vPT/Noticias_Eventos/Comunicados/Paginas/Comunicado_AdC_201318.aspx* (accessed 15 April 2015).

Pereira, P., T. Ribeiro and J. Vareda (2013), "Delineating markets for bundles with consumer level data: The case of triple-play", *International Journal of Industrial Organisation*, Vol. 31/6, pp. 760-773.

Rey, P. and Tirole, J. (2006), "A primer on foreclosure", in M. Armstrong and R. Porter (Eds), *Handbook of Industrial Organization*, Vol. 3, Elsevier, New York.

RSPG, (2013), *RSPG Opinion on Licensed Shared Access*, Radio Spectrum Policy Group, Brussels, *https://circabc.europa.eu/sd/d/3958ecef-c25e-4e4f-8e3b-469d1db6bc07/RSPG13-538_RSPG-Opinion-on-LSA%20.pdf*.

Sandgren, P. and B.G. Mölleryd (2013), "How liberalized is the optical fiber broadband market? Examining the role of public money in the fiber deployment in Sweden", paper presented at the 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, *www.econstor.eu/bitstream/10419/88544/1/774543892.pdf*.

Toledano, J. (2014), *Rapport: Une Gestion Dynamique du Spectre pour l'Innovation et la Croissance (Report: Dynamic Spectrum Management for Innovation and Growth)*, Report commissioned by the French Minister for SMEs, Innovation and the Digital Economy, *www.economie.gouv.fr/files/files/PDF/rapport-gestion-dynamique-spectre-2014-06-30.pdf*.

Völcker, S.B. (2004), "Mind the Gap: Unilateral Effects Analysis arrives in EC Merger Control", *European Competition Law Review*, Vol. 25/7, pp. 395-409, *www.wilmerhale.de/uploadedfiles/shared_content/editorial/publications/german_publications/mind_the_gap.pdf*.

White House (2010), *Presidential Memorandum: Unleashing the Wireless Broadband Revolution*, Memorandum for the Heads of Executive Departments and Agencies, White House, Washington DC, *www.whitehouse.gov\\thepressoffice\\presidentialmemorandumunleashingwirelessbroadbandrevolution* (accessed 15 April 2015).

WIK (2014), *Vectoring Benefits and Regulatory Challenges*, PowerPoint presentation at the FSR Communications Media 2014 Scientific Seminar "Economics and Policy of Communications and Media, Policy Challenges in Digital Markets", Florence School of Regulation, 28-29 March 2014, *www.wik.org/uploads/media/FSR_Vectoring_Benefits_and_RegChallenges_20140409.pdf*.

© OECD 2015

Chapter 5

Trust in the digital economy: Security and privacy

Trust plays a vital role in social and economic interactions. It functions as a powerful tool in complex environments for reducing uncertainties and enabling reliance on others. Trust underpins business, institutional and personal relationships and is particularly important in the global online environment. The opportunities presented by the digital economy will not be realised in the absence of trust. This chapter examines two key elements of trust online: security and privacy. It covers a select number of trends, which taken together provide an overview of digital security and privacy, both in terms of the risks and responses.

5.1 The growing profile of digital security and privacy risks

The OECD began developing its policy framework for trust online in the 1990s with a view to helping governments realise the economic and social potential of the Internet. Two decades later, information communication technologies (ICTs) and the Internet are widely integrated into economic and social activities. The resulting dependence of all sectors of OECD countries on the digital environment makes addressing security and privacy risk essential.

Digital security and privacy routinely feature on the front page of newspapers and in government strategies and speeches by senior political figures and corporate executives. In a 2014 OECD survey on the digital economy, governments identified security as the second highest priority area and privacy as the third out of 31 possible priority areas, with only broadband coming higher (OECD, 2014).

Privacy has also joined cybersecurity on the US Government's "High Risk List", attributed to the challenges posed by advances in technology, which have dramatically enhanced the ability of both government and private sector entities to collect and process extensive amounts of personal information (US GAO, 2015). Although the disclosures in 2013 by former NSA contractor Edward Snowden have no doubt elevated the visibility of security and privacy, the increasing prominence of these issues is the result of a transformation in the way data is generated, shared and analysed, and the corresponding benefits that these developments have brought in terms of innovation, growth and well-being.

This chapter reviews a number of topics addressed in a 2012 OECD survey of the evidence base for security and privacy, which uncovered a rich diversity of empirical data that could potentially enhance policy making in this sector (OECD, 2012a). It examines the available evidence in a number of discrete areas across the security and privacy landscape. This evidence is suggestive of the growing attention paid to security and privacy, shown for example by the booming professional class of privacy and security experts, as well as an important if less dramatic strengthening of the government bodies charged with protecting privacy and security. At the international level, one important development underway is the revision of the 2002 OECD Security Guidelines to help stakeholders better address digital security risks.

At the national level, governments continue to release and update national cybersecurity strategies (see Section 5.4). Opportunities for skilled security professionals continue to grow (see Section 5.2) and the role of national Computer Security Incident Response Teams (CSIRTs) is highlighted as a key response (see Section 5.3). In terms of legislation, data security breach notification, which bridges privacy and security risks, is on the rise (see Section 5.4). On the technical side, implementation of Domain Name System Security Extensions (DNSSEC) promises to provide security in the domain name system (Section 5.4).

Consumers report growing privacy concerns

Surveys suggest that the evolving risk environment is causing concern for security and privacy. A 2014 CIGI-Ipsos survey of Internet users on Internet security and trust, found that 64% of respondents in the 24 countries surveyed were more concerned about privacy than they were in 2013 (CIGI, 2014). According to a 2014 Pew Research Center poll, 91% of Americans surveyed agree that consumers have lost control of their personal information and data (Madden, 2014). In a special 2014 Eurobarometer report on cybersecurity, the top two concerns reported by EU Internet shoppers were misuse of personal data and security of online payments. In both areas the level of concern has grown since 2013, with fear of personal data misuse increasing from 37% to 43% and security concerns rising from 35% to 42% (EC, 2015).

Significantly, expressions of concern are not always accompanied by a change in behaviour. For example, numerous studies document how individuals reporting privacy fears nevertheless engage in risky behaviour involving their personal data, a phenomenon dubbed the "privacy paradox" (Taddicken, 2014). Recent surveys, however, suggest that users are taking steps to address their concerns. The CIGI-Ipsos 2014 study found that out of the 60% of Internet users that had heard of Edward Snowden, 39% took steps to protect their privacy and security as a result of his revelations. Recent Eurobarometer numbers are more striking, with 88% of EU respondents claiming in 2014 to have changed the way they use the Internet because of concerns about security, up from 81% in 2013. Password management is among the actions reportedly taken, with 31% reporting that they use different passwords for different sites, and 27% reporting that they change those passwords regularly (EC, 2015).

Surveys like these cannot of course conclusively establish the importance of consumer trust in the current online environment. However, there is increasing recognition of the need for better metrics and other evidence to inform policy makers in government and organisations of the size of the problem and to develop strategies to address the challenges (OECD, 2011a, 2012a, 2013b). Nevertheless, the perception that consumer trust is at stake persists and is reflected in recent business practices. For example, the last few years have seen an increasing number of multinational Internet and communication companies release transparency reports (see Section 5.4), which indicates growing recognition among companies of the linkage between consumer trust (whose data and loyalty are essential to the bottom line) and the need for public steps to protect privacy and secure online services.

Impact of security breaches can be significant

In 2014, security incidents featured regularly in mainstream media. One observable trend is an increase in theft of card account and customer credentials, as highlighted in the Target and Home Depot cases – two major US retailers. The Target breach reportedly involved payment card and other data of 70 million customers. Target corporate filings for 2013-14 recorded expenses related to the breach of USD 252 million, which even after being offset by USD 90 million in insurance proceeds, leave charges of USD 162 million. Ongoing litigation and regulatory proceedings have added further costs, including an estimated USD 200 million to issue new cards, which still omits the more speculative reputational costs. The breach at Home Depot involved 56 million payment card accounts and 53 million customer email addresses (Home Depot, 2014). Another major breach in 2014 involved three Korean credit card companies and affected 20 million individuals – 40% of the Korean population. Some three dozen executives lost their jobs as a result (Choe

Sang-Hun, 2014). The beginning of 2015 has continued the trend, with Anthem Inc., a large US-based health insurance company, announcing that hackers broke into its servers and stole social security numbers and address, email and employment data across its business lines, which will by some estimates affect 80 million individuals.

The impact of these security incidents can be significant for the organisations in question. Perhaps the most prominent malicious breach occurred at the end of 2014, when Sony Pictures Entertainment suffered a cyber attack that exposed unreleased movies, employee data, emails between employees, and sensitive business information such as sales and marketing plans. The duration of the hack is as yet unknown, although evidence suggests that the intrusion was ongoing for more than a year, prior to its discovery in November 2014. Although the direct financial costs of the breach may be covered by cyber insurance policies (see Section 5.4), the damage to the firm's reputation, relationships in the industry and impact on employees may be longer-lasting and hard to measure.

Although only larger incidents tend to capture the headlines, research suggests that data security breaches are commonplace. A 2014 study commissioned by the UK government found that 81% of large UK organisations suffered a security breach in the past year (BIS, 2014). Although this figure seems high, it actually represents a reduction of 5% from the 2013 survey. However, the severity and impact of security breaches has increased, with the cost of individual breaches nearly doubling in a single year. Major breaches are estimated to cost large organisations between GBP 600 000 and GBP 1.15 million. As discussed in Section 5.4 below, a new report from the Attorney General in California singled out the retail and health sectors as the target of a disproportionate percentage of reported data security breaches. Data security breaches are increasingly the subject of litigation, with card issuers looking to the hacked companies to recover the costs of reissuing payment cards, while class-action lawsuits brought by affected individuals are a growing possibility (Section 5.4). Moreover, breaches are not limited to the private sector. In Canada, the Office of the Privacy Commissioner stated that the number of data breaches reported by other Canadian government agencies more than doubled during the 2013/14 fiscal year. Accidental disclosure was indicated by reporting organisations as the reason behind more than two thirds of breaches.

The digital security threat landscape continues to evolve, sustained by often profitable business models. For example, "ransomware" is a type of file-encrypting malware increasingly deployed by cybercriminals to encrypt the computer files of an organisation or individual, who must then make a payment (i.e. the "ransom") in exchange for decryption of their files. The most prominent strain of ransomware is "CryptoLocker", which is spread via email attachments. Experts estimate that CryptoLocker infected some 234 000 computers, extracting more than USD 27 million in ransom payments, during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States (US DoJ, 2014).

New security vulnerabilities continue to be discovered with recent examples affecting the operation of key Internet protocols. "Heartbleed" involved the exposure of a critical vulnerability in Open SSL (Secure Sockets Layer), a security technology commonly used by websites to encrypt communications with users. By exploiting this vulnerability, an attacker was able to steal usernames, passwords and private encryption keys. The carefully chosen name "Heartbleed" illustrates the increasing efforts of security researchers who discover these vulnerabilities to publicise their findings. Heartbleed even has its own website: *http://heartbleed.com/*.

A similar vulnerability, dubbed "Shellshock", was disclosed in September 2014. It affects websites using the Unix and Linux operating systems. Like Heartbleed, Shellshock affects numerous systems that require a patch. In October 2014, a flaw in one version of SSL used by most commercial sites to protect user privacy and security was disclosed. Attackers can also exploit the "Poodle" vulnerability to decrypt passwords or other data from an SSL-encrypted transaction and other security protocols.

Responses to the evolving security risk landscape have been many-faceted and samples of these are provided at the end of the chapter.

The privacy risk landscape is evolving

Privacy issues have also received a significant rise in attention, including at the political level. President Obama's "State of the Union" speech to the US Congress referred to privacy on several occasions – a first for such an address (White House, 2015). In a speech announcing his legislative priorities on the eve of becoming President of the European Commission, Jean-Claude Juncker, committed to "swiftly concluding negotiations on common European data protection rules" (Junker, 2014).

No longer just the concern of specialists, privacy has attracted the attention of the scientific community as the subject of a special report in *Science* (2015). Concern about privacy has also spilled over into contemporary art, with the opening of the play *Privacy* in London's West End in 2014. One commentator has compared the role of privacy in the digital economy to that of competition policy reacting to the excesses of the Industrial Revolution in the early twentieth century (Tene, 2015).

Post-Snowden, much of the focus of the privacy community and media is framed in relation to the activities of national security agencies involving communications and Internet data. But the increasingly data-driven character of economic and social activities has raised privacy concerns around a host of other developments. Big data, the Internet of Things and data brokers have joined Internet search and social networking as regular topics subject to commentary and debate at conferences. One cannot consider the evolving privacy risk environment without recalling that many of the data security breaches noted above involved personal data, and as such represent a breach of privacy.

Legislation continues to feature as a key response to privacy risk, with security breach notification requirements (see Section 5.2) typically found in privacy laws. A series of developments in privacy legislation have taken place across OECD countries. Legal reforms came into effect in Australia in 2014, enhancing the powers of the Office of the Australian Information Commissioner (OAIC), while updating the Australian Privacy Principles. Canada's anti-spam legislation (CASL) came into effect in July 2014, requiring organisations to obtain consent before sending commercial electronic messages to an email, telephone or instant messaging account. Korea significantly revised its privacy law in 2012 to require data breach notification, with further revisions in 2014 to increase data breach fines and allow individuals to claim statutory compensation. Japan established its first independent data protection authority in 2014, with authority over personal information related to government-issued identification numbers for social security, taxation and disaster management.

Countries outside the OECD have also implemented changes in privacy legislation. China amended its consumer rights law, effective March 2015, to add a number of provisions regarding the protection of personal information. In 2014, Brazil adopted a long-awaited law

on the rights of Internet users – the "Marco Civil da Internet" – that creates fundamental rights regarding personal data covering consent, data deletion and purpose specification (see Chapter 1, Box 1.3). In November 2013, South Africa adopted the Protection of Personal Information Act, parts of which came into effect in 2014, including the establishment of an information regulator. Singapore's new law governing the collection and use of personal data by private sector organisations came into force in July 2014. Other countries with legislative developments include the Dominican Republic and Dubai (NYMITY, 2014).

In terms of major legislative initiatives, proposed privacy legislation in Europe and the United States remain works in progress. Negotiations are still underway in Brussels and EU member state capitals to complete a major overhaul of Europe's data protection framework, with work continuing to finalise proposals first announced by the European Commission in January 2012. The Obama administration has released a discussion draft of legislation to implement the Consumer Privacy Bill of Rights, and is supporting more targeted measures to address data breach notification and student privacy. Elsewhere, a process to reform Canada's private sector law "PIPEDA" remains underway and Japan is currently reviewing its Personal Data Protection Law to ensure its suitability for a world of "big data" and to improve its global compatibility (Cabinet Office of Japan, 2014)

Although privacy issues are seldom considered in a vacuum, a number of efforts to link privacy to other policy domains are noteworthy. Attempts to link trade and privacy are on the rise, in particular in the context of negotiations between the EU and the US towards a Transatlantic Trade and Investment Partnership. The European Data Protection Supervisor has taken steps to establish closer links between data protection and competition policy (EDPS, 2014), as personal data replaces natural resources as a key source of market power (Tene, 2015). In the research community, efforts continue to apply insights from behavioural economics to privacy policy.

In terms of international developments, the Council of Europe is working to update its primary data protection instrument, Convention 108. Meanwhile, Asia-Pacific Economic Co-operation (APEC) has begun a review of its 2004 Privacy Framework, with a view to possibly drawing on elements from the 2013 update to the OECD Privacy Guidelines. APEC is also working to implement its Cross-border Privacy Rules (CBPR) system, whose members include Japan, Mexico, the United States and most recently, Canada. Officials from APEC economies and representatives of the EU Working Party 29 are also continuing their collaboration to improve interoperability between the CBPR system and the EU's Binding Corporate Rules system. Lastly, the Organization of American States is working on a model law on personal data protection.

Encryption to protect user data is going mainstream

On the technology front, Apple, Google and other companies have increased the default use of encryption in respose to the Snowden disclosures. Apple's latest mobile operating system encrypts nearly all data on iPhones and iPads by default. Google's Gmail now uses an encrypted connection when checking or sending email via a browser. The company has also released a new browser extension to simplify the use of Open PGP, a common encryption tool (Somogyi, 2014). The popular messaging tool, WhatsApp, announced its own end-to-end encryption. Apple, now the world's most valuable publicly traded company, has also begun to explicitly market its privacy practices at the CEO level, emphasising security and privacy as fundamental design elements in Apple products and services. Such

developments offer encouragement to policy makers who have long hoped that businesses would treat privacy protection as a business differentiator.

Other developments that address privacy risks are covered throughout the remainder of this chapter. Of particular note is the increasing role of courts, in particular the *Costeja* decision of the European Court of Justice, which established an individual's right to have a search engine de-list certain results (commonly referred to as the "right to be forgotten") (Section 5.4). Another development is the upward trend in the number of privacy professionals working in the private sector. Growth in the privacy profession has been particularly striking, with one estimate putting overall expenditure on privacy programmes among Fortune 1000 companies at USD 2.4 billion per year (Section 5.2).

However, the growing profile of privacy and security issues has not been matched by an equivalent acceleration in the development of metrics and other evidence needed by policy makers in government and organisations, to help them evaluate the size of the problem and address challenges posed by the current environment (see OECD, 2011a, 2012a, 2013b). Furthermore, unlike cybersecurity, governments have not yet started to develop national privacy strategies, as called for in the OECD Privacy Guidelines, to address privacy issues in a coordinated, holistic manner, which would enables stakeholders to clarify the depth of protection to be afforded to individuals and the limitations society is willing to accept to serve collective public interests.

5.2 The job market for security and privacy professionals

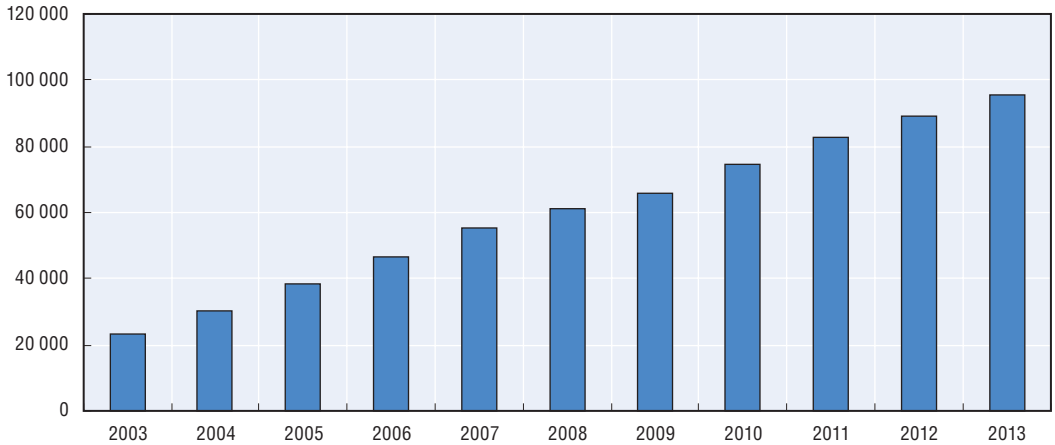
The growing importance and visibility of security and privacy risks has increased professional opportunities for experts in these areas. Demand for security expertise is characterised by a continuation of the steady growth evident over the last decade, while growth in demand for privacy professionals has accelerated rapidly in recent years. A new website devoted exclusively to jobs for privacy and cybersecurity professionals (*www.dataprivacycareers.com*) has emerged, with new opportunities posted daily. However, locating available professionals with the required skills and expertise in privacy and security remains a challenge for organisations looking to strengthen capacities in these areas.

Security professionals are in short supply as demand rises

The issue of cybersecurity now features prominently on national policy agendas. One of the most critical aspects is the availability of skilled professionals capable of helping organisations manage cybersecurity risks. However, the number of professionals worldwide continues to rise steadily. Bodies issuing professional certifications for cybersecurity skills provide a useful source of data on the growth of professionals this sector. For example, the International Information Systems Security Certification Consortium, otherwise known as $(ISC)^2$, issues a range of cybersecurity certifications. By end-2013, $(ISC)^2$ had certified 95 781 individuals worldwide (Figure 5.1), representing a four-fold increase in the last decade.

Despite this increase, the supply of skilled cybersecurity professionals falls well short of demand. A 2013 report by Japan's National Information Security Center suggests a shortage of 80 000 information security engineers in the country. Moreover, the report noted that most practising cybersecurity professionals lack the necessary skills to counteract online threats effectively (Humber and Reidy, 2014).

Figure 5.1. **Number of (ISC)² certified individuals worldwide, 2003-13**



Source: (ISC)², 2011 and e-mail correspondence with company.

StatLink http://dx.doi.org/10.1787/888933225200

In the United States, the Bureau of Labor Statistics forecasts a 37% rise in demand for graduate-level cybersecurity workers over the next decade – more than twice the predicted rate of increase for the overall computer industry (Coughlan, 2014).

In the United Kingdom, an analysis of government statistics on students leaving higher education in 2012-13, showed that less than 0.6% of recent computer science graduates work in cybersecurity (Barrett, 2014). The UK's National Audit Office has warned that it could take 20 years to fill the skills gap in trained cybersecurity staff (Coughlan, 2014). The National Cyber Security Programme, the Department for Business Innovation and Skills, the Government Communications Headquarters and the Cabinet Office have since partnered to lead and support activities to increase cybersecurity skills at all levels of education (HM Government, 2014).

In summary, available evidence suggests that despite growth in the cybersecurity profession, organisations still face a severe skills shortage in both the public and private sectors.

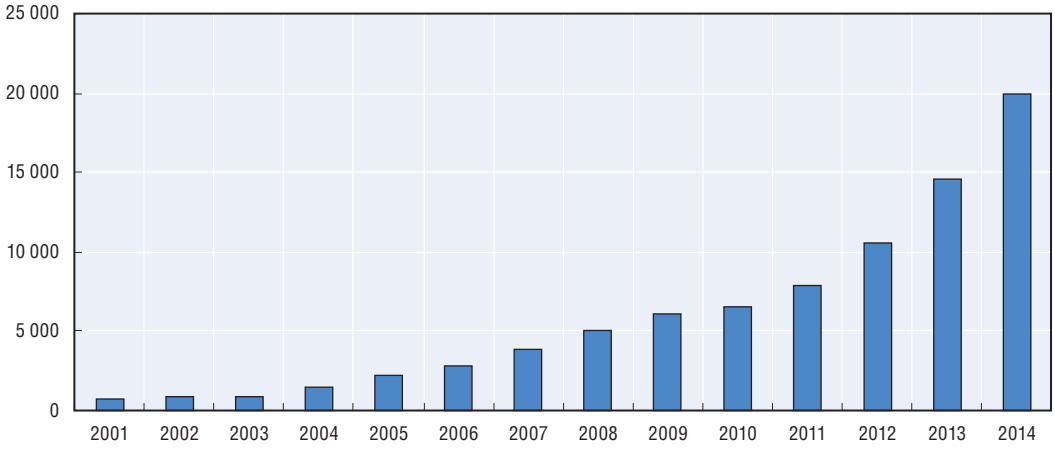
Privacy professionals are in demand

One of the most important developments in effective privacy protection measures has been the emergence of a professional class of privacy officers and experts in organisations. (Bamberger and Mulligan, 2010). In some countries, there is a statutory basis to support or encourage the role of privacy professionals. For example, Germany's Bundesdatenschutzgesetz (Federal Data Protection Act) sets out specific requirements concerning data protection officials in organisations. Canada's federal private sector legislation, PIPEDA, requires organisations to designate an individual(s) responsible for personal data-handling activities, and the EU Directive also contains a reference to a personal data protection official. New Zealand's Privacy Act requires every agency in both the public and private sectors to appoint a privacy officer and various pieces of US legislation require federal agencies to have chief privacy officers or senior agency officials for privacy. Both of Korea's privacy laws require companies to designate a person responsible for the management of personal information. Lastly, the proposed EU data protection regulation would require the appointment of data protection officers for all

public authorities and for companies processing more than 5 000 data subjects, which would further elevate the numbers of professionals.

These developments have been encouraged and supported by professional associations, setting the parameters for the development of a privacy workforce, including chief privacy officers (CPOs) and their staff (Clearwater and Hughes, 2013). These associations provide training, certification, conferences, publications, professional resources and industry research to a growing membership. The largest and most global in reach – the International Association of Privacy Professionals (IAPP) – now has more than 18 000 members (a 24% increase from September 2013) in 83 countries around the world (Figure 5.2). Others include the Privacy Officers Network, through which senior privacy officers involved in the practical implementation of privacy initiatives meet and exchange ideas through a professional support network,[1] and national bodies such as the Association Française des Correspondants à la Protection des Données à Caractère Personnel in France,[2] and the Asociación Profesional Española de Privacidad in Spain.[3]

Figure 5.2. **Total number of IAPP members, 2001-14**



Note: The figure for 2014 is a projection. As of October 2014 the number of members was 18 000.

Source: IAPP (2014). https://privacyassociation.org.

StatLink http://dx.doi.org/10.1787/888933225215

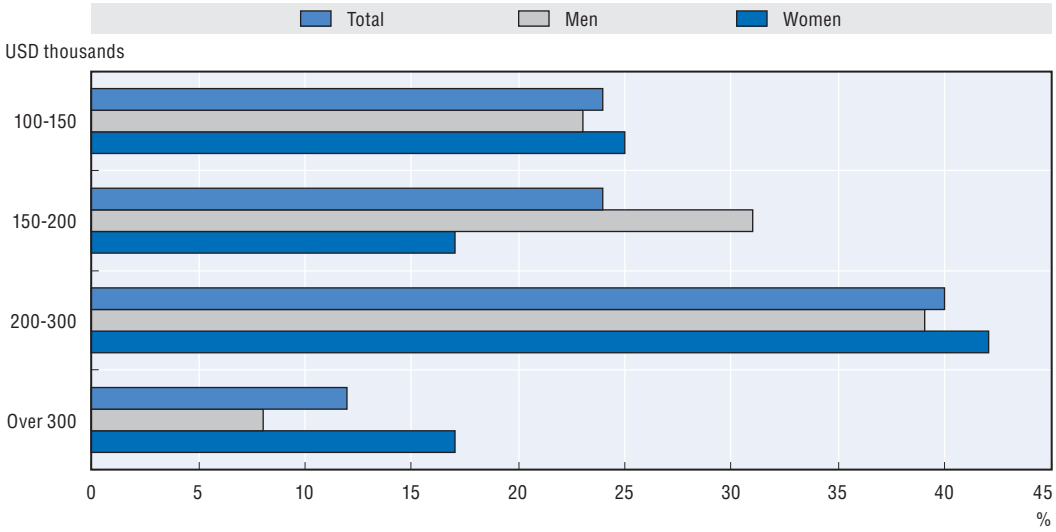
The steep growth in IAPP's membership numbers – from over 10 000 in 2012 to almost 20 000 projected by the end of 2014 – highlights increasing recognition of the importance of sound data governance practices. While budgets vary widely across Fortune 1000 companies, IAPP's "Fortune 1000 Privacy Program Benchmarking Study" found that the average privacy budget is USD 2.4 million, of which 80% is spent internally on areas ranging from developing policies, training, certification and communications, to audits and data inventories. Fortune 1000 companies spend an average of USD 76 per employee on privacy (IAPP, 2014). According to IAPP, overall expenditure on privacy among these companies is estimated at USD 2.4 billion per year.

A majority of respondents (59%) reported that they had personally established their company's privacy programme. This indicates that the privacy industry is still nascent with significant growth opportunities. Indeed, privacy budgets are likely to grow, with nearly 40% of privacy professionals predicting an average increase in their budget of 34% in coming years, and 33% of professionals intending to hire new privacy staff.

The IAPP's annual salary survey corroborates the results of the benchmarking study. The survey demonstrates a steady increase in privacy officers' pay (Figure 5.3), with CPOs earning an average of USD 180 000 per year in the United States, while privacy leaders (who do not hold the title of CPO) earn an average of USD 131 000 in the United States and USD 125 000 worldwide (IAPP, 2013).

Figure 5.3. **Annual income of a privacy professional in a Fortune 1000 company**

USD thousands



Source: IAPP (2013). *https://privacyassociation.org*.

StatLink http://dx.doi.org/10.1787/888933225226

For data-centred organisations, meeting privacy expectations requires more than legal compliance and sound security practices. Under the 2013 revisions to the OECD Privacy Guidelines, accountable organisations need to put in place multifaceted privacy management programmes, and be ready to demonstrate them on request from a privacy enforcement authority (OECD, 2013a, para. 15). Implementing such programmes requires legal, technical, communications, governance and public relations skills, among others. This has resulted in an increased focus on training, education and certification activities.

The growth in data-driven innovation, fuelled in part by data analytics, is also highlighting the importance of data ethics as a key element in protecting privacy (OECD, 2015a forthcoming: Chapter 6). Companies will need to adjust their perception of privacy as a compliance matter to be addressed by legal departments or as a technical issue to be handled by IT departments, and put in place ethical review processes. They must also ensure that privacy-literate employees are designated throughout the organisation to identify possible issues. Developing the skills and insights needed to meet these evolving needs should ensure continued demand for professional networks and associations for privacy professionals. However, this demand may have an adverse effect on privacy enforcement authorities – from whose rosters the private sector may increasingly look to recruit staff with the needed expertise and experience.

Although the growth in security and privacy professionals documented here is both impressive and important, it does not fully capture the shift in some organisations towards integration of these topics across workflows. For these companies responsibility for privacy/security issues is not limited to designated staff; instead it is shared among of all parts of the organisation dealing with personal data and matters impacting security.

5.3 Privacy enforcement and security response

The importance of privacy enforcement authorities is recognised in the 2013 revision of the OECD Privacy Guidelines, which includes a new provision calling specifically for the establishment of privacy enforcement authorities with the "governance, resources and technical expertise necessary to exercise their powers effectively" (OECD 2013a, para. 19). Approximately one third of OECD countries had such an authority in 1980 when the Privacy Guidelines were first adopted. Today, virtually all OECD countries report having established one or more privacy enforcement authorities.

Box 5.1. **What is a Privacy Enforcement Authority?**

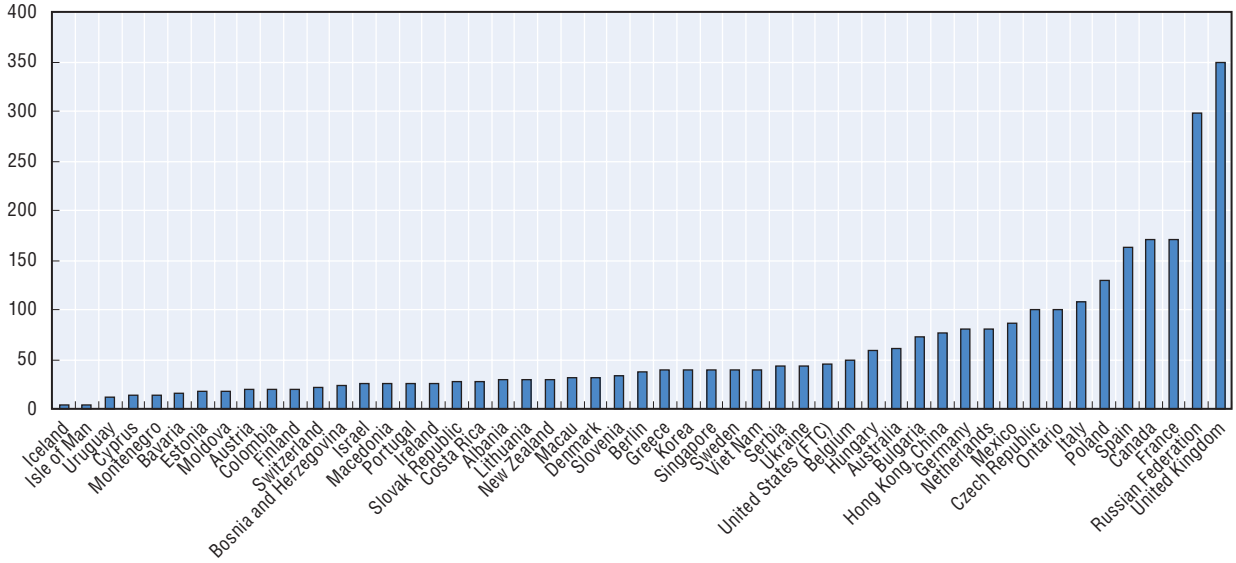
"Privacy Enforcement Authority" means "any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings." Federal countries may have regional or local authorities that fall within the definition.

Source: OECD (2013a, para. 1)

Budgetary resources

In 2013, the European research consortium PHAEDRA, established to improve co-operation among data protection authorities, surveyed 79 data protection authorities and privacy commissioners around the world. The survey included one question on staffing: How many full-time employees does your organisation have?" The results indicate that staff size varies widely across countries, from quite small to relatively large (Figure 5.4). With 350 full-time employees, the United Kingdom reports the highest number of full-time employees (FTE).

Figure 5.4. **Number of full-time employees in privacy enforcement authorities worldwide, March 2014**



Source: PHAEDRA (2014).

StatLink http://dx.doi.org/10.1787/888933225238

However, it is important to take note of the difficulties some countries face in answering questions regarding staffing levels. In Japan, for example, there was no dedicated authority for privacy protection until 2014. Prior to this date, sixteen different ministries took on the role of privacy enforcement authority in the sectors overseen by their government administration. Likewise, in some countries the number and role of sub-national level authorities can be quite significant. Generalising about staffing levels for privacy enforcement matters is therefore challenging.

Technical resources

Privacy concerns typically follow on from technological developments. In recent years, the rapid evolution in technology-driven business models and practices has posed challenges for enforcement authorities working to understand the implications of these changes for privacy. The integration of data-driven innovation more fully within firms will exacerbate these challenges (OECD, 2015a).

The explanatory memorandum to the revised OECD Privacy Guidelines underlines the importance of technical expertise in light of the increasing complexity of data usage, and supports the emerging trend within privacy enforcement authorities of retaining staff with a technical background. A small sampling of countries is suggestive of an increasing trend within privacy enforcement authorities of bring technical expertise in house. However, among the nine countries reporting on this issue for the period 2011-13, the ratio of technological experts to staff remains relatively low (Table 5.1).

Table 5.1. **Ratio of technological experts to total staff in privacy authorities for selected countries**

Country	2011	2012	2013
Belgium	1/52	1/52	1/52
Canada	3/160	5/161	5/173
Hungary	No data	3/47	3/56
Ireland	0/21	0/27	1/28
Italy	4/123	4/122	4/122
Lithuania	4/30	4/30	4/30
New Zealand	0/30	0/30	0/30
Sweden	1/40	1/40	4/41
United Kingdom*	2/256	3/280	3/288
Total technologists	*15*	*21*	*25*

Note: * The UK staffing figures are higher in Figure 5.4 because they include staff working on freedom of information issues.

Source: OECD DEO survey 2014.

These numbers do not reflect the situation in Korea (not shown) where numbers of technical staff are much higher, accounting for more than half of privacy employees; or in the United States, which also attaches importance to ensuring decisions are informed by sufficient technical expertise. This importance is reflected by the establishment of the position of Chief Technology Officer at the Federal Trade Commission (FTC) in 2010, a senior post held by prominent computer scientists. The FTC also reported a wide range of investigators and attorneys with technical skills in the United States, but was unable to identify a precise number. Likewise, with 16 ministries involved in privacy enforcement, the situation in Japan is complex. Each ministry devotes 2 to 13 employees

to privacy enforcement, many of whom co-operate with outside agencies to benefit from additional expertise.

Co-operation among privacy enforcement authorities is growing

Since the adoption of an OECD recommendation in 2007, co-operation among privacy enforcement authorities has become a priority (OECD, 2007). A 2011 OECD report highlights a number of areas in which progress is being made, including the formation of the Global Privacy Enforcement Network (GPEN) (see below). The report also highlights challenges and obstacles to more effective co-operation, particularly in the area of information sharing (OECD, 2011b). Recognising the need to take additional steps, privacy enforcement authorities have developed a "Global Cross Border Enforcement Cooperation Arrangement", which

> *encourages and facilitates all [privacy enforcement authorities'] cooperation with each other by sharing information, particularly confidential enforcement-related information about potential or on-going investigations, and where appropriate, the Arrangement also coordinates [privacy enforcement authorities'] enforcement activities to ensure that their scarce resources can be used as efficiently and effectively as possible (OPC, 2014b).*

In October 2014, the International Conference of Data Protection and Privacy Commissioners adopted a resolution endorsing the new Arrangement as a basis for facilitating enforcement co-operation among its members, and encouraged participation among all privacy enforcement authorities (OPC and ICO, 2014). While not legally binding, the Arrangement takes a number of important steps forward in strengthening the framework for cooperation among authorities. It aims to operationalise many of the good practices from the 2007 OECD Recommendation, including detailed provisions related to reciprocity and confidentiality. It also goes beyond the OECD recommendations, particularly in the area of coordination of international activities, and empowers the Conference's Executive Committee to help administer the Arrangement.

…as reflected in the activities of the Global Privacy Enforcement Network (GPEN)

As noted above, progress in enforcement co-operation is reflected in the activities of the Global Privacy Enforcement Network (GPEN), formed in 2010 on the recommendation of the OECD. GPEN aims to facilitate co-operation between data protection regulators and authorities throughout the world in order to strengthen personal privacy globally. GPEN currently consists of 51 data protection authorities across some 39 jurisdictions. One interesting development has been the addition of new authorities outside the usual data protection family; for example, the US Federal Communications Commission joined GPEN in October 2014 (FCC, 2014).

A collective GPEN survey, or "sweep", examined disclosure practices regarding the use of personal data by mobile apps. Over the course of a week in May 2014, GPEN's "sweepers" – consisting of 26 data protection authorities across 19 jurisdictions – participated in the activity by downloading and briefly interacting with more than 1 200 of the most popular apps released by developers. The purpose of the sweep was to increase public and commercial awareness of data protection rights and responsibilities, and to identify specific issues that may become the focus of future enforcement actions and initiatives (Box 5.2).

Box 5.2. **GPEN sweep results**

The sweep identified the following privacy challenges:

- 85% of apps failed to explain clearly how personal information would be processed.
- 59% of apps did not clearly indicate basic privacy information (with 11% failing to include any privacy information whatsoever).
- 31% of apps were excessive in their permission requests to access personal information.
- 43% of apps had not sufficiently tailored their privacy communications for the mobile app platform, often relying instead on full version privacy policies found on websites.

The sweep identified the following good practices:

- Many apps provided clear, easy-to-read and concise explanations about exactly what information would be collected, how and when it would be used and, in some instances, explained specifically and clearly what would not be done with the information collected.
- Some apps provided links to the privacy policies of their advertising partners and opt-out elections in respect of analytic devices.
- Some apps provided good examples of privacy policies specifically tailored to the app platform. These included use of just-in-time notifications (warning users when personal information was about to be collected or used), pop-ups and layered information, which allowed consumers to obtain more detailed information if required.

Source: UK Information Commissioner's Office.

On 10 September 2014, GPEN published the results of the sweep, which suggest that a high proportion of the apps downloaded did not sufficiently explain how consumers' personal information would be collected and used. Numerous instances were identified where apps which appeared to collect personal information did not have a privacy policy (or other up-front privacy information), thus removing the opportunity for individuals to be meaningfully informed when making decisions about the collection, use and/or disclosure of their personal information.

In December 2014, 23 privacy authorities from around the world signed an open letter to the operators of seven app marketplaces urging them to make links to privacy policies mandatory for apps that collect personal information (OPC, 2014a). The letter was sent to Apple, Google, Samsung, Microsoft, Nokia, BlackBerry and Amazon.com, but was intended for all companies that operate app marketplaces. It called on operators of app marketplaces to require each app capable of accessing or collecting personal information to provide users with timely access to the app's privacy policy.

..and in growing actions across Computer Security Incident Reponses Teams

Incident response is a fundamental part of cybersecurity risk management. In recognition of this fact, the 2002 OECD Guidelines for the Security of Information Systems and Networks ("Security Guidelines")[4] include a Response principle.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

A Computer Security Incident Response Team (CSIRT) is a group that acts as a trusted point of contact for computer security incident response. While all participants have a role to play in incident response, CSIRTs are dedicated to co-ordinating response activities. Their main responsibility is to handle and mitigate computer security incidents with the aim of protecting their constituencies (i.e. their customer base). A CSIRT may provide a range of services to its constituents, such as issuing alerts and advising on current and impending computer-related threats, or collecting and gathering data to analyse incidents in order to provide constituents with solutions and courses of actions to reduce risks and minimise the expected damage. CSIRTs may also issue advice on vulnerabilities and malware in the software and hardware running on their constituents' systems, allowing them to promptly patch or update their systems to prevent infection or further damage.

The Response principle of the OECD Security Guidelines also emphasises the co-operative nature of security incident response and the need for international co-operation in some instances. The spirit of this principle is reflected in numerous high-level policy statements and commitments at national, regional and international levels. For example, the United States *International Strategy for Cyberspace*,[5] the Association of Southeast Asian Nations (ASEAN) Regional Forum 2006 *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space* and the International Telecommunication Union's *Resolution 130*[6] all emphasise the importance of international co-operation in incident response.

In 2013, the UN Group of Governmental Experts recommended enhanced information sharing and co-operation in security incident response as a confidence-building measure, noting the importance of:

> *enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms (UN, 2013: 9).*

While there are currently no metrics for directly measuring international co-operation among CSIRTs, there are indications of interest in establishing closer links among teams globally. Statistics from the Forum of Incident Response and Security Teams (FIRST) reveal a steady increase in CSIRT participation at the Annual FIRST Conference – the premier international CSIRT event (Figure 5.5). At the 2014 conference in Boston, 299 teams participated. These statistics provide a good indication of increased interaction, information sharing, collaboration and co-operation among teams, which should lead to improved incident response and better cybersecurity risk management.

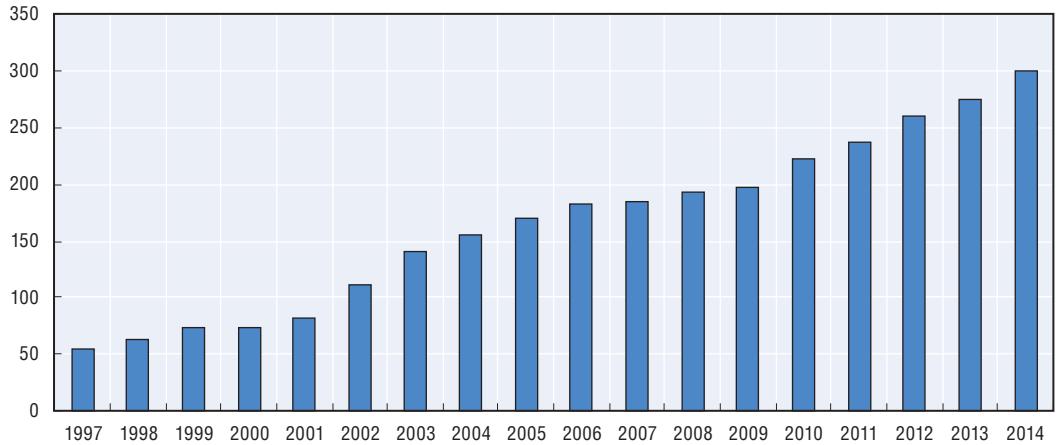
With increased recognition of the essential role that CSIRTs play in cybersecurity risk management comes increased expectations about the extent of their responsibilities, particularly from policy makers whose appetite is growing for reliable, trustworthy information about current and historical cybersecurity trends and the effectiveness of measures. There is mounting interest in CSIRT statistics among policy makers, but it is important that such statistics are of high quality and are internationally comparable if they are to inform decision making.

The 2012 OECD report on *Improving the Evidence Base for Information Security and Privacy Policies* found that many CSIRTs already generate statistics based on their daily activities, particularly statistics on the number of incidents handled (OECD 2012a). CSIRTs also collect

data or potentially have access to data that could be used to generate statistics on other relevant phenomena if appropriate guidance were available. However, the quality and international comparability of these existing and potential statistics raise many challenges. The OECD is therefore working with the incident response community to develop guidance to improve the international comparability of statistics produced by CSIRTs (see OECD, 2015b, forthcoming).

Figure 5.5. **Attendants to the Annual FIRST Conference**

Number of Computer Security Incident Response Teams (CSIRT)



Source: Based on statistics from the Forum of Incident Response and Security Teams (FIRST).

StatLink http://dx.doi.org/10.1787/888933225245

5.4 Other selected trends impacting trust

Reliable trend data are difficult to obtain in this area. The following six subsections therefore examine very different aspects of the trust environment. The first considers the ongoing development of **national cybersecurity strategies** by OECD members and non-members. The second focuses on **data security breaches** involving personal data and the growth in **notification** requirements. One purpose of these notifications is to better position enforcement agencies to take appropriate measures in response. Likewise, notification is required in some circumstances to alert affected individuals who may then take steps to respond. Breach notification also enables authorities to gather statistical information to better understand the dimensions of the data security breach challenge. The third subsection explores the growth of **cyber risk insurance** markets. The fourth looks at the deployment of a promising new security measure: **DNSSEC**. The fifth subsection discusses the emergence of **transparency reporting** as a tool for better understanding the scale of government access to commercial data. The sixth and final subsection, highlights the increasing **role of the courts** in the governance of privacy and data protection.

A new generation of national cybersecurity strategies

In 2012, the OECD published a comparative analysis of the new generation of national cybersecurity strategies. The report found that in many countries, cybersecurity had become a national policy priority supported by high-level leadership. It also concluded that new national strategies were becoming integrated and comprehensive, approaching

cybersecurity in a holistic manner encompassing economic, social, educational, legal, law enforcement, technical, diplomatic, military and intelligence-related aspects, and that "sovereignty" concerns were growing increasingly important (OECD, 2012c).

The 2012 report focused on the strategies of ten OECD member countries: Australia, Canada, Finland, France, Germany, Japan, the Netherlands, Spain, the United Kingdom and the United States. These strategies recognise that economies, societies and governments now rely on the Internet for many essential functions and that cyber threats are increasing and rapidly evolving. Most of the strategies aim to enhance government policy and operational co-ordination and to clarify roles and responsibilities, while calling for improved international co-operation.

Since the report was released, several other countries have pursued the development of national cybersecurity strategies. Across the OECD, new strategies have been published in Austria (2013), Belgium (2013), Hungary (2013), Italy (2013), Norway (2012), Switzerland (2012) and Turkey (2013). In addition, Japan (2013), the Netherlands (2013) and Estonia (2014) have published updates to their national strategies. In November 2014, Australia announced that it would undertake a six-month review of its strategy to identify strengths and weaknesses (Government of Australia, 2014).

In November 2014, Japan adopted its Basic Act on Cybersecurity. The Act states that cybersecurity policies shall be carried out according to the following principles: (i) ensuring the free flow of information, (ii) respecting citizen rights, (iii) taking a multistakeholder approach, (iv) co-operating internationally, and (v) promoting an advanced information and telecommunications network society. In January 2015, Japan established its Cybersecurity Strategic Headquarters, which will formulate the draft of the national cybersecurity strategy, working under the Cabinet. Japan has also established the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which functions as the headquarters' secretariat and the national cybersecurity operation centre.

Many non-OECD members have recently adopted or revised their national cybersecurity strategies, including India (2013), Kenya (2013), Latvia (2014), Qatar (2014), Russian Federation (2013), Singapore (2013), South Africa (2013), Trinidad and Tobago (2012) and Uganda (2013). Several other countries are currently in the process of developing national strategies.

In 2014, the Chinese government organised a high-level working group on cybersecurity and Internet management, chaired by the country's president. The group was formed, in part, to better co-ordinate China's Internet security policies. At present, no fewer than six different agencies and ministries provide input into China's cybersecurity policies, including the Ministry of Public Security, the State Encryption Bureau, the State Secrets Bureau, the Ministry of State Security, the Ministry of Industry and Information Technology and the People's Liberation Army. The group aims to improve co-operation among different agencies and ministries, while raising the profile of cybersecurity among leaders (Segal, 2014).

One notable trend for national cybersecurity strategies is the increasing role played by international and regional organisations in their development, implementation and evaluation. In Europe, the Cybersecurity Strategy of the European Union (2013) is accompanied by draft legislation that would oblige member states to adopt a national cybersecurity strategy. Eighteen of the European Union's 28 member states currently have a national cybersecurity strategy (ENISA, 2013).

The Organization for American States has assisted Colombia, Panama, and Trinidad and Tobago in drafting and adopting their national cybersecurity strategies. The OAS has also initiated a process with the governments of Dominica, Jamaica and Suriname to develop their national strategies, and also aims to assist Paraguay and Peru (OAS, 2014).

The African Union Convention on Cyber Security and Personal Data Protection (2014) calls on AU members to develop national cybersecurity strategies, focusing in particular on legislative reform and development, capacity building, public-private partnerships and international co-operation. Moreover, it stresses that such strategies should define organisational structures, set objectives and timeframes for successful implementation and lay the foundation for effective management of cybersecurity incidents and international co-operation.

In late 2014, ENISA published a framework for evaluating national cybersecurity strategies. It noted that many countries have different views on the intended outcomes or impacts of their strategies, or on how to achieve them (ENISA, 2014). The ENISA report suggested a number of possible key performance indicators for national cybersecurity strategies across five policy objectives: (i) developing cyberdefence capabilities, (ii) achieving cyber resilience, (iii) reducing cybercrime, (iv) developing industrial and technological resources for cybersecurity, and (v) securing critical information infrastructure.

To date, the process to revise the 2002 OECD Security Guidelines has underlined the need for national strategies to pursue the following complementary objectives: (i) create the conditions for all stakeholders to manage digital security risk to economic and social activities and foster trust and confidence in the digital environment; (ii) safeguard national and international security, and (iii) preserve human rights. Discussions supporting the revision of the 2002 OECD Recommendation also highlighted the need for further effort on ways to best support Small and Medium Enterprises and individuals, to manage digital security risks to their activities.

Data security breach notification

Notification requirements for data security breaches that affect personal data trace their origins to the United States, where virtually every state has followed in the footsteps of a 2003 breach notification law in California. The revised OECD Privacy Guidelines call for controllers to provide notifications in cases where there has been a significant security breach affecting personal data (OECD, 2013a, paragraph 15c). Countries outside the United States have begun to include data breach notification in their laws and policies.

In terms of generally applicable or "ominibus" laws, Korea's Personal Information Protection Act has a general notification requirement to relevant authorities in the event of a data breach. Meanwhile, proposed legislative reforms would make breach notification mandatory in Canada.

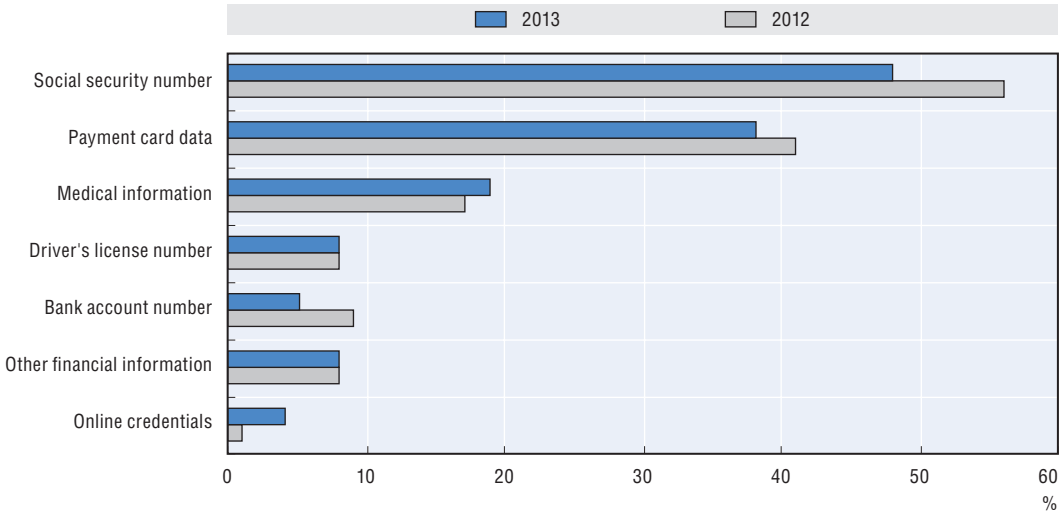
Sector-specific rules apply in EU/EEA countries, where breach notification requirements affecting the telecommunications sector arise out of the "e-privacy" Directive, 2002/58/EC. The required notice is directed to the relevant data protection authority and to individuals in particular circumstances, some of which vary depending on the country. Notification to an individual is required in Ireland in cases where the breach is likely to adversely affect the personal data or privacy of that individual. In Italy, preliminary notice to the Data Protection Authority must be provided within 24 hours, with additional information sent within three days via a form available on the website. In Hungary, notice is sent to the communications regulator, who may inform the public in appropriate cases. Given

the potential damage from breaches in the communications sector, Korea has included additional requirements to its general notification provisions for communication service providers to notify affected individuals and relevant authorities within 24 hours of a breach. Other sector-specific requirements are in place in Canada, where they apply to the public sector, with notifications to the OPC and Treasury Boards.

There are numerous non-binding guidelines or codes of practice outlining circumstances where notification would be appropriate. In some cases, these have general application (Ireland, New Zealand) and in others they are sector specific, for example, covering health (United Kingdom). In some cases, the authority has provided guidelines for compliance. For example, the Italian Data Protection Authority issued guidelines in 2013 (DPA, 2013) addressing issues such as coverage of specific entities.

One important benefit of notification obligations is the opportunities they provide for measurement of data breaches. For example, the US state of California's data breach report, issued in October 2014, reported 167 data breaches for 2013, an increase of 28% from 2012 (OAG California, 2014).

Figure 5.6. **Types of data breached in California, 2012-13**



Note: The total is bigger than 100% because some breaches involved more than one data type.

Source: OAG California (2014).

StatLink http://dx.doi.org/10.1787/888933225252

These breaches involved the personal information of more than 18.5 million California residents, an increase of more than 600% over 2012. This rise was due largely to two massive retailer breaches, one of which – the Target breach – involved the payment card data of 41 million individuals, including 7.5 million Californian residents. A majority of reported breaches (53%) resulted from malware and hacking, affecting 93% of all compromised records.

A number of national privacy enforcement authorities have begun to publish information on the volume of data security breach notices they receive, often in annual reports (e.g. Ireland, New Zealand, United Kingdom). Anecdotal evidence suggests that enforcement activity as a result of security breaches appears to be on the rise. As an example, the French regulator has issued a public warning to Orange France in response to failures that resulted in a data security breach compromising the personal data of more than 1 million customers.[7]

Cyber insurance policies

The extension of existing insurance policies, such as those covering first-party commercial property or business interruption, to protect businesses and individual users from Internet-based risks – and more generally from risks relating to information technology infrastructure and activities – may provide sufficient coverage for some cybersecurity incidents. In practice, however, insurance companies have been traditionally averse to covering risks associated with widespread corporate use of IT infrastructure (including the Internet) or the risks associated with non-tangible assets such as data. For example, most property, business interruption, theft and terrorism policies are based on loss of – or damage to – physical assets (data is not generally considered "property") (Marsh, 2013: 5). Both liability coverage and errors and omissions coverage generally respond to negligence by the insured and do not usually cover the expenses associated with a data breach, such as customer notification costs and regulatory fines (Marsh, 2013: 10). Even kidnap and ransom insurance will generally not cover "cyber extortion" without a specific amendment (Box 5.3).

Box 5.3. **Cyber insurance policies for enhancing risk management**

Cyber insurance policies have long reflected the approach taken by organisations towards the role of ICTs in their overall functioning (i.e. relative isolation from other business processes). Accordingly, insurance policies have considered IT risk exposure in terms of technological risk (e.g. "Operational Technology" exposure). However, ICTs have progressively become essential to the functioning and development of all aspects of the value chain and competitiveness of organisations. Simultaneously, incidents are multiplying across all sectors and are generating significant losses.

Organisations are therefore progressively integrating risks related to the use of ICTs into the broader enterprise risk management framework, and are approaching it from a business needs perspective. This relatively new context provides a basis for organisations to explore the option of risk transfer, as well as the possibility of a growing "cybersecurity" risk insurance market.

The insurance market is, however, evolving to respond to increased demand for new cybersecurity risk insurance products. Specialised cybersecurity risk insurance, sometimes referred to as "cyber risk" insurance or simply "cyber" insurance, has been designed to mitigate losses from cybersecurity incidents such as data breaches, business interruption and computer network damage. Following an incident, significant costs may arise from forensic investigations, lawsuits, data breach notification expenses, regulatory investigations, regulatory fines, attorneys and consultants, public relations professionals and remedial measures (Ferrillo, 2014).

It is estimated that over 50 insurers in 2014 offered stand-alone cybersecurity risk insurance policies (Armerding, 2014). Most of these insurers are based in the United States, where the policies are commonly used to transfer risk in jurisdictions which have mandatory data breach notification laws that require organisations to inform customers when their data has been lost or stolen. According to the Ponemon Institute (2014), 26% of companies in the United States held cybersecurity risk insurance policies in 2014, up from 10% in 2013.

However, the cybersecurity risk insurance market is still nascent compared to other insurance markets. In the United States, where the market is most mature, insurers write just over USD 2.5 billion of premium income per year, equivalent to less than 0.5% of the country's commercial insurance market (Gray, 2014). The cybersecurity risk market is even smaller in Europe, where the industry writes an estimated USD 150 million worth of premiums a year (Gray, 2014). However, the number of cybersecurity risk insurance products is growing. In 2013, insurers introduced 38 new cybersecurity risk insurance products (Advisen, 2014).

National and regional regulation likely has an influence on the size and attractiveness of the cyber insurance market. For example, data breach notification laws adopted in the United States may have served as a driver for insurance, as the costs of notifying affected users can be very high. Regulatory trends in the European Union with respect to the protection of critical infrastructures could have a similar effect on the European cybersecurity insurance market.

Governments are beginning to explore ways to promote the growth of cybersecurity risk insurance markets as a means to improve overall cybersecurity risk management in organisations. For example, a robust cybersecurity insurance market may help reduce the number of successful cyber attacks by (i) promoting the adoption of risk reduction measures in return for better coverage, and (ii) encouraging the implementation of best practices by basing premiums on the insuree's level of protection (DHS, 2014). A key question – and an area for further research – relates to the potential obstacles and inhibitors preventing the cybersecurity insurance market from expanding at a faster pace.

On the supply side, lack of actuarial data has impeded the development of policies. The high prices of available policies reflect uncertainty among underwriters, who find it challenging to price risks when they lack experience with past claims. In addition, insurance coverage for cyber risks requires a significant investment by insurers in the necessary technical expertise to assess such risks. Insurers need to develop an evidence base and to refine methodologies to assess the cybersecurity risks of different industries and organisations. This is important because different industries face different kinds of cybersecurity risks.

On the demand side, an important limitation is the slow pace at which businesses have progressed in adopting a wider operational risk management approach. While many organisations are progressively adjusting their digital security risk management governance to better integrate it within the broader enterprise risk management framework, many leaders and decision makers still view "cybersecurity" as a technical issue, reducing the potential scope for insurance.

It has also been recognised that many organisations forego available insurance policies due to their perceived high cost, confusion about what they cover and how much insurance to purchase, as well as uncertainty regarding the assessment of cyber risk (DHS, 2014). It will be important to track how governments respond to ongoing developments in the cyber insurance industry, and to further ascertain which measures prove effective in strengthening and supporting the market.

Validation of Domain Name System Responses (DNSSEC Validation)

The Domain Name System (DNS) is one of the key components of the Internet, and also a critical point of vulnerability. Hostile attacks that manage to replace a genuine DNS response with a crafted response can misdirect a user's traffic to unintended locations.

This may result in a breach of confidentiality (data snooping) and/or permit the launch of various forms of deceptive attacks against the user. Internet users are placed in the position of being forced to trust the responses they receive from their queries, yet have no certain means to assure themselves that they are not being misled by a malicious third party.

The response to this vulnerability in the DNS is to add digital signatures to the DNS resource records. While this does not prevent third parties from attempting to inject false information into the DNS, it does enable a DNS resolver to validate the DNS response it receives by validating the digital signature signed across the response, thereby confirming that the received DNS information is genuine. The security technology, called Domain Name System Security Extensions (DNSSEC), defines a method for adding digital signatures to a DNS zone, and a validation procedure to authenticate both responses provided by the DNS and assertions of non-existence in the DNS for entries in signed zones.

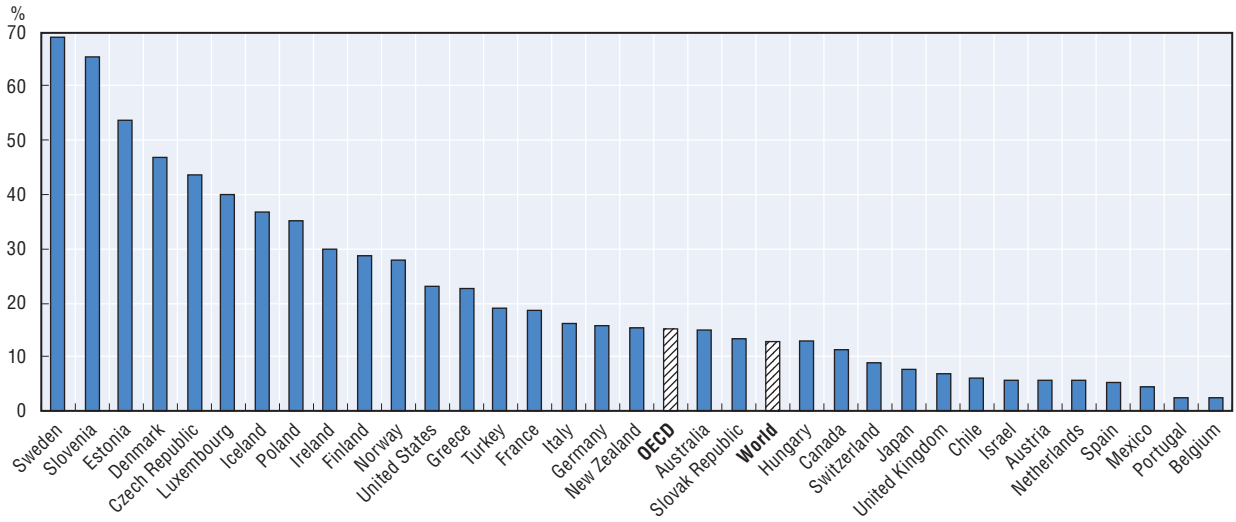
Widespread adoption of DNSSEC has the potential to significantly improve the robustness and reliability of the Internet, by providing an effective means to detect attempts to subvert the functioning of the Internet's naming system and to avoid the use of falsified DNS responses. The overall effectiveness of DNSSEC depends on two factors: the extent to which domain name zone administrators use DNSSEC to sign the contents of their DNS zone, and the extent to which clients use DNS resolvers that perform DNSSEC validation when they receive a digitally signed response. The greater the number of clients who use DNS resolvers that perform DNSSEC validation, the greater the level of motivation for DNS zone administrators to use DNSSEC to sign their zone as a measure to improve confidence in the integrity of the online services provided under the auspices of a particular DNS name.

It is possible to estimate the proportion of end users who pass their DNS queries to a DNS resolver that performs DNSSEC validation. The experimental technique[8] used to automatically gather the data (Figure 5.7) involves the presentation of a set of simple DNS tasks to a very large cross-section of users, where the task includes the resolution of a DNS name signed using DNSSEC. The users who contributed experimental results were gathered using an online advertising network with broad penetration across the entire Internet user population. Figure 5.7 shows the estimated percentage of users in each OECD country who use DNSSEC-validating DNS resolvers. Adoption of DNSSEC validation in DNS resolvers varies significantly across countries.

Several factors are hindering more widespread adoption of DNSSEC validation. Among these is the perception that efforts to improve the integrity of basic query/response transactions within DNS operation are of a lower level of relative priority than, for example, devising methods to mitigate use of the DNS as a platform for launching various forms of denial-of-service attacks. Another factor might be the relatively conservative approach of many service providers with respect to possible changes to the existing operational DNS infrastructure required for DNSSEC adoption. Considering that almost every transaction on the Internet intrinsically requires a call for DNS name resolution, and that the stability and consistency of DNS resolver operations is a critical element of online service provision, some conservatism with respect to adoption of changes to the operation of DNS services is not unreasonable.

Further studies of validation activity would be needed to corroborate the results reported in Figure 5.7. Nevertheless, the figure shows a high level of variance in the use of DNSSEC-validating resolvers across the member countries of the OECD. The exceptional

Figure 5.7. **Use of DNSSEC validation, 2015**



Note: These statistics reflect the proportion of end users who pass their DNS queries to a DNS resolver that performs DNSSEC validation from 1 January 2015 through to 22 April 2015. It does not reflect the use of DNSSEC by domain name zone administrators to sign the contents of their DNS zone.

Source: Asia Pacific Network Information Center, April 2015. *http://stats.labs.apnic.net/dnssec*.

StatLink *http://dx.doi.org/10.1787/888933225269*

results of Sweden, where almost three quarters of the national user population use DNSSEC-validating resolvers, were the result of the co-ordination of efforts undertaken by name registrants, name registrars, DNS resolver operators and governmental agencies in the country. The .se operator provided financial incentives through reduced registration fees when domain name registrars registered signed domain names in .se. Additional outreach efforts by the .se national registry to the major DNS resolver operators in Sweden prompted a number of access service operators to experiment with switching on DNSSEC validation for their customers. Following the decision of one of the largest access providers to switch on DNSSEC validation – and the lack of negative impact from the change – other major access providers in Sweden followed suit. As a result, some three quarters of Swedish Internet users now have their name queries handled by DNS resolvers which use DNSSEC to validate DNS responses when querying for names that are DNSSEC-signed. The Swedish experience suggests that co-ordinated efforts by key stakeholders can have a positive impact on the adoption rate of this promising technology.

Transparency reporting

Governments have long recognised the importance of accessing data about citizens to achieve public interest objectives, particularly in the context of law enforcement and national security. As more and more human activity generates data that traverses global commercial networks, government actors are increasingly looking to communications providers and Internet intermediaries to help meet their data needs. Laws and oversight mechanisms shape government access to this type of data, but government power may also induce business co-operation beyond what is mandated by data access provisions.

Today there are concerns about the level of transparency regarding the scale and scope of access to commercial data for law enforcement and national security purposes. Laws and agency practices in these areas typically impose secrecy requirements on the commercial

targets of access requests. The result is an increasing flow of data from businesses to government that is largely opaque to the customers and citizens whose data are at issue.

Fostering trust in the digital economy though improved transparency is a long-standing OECD objective. The "openness" principle of the OECD Privacy Guidelines dates back to the original 1980 adoption and counsels in favour of a general policy of openness about the processing of personal data. The 2011 OECD Recommendation on Principles for Internet Policy Making (IPPs) also calls for policies that ensure transparency, fair process and accountability. It recognises that policy making for the Internet should promote openness and be grounded in respect for human rights and the rule of law.

Transparency is an important means of ensuring trust in an organisation, particularly where it handles personal data. Concerns about government access requests – particularly to data entrusted to providers of cloud computing services – predate the revelations by Edward Snowden in 2013 and are not limited to intelligence gathering. But it is clear that those revelations have brought into sharper focus the need for transparency. Today, Internet and communications businesses with large data holdings about individuals are under market pressure to be much more open about the manner in which they respond to government access requests.

Responding to those market pressures in a manner consistent with government rules and practices can be difficult for businesses. As mentioned above, law enforcement and national security legislation often includes restrictions preventing businesses from disclosing information relating to government access demands, barring even the disclosure of aggregate statistics. In many countries, commercial operators are also prohibited from providing the public with any insight into the manner in which they respond to those demands. These restrictions can make it difficult for companies to respond to public demand for greater transparency.

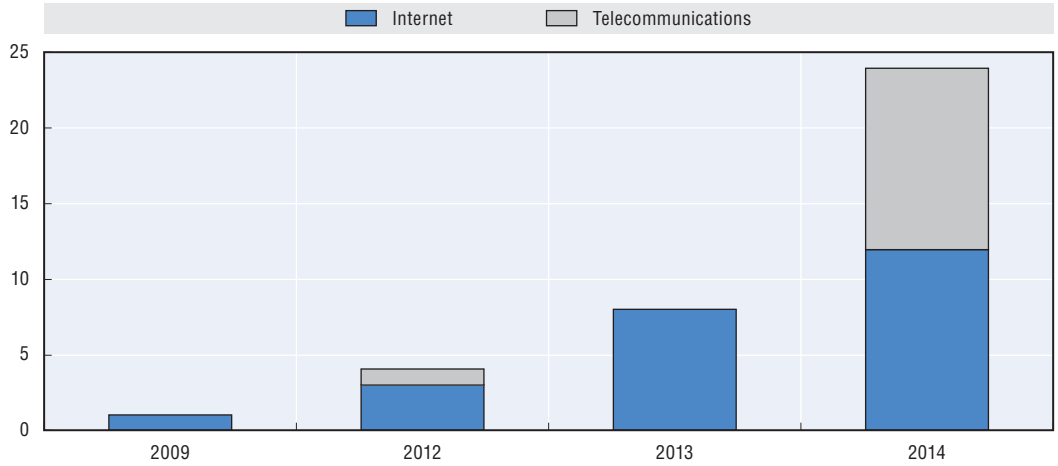
In 2011, The Privacy Projects (TPP) began to study the issues surrounding systematic government access to commercial data through a series of expert reports and roundtable discussions. One of the key findings from that work is the existence of a serious transparency gap surrounding both the laws and governmental agency practices (Box 5.4).

Box 5.4. **Preliminary findings from TPP work**

- Systematic access demands do appear to be growing, although the recent disclosures make it clear that governments are not only demanding stored data in bulk, but also are tapping into cables to collect or filter large swaths of data as it moves across the Internet.
- There is a profound lack of transparency about countries' laws and practices. Relevant laws are at best vague, and government interpretations of them are often hidden, especially in the national security realm.
- In particular, published laws and policies do not expressly address the unique challenges of bulk collection.
- Plummeting data storage costs and enhanced analytical capabilities spur governments' appetites to collect more data.
- As Internet-based services have become globalised, surveillance has become trans-border, posing increased legal and reputational risks to businesses operating globally.

One response to this situation has been an effort by companies to shed light on the issue through the publication of transparency reports. Since the release of the first such report by Google in 2009, more than 30 companies have issued public reports.[9] According to the Transparency Reporting Index, as of November 2014 there are 37 companies reporting on transparency. Out of these, 65% are Internet companies, while 35% are telecommunications firms. Out of 37 companies, around two thirds began reporting in 2014. The majority of companies report on a six-month basis (54%), and 32% prefer to do so on a yearly basis (Figure 5.8).

Figure 5.8. **Company transparency reporting, 2009-14**



Source: Based on data from the Transparency Reporting Index, November 2014. *https://www.accessnow.org/pages/transparency-reporting-index.*

StatLink http://dx.doi.org/10.1787/888933225279

These reports represent an important step forward in increasing the transparency associated with government access to commercial data. However, there is little consistency or comparability in the reports produced so far. For example:

- Some report on the number of individual demands received, while others report on the cumulative number of targeted accounts, communications services or subscribers.
- Sometimes multiple legal powers are used to obtain the same record, creating classification challenges.
- The same demand may be described or disclosed in a different way by different companies. There are therefore significant risks of over-counting/under-counting (Vodaphone, 2014).

While governments have begun to acknowledge the need to improve transparency and are taking steps in that direction,[10] more work is needed to improve public understanding about how governments access and use commercial data. Transparency reports are an important step forward in this regard, but work is needed to improve the quality and comparability of these reports and to identify unnecessary barriers to making these improvements.

The role of the courts

Courts have begun asserting greater influence over the rules governing privacy and data protection. The shift is most pronounced in the European Union, where the Court of Justice issued three significant rulings in 2014.[11] One ruling struck down the EU Data

Retention Directive, which obliged communications companies to retain communications metadata for law enforcement access. The Court considered that the Directive interfered with the fundamental right to private life and the protection of personal data.

A second key ruling involved the search engine Google, which interpreted the EU data protection directive as establishing a limited right for individuals to have search engines delete material from search results (commonly referred to as the "right to be forgotten").[12] The ruling places Google in the position of evaluating whether a link should be removed. As of January 2015, Google had removed approximately 40% of the 700 000 URLs it evaluated, amounting to nearly one quarter of a million links (Google, 2014).

The final ruling involved the "household exception", which exempts certain types of domestic processing from data protection rules. A homeowner's decision to install a CCTV camera succeeded in helping him identify individuals who attacked the property. However, the court ruled that because the cameras partially monitored a public space, the household exemption did not apply and that therefore the homeowner should have complied with the relevant data protection rules.

According to one commentator, the cumulative effect of these three rulings is to suggest increasing discomfort on the part of the court regarding society's dependence on data (Ustaran, 2014). The impact of these rules goes well beyond the particular parties to the cases, setting standards across Europe. The Google case, in particular, raises issues related to the role of intermediaries, extraterritorial jurisdiction, and the challenges of balancing data protection with other fundamental rights. Likewise, a challenge to the Safe Harbor arrangement under the EU Charter of Fundamental Rights, referred to the CJEU in June 2014 by the Irish High Court, could allow for an overturning of the adequacy finding for Safe Harbor by the European Commission. If the decision were to lead to the overturn of Safe Harbor, it would have direct implications for the governance of data flows.

While the evolving role of the judiciary is most pronounced in the European Union, there are other court decisions with significant policy implications. In a case that is still pending, a New York court is considering a challenge by Microsoft to an effort by a US prosecutor to gain access to emails held on a Microsoft server in Ireland, without using existing treaty-based arrangements. The government of Ireland has intervened in the case on the side of Microsoft, arguing that it is illegal under Irish data protection law for Microsoft to provide the data to the US authorities without approval by the Irish courts. The case raises important issues regarding the trust individuals can place in the privacy protections of their own laws and courts. A number of US business associations have also filed briefs in the proceedings, arguing that law enforcement access requests place at risk much of the benefits promised by cloud computing.[13]

Although the role of courts, and particularly appellate courts, has been less evident in the context of security issues, some commentators see signs of new developments regarding liability in tort for cybersecurity breaches (Rosenzwieg, 2013). Where a security breach involves payment card data, card issuers have begun to look to the affected retailer to recover the costs of reissuing cards.[14] Government efforts to promote good practices, such as the Framework for Improving Critical Infrastructure Cybersecurity, released by the US National Institute of Standards and Technology in 2014, may provide a de facto standard for determining negligence in the event of a cyber incident (NIST, 2014).

Notes

1. For more information, see *www.privacylaws.com/Privacy-Officers-Network/*.
2. For more information, see *www.afcdp.net/*.
3. For more information, see *www.apep.es/*.
4. These guidelines are currently under review. For more information, see *http://oe.cd/security-guidelines-review*.
5. "No one nation can have full insight into the world's networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all. As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response – including between government and industry." (White House, 2011: 19)
6. "[C]oordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents" (ITU, 2010: 1)
7. The CNIL was notified of the breach, which happened due to a technical error by one of the phone company's providers, in April 2014. (All publicly available EU electronic communications services are obliged to report data breaches to the regulator.) In May, the CNIL carried out an inspection on Orange and its subcontractors, and found gaps in data security. According to the CNIL, the company claimed to have taken all necessary measures to fulfil its data security obligations, but had not conducted a sufficient security audit before using a certain technical solution for sending email campaigns.
8. For more details about the methodology, see Huston (2012, 2013).
9. Access maintains a compilation here: *www.accessnow.org/pages/transparency-reporting-index*.
10. The US Department of Justice authorised greater disclosures in January 2014, in response to a lawsuit brought by a number of Internet companies. President Obama called for still greater transparency in a February 2014 speech.
11. The first is called C-293/12 and C-594/12 Digital Rights Ireland. For more information see *http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=313440*.
12. The ruling is available at: *http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=152065&occ=first&dir=&cid=45442*.
13. Documentation and commentary about the case, including the legal briefs and opinions, are maintained at *www.digitialconstitution.com* (accessed 6 January 2015).
14. For more information see "In re: Target Corp. Customer data Security Breach Litigation", Memorandum and Order (US Dist. Ct. Minn.) (2 December 2014), *http://cdn.arstechnica.net/wp-content/uploads/2014/12/document3.pdf*.

References

Advisen (2014), *20% New Cyber Insurance Products Uptick in 2013*, Advisen, New York, *www.cyberrisknetwork.com/2014/01/31/new-cyber-insurance-products-20-percent-uptick-in-2013/* (accessed 25 April 2015).

Armerding, T. (2014), "Cyber insurance: Worth it, but beware of the exclusions", *CSO Online*, 20 August 2014, *www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html* (accessed 25 April 2015).

Bamberger, K. and D. Mulligan (2010), "Privacy on the Books and on the Ground", *Stanford Law Review*, Vol. 63/2, pp. 247-315.

Barrett, C. (2014), "Skills gap leaves UK vulnerable to cyber attack, says business", *Financial Times*, 6 August 2014, *www.ft.com/intl/cms/s/0/76b1eef4-1d3c-11e4-8b03-00144feabdc0.html#axzz3XOcYy48T* (accessed 15 April 2015).

BIS (2014), *Information Security Breaches Survey 2014: Technical Report*, UK Department for Business, Innovation and Skills, London, *www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf*.

CIGI (2014), *CIGI-Ipsos Global Survey on Internet Security and Trust*, Centre for International Governance Innovation, Waterloo, ON, *www.cigionline.org/internet-survey* (accessed 15 April 2015).

Cabinet Office of Japan (2014), "Policy Outline of the Institutional Revision for Utilization of Personal Data" Cabinet Office of Japan, Tokyo, *http://japan.kantei.go.jp/policy/it/20140715_2.pdf*.

Choe Sang-Hun (2014), "Theft of data fuels worries in South Korea", *New York Times*, 20 January 2014, *www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html?_r=1* (accessed 15 April 2015).

Clearwater, A. and J.T. Hughes (2013), "In the Beginning … An Early History of the Privacy Profession", *Ohio State Law Journal*, Vol. 74/6, pp. 897-921, *http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/8-Clearwater-Hughes.pdf*.

Coughlan, S. (2014), "Cyber-attacks increase leads to jobs boom", *BBC News*, *www.bbc.com/news/business-26647795* (accessed 15 April 2015).

DHS (2014), *Cybersecurity Insurance*, US Department of Homeland Security, Washington DC, *www.dhs.gov/publication/cybersecurity-insurance* (accessed 15 April 2015).

DPA (2013), *Implementing Measures with Regard to the Notification of Personal Data Breaches*, 4 April 2013, Italian Data Protection Authority, Rome, *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2414592* (accessed 15 April 2015).

EC (2015), *Special Eurobarometer 423: Cyber Security Report*, European Commission, Brussels, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf*.

EDPS (2014), Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition and Consumer Protection in the Digital Economy, European Data Protection Supervisor, Brussels, *https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf*.

ENISA (2014), *An Evaluation Framework for Cyber Security Strategies*, European Union Agency for Network and Information Security, Haraklion, Crete, *www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1* (accessed 15 April 2015).

ENISA (2013), *National Cyber Security Strategies in the World*, European Union Agency for Network and Information Security, Haraklion, Crete, *www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world* (accessed 15 April 2015).

FCC (2014), *FCC Joins Global Privacy Enforcement Network*, Press release, Federal Communications Commission, Washington DC, *www.fcc.gov/document/fcc-joins-global-privacy-enforcement-network* (accessed 15 April 2015).

Ferrillo, P. (2014), *Cyber Security, Cyber Governance, and Cyber Insurance*, Harvard Law School Forum on Corporate Governance and Financial Regulation, Cambridge, MA, *http://corpgov.law.harvard.edu/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/* (accessed 25 April 2015).

Google (2014), "European privacy requests for search removals", *Tranparency Report*, *www.google.com/transparencyreport/removals/europeprivacy/?hl=en* (accessed 15 April 2015).

Government of Australia (2014), *Cyber Security Review*, Government of Australia, Canberra, *www.pm.gov.au/media/2014-11-27/cyber-security-review-0* (accessed 15 April 2015).

Gray, A. (2014), "Cyber insurance market tempts new participants", *Financial Times*, 6 October 2014, *www.ft.com/intl/cms/s/0/69db580c-4d37-11e4-8f75-00144feab7de.html* (accessed 15 April 2015).

HM Government (2014), *Cyber Security Skills: Business Perspectives and Government's Next Steps*, HM Government, London, *www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf*.

Home Depot (2014), *The Home Depot Reports Findings in Payment Data Breach Investigation*, Press release, *https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf*.

Humber, Y. and G. Reidy (2014), "Japan takes its first step to fight hackers", *Bloomberg Business*, 24 July 2014, *www.bloomberg.com/bw/articles/2014-07-24/proposed-law-would-fix-japans-lax-cybersecurity* (accessed 15 April 2015).

Huston, G. (2013), "DNS, DNSSEC and Google's public DNS service", *CircleID* blog, 17 July 2013, *www.circleid.com/posts/20130717_dns_dnssec_and_googles_public_dns_service/* (accessed 15 April 2015).

Huston, G. (2012), "Counting DNSSEC", *RIPE Network Coordination Centre*, *https://labs.ripe.net/Members/gih/counting-dnssec* (accessed 15 April 2015).

IAPP (2014), "Benchmarking privacy management and investments of the Fortune 1000", *International Association of Privacy Professionals* (IAPP) website, *https://privacyassociation.org/resources/article/benchmarking-privacy-management-and-investments-of-the-fortune-1000-2/* (accessed 15 April 2015).

IAPP (2013), "IAPP Privacy Professionals Role, Function and Salary Survey", *International Association of Privacy Professionals* (IAPP) website, *https://privacyassociation.org/resources/article/2013-iapp-privacy-professionals-role-function-and-salary-survey* (accessed 15 April 2015).

(ISC)[2] (2011), *Annual Report 2010*, International Information Systems Security Certification Consortium, Palm Harbor, FL, *www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Annual_Reports/2010%20Annual%20Report.pdf*.

ITU (2010), Resolution 130: Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies, Plenipotentiary Conference of the International Telecommunication Union, Guadalajara, *www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf*.

Junker, J-C. (2014), *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change*, Strasbourg, *http://ec.europa.eu/priorities/docs/pg_en.pdf#page=6*.

Madden, M. (2014), "Few feel that the government or advertisers can be trusted", *Pew Research Center*, 12 November 2014, *www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/* (accessed 15 April 2015).

Marsh (2013), *Cyber Risks Explained: What They Are, What They Could Cost and How to Protect Against Them*, March & McLennan Companies, New York, *http://uk.marsh.com/Portals/18/Documents/Cyber_risk_client_briefing_FINAL_exp%20Apr13.pdf*.

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, MD, *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*.

NYMITY (2014), *Global Privacy Research Report 2014*, NYMITY, Toronto, ON, *www.nymity.com/innovations/privacy-research-2014-infographic/~/media/NymityAura/Resources/Research/Global-Privacy-Research-Report-2014.pdf*.

OAG California (2014), *California Data Breach Report 2014*, Office of the Attorney General, California Department of Justice, Sacramento, CA, *http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf*.

OAS (2014), "OAS begins supporting Suriname in the development of a national cyber security plan", Press release. Organization of American States, Washington DC, *www.oas.org/en/media_center/press_release.asp?sCodigo=E-555/14* (accessed 15 April 2015).

OECD (2015a), *Data Driven Innovation for Growth and Well-Being*, OECD Publishing, Paris.

OECD (2015b), *Improving the International Comparability of Statistics Produced by Computer Security Incident Response Team*, OECD Publishing, Paris.

OECD (2014), *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, DOI: 10.1787/9789264221796-en.

OECD (2013a), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, *http://oe.cd/privacy*.

OECD (2013b), *The OECD Privacy Framework*, OECD Publishing, Paris, *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*.

OECD (2012a), *Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online*, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5k4dq3rkb19n-en*.

OECD (2012b), *Internet Economy Outlook 2012*, OECD Publishing, Paris, *www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm*.

OECD (2012c), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5k8zq92vdgtl-en*.

OECD (2011a), *Recommendation on Principles for Internet Policy Making*, OECD, Paris, *www.oecd.org/sti/ieconomy/49258588.pdf*.

OECD (2011b), *Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, DOI: 10.1787/5kgdpm9wg9xs-en.

OECD (2007), *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, *www.oecd.org/sti/ieconomy/privacylawenforcementco-operation.htm* (accessed 15 April 2015).

OPC (2014a), *Joint Open Letter to App Marketplaces*, Office of the Privacy Commissioner of Canada, Ottawa, *www.priv.gc.ca/media/nr-c/2014/let_141210_e.asp* (accessed 15 April 2015).

OPC (2014b), *Global Cross Border Enforcement Cooperation Arrangement*, Office of the Privacy Commissioner of Canada, Ottawa, *www.privacyconference2014.org/media/16667/Enforcement-Cooperation-Agreement-adopted.pdf*.

OPC and ICO (2014), *Resolution on Enforcement Cooperation*, 36th International Conference of Data Protection and Privacy Commissioners, Office of the Privacy Commissioner of Canada, Ottawa, and Information Commissioner's Office, Wilmslow, UK, *www.privacyconference2014.org/media/16430/Resolution-International-cooperation.pdf*.

PHAEDRA (2014), *Workstream 1 Report: Co-ordination and Co-operation Between Data Protection Authorities*, PHAEDRA, *www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf*.

Ponemon Institute (2014), "2014 Cost of Data Breach Study", *www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/* (accessed 15 April 2015).

Rosenzweig, P. (2013), "When companies are hacked, customers bear the brunt. But not for long", *New Republic*, 15 October 2013, *www.newrepublic.com/article/115187/cybersecurity-liability-court-cases-are-changing-blame-game* (accessed 15 April 2015).

Science (2015), "The end of privacy", *Science*, Special Issue, 30 January 2015, *www.sciencemag.org/site/special/privacy/index.xhtml* (accessed 15 April 2015).

Segal, A. (2014), "China's new small leading group on cybersecurity and Internet management", *Forbes*, 27 February 2014, *www.forbes.com/sites/adamsegal/2014/02/27/chinas-new-small-leading-group-on-cybersecurity-and-internet-management/* (accessed 15 April 2015).

Somogyi, S. (2014), "Making end-to-end encryption easier to use", *Google Online Security Blog*, 3 June 2014, *http://googleonlinesecurity.blogspot.fr/2014/06/making-end-to-end-encryption-easier-to.html* (accessed 15 April 2015).

Taddicken, M. (2014), "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived societal relevance on different forms of self-disclosure", *Journal of Computer-Mediated Communication*, Vol. 19, pp. 248-273. DOI: 10.111/jcc4.12052.

Tene, O. (2015), "Privacy is the New Antitrust: Launching the FTC Casebook", *International Association of Privacy Professionals* (IAPP) website, 15 January 2015, *https://privacyassociation.org/news/a/privacy-is-the-new-antitrust-launching-the-ftc-casebook/* (accessed 15 April 2015).

UN (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations, New York, *www.un.org/ga/search/view_doc.asp?symbol=A/68/98* (accessed 24 April 2014).

US DoJ (2014), "U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator", US Department of Justice, Washington DC, *www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware* (accessed 15 April 2015).

US GAO (2015), *High Risk List*, US Government Accountability Office, Washington DC, *www.gao.gov/highrisk/overview* (accessed 15 April 2015).

Ustaran, E. (2014), "The judiciary v. the surveillance society", *LinkedIn* blog, 15 December 2014, *www.linkedin.com/pulse/judiciary-v-surveillance-eduardo-ustaran?trk=object-title* (accessed 15 April 2015).

Vodaphone (2014), *Sustainability Report 2013/14*, Vodaphone, Newbury, UK, *www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf*.

White House (2015), "State of the Union Address", White House, Washington DC, *www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015* (accessed 15 April 2015).

White House (2011), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, White House, Washington DC, *www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*.

© OECD 2015

Chapter 6

Emerging issues: The Internet of Things

This chapter explores convergence between ICTs and the economy on a grand scale, otherwise known as the Internet of Things (IoT). The term implies the connection of most devices and objects over time to a network of networks. It encompasses developments in machine-to-machine communication, the cloud, big data and sensors, actuators and people. This convergence will lead to machine learning, remote control and eventually autonomous machines and systems. Estimates indicate that potentially 50 billion devices could be connected by 2020, but challenges remain in gathering concrete and accurate data on the widespread use of IoT technology, now and in the future. Adoption will depend to a large extent on the capacity of governments to create an adequate regulatory framework in key areas including telecommunication, privacy and consumer policy.

Policy makers and regulators have taken a keen interest in convergence between fixed and mobile networks, and between telecommunications and broadcasting. They now recognize that the Internet of Things (IoT) represents the next step in convergence between ICTs and the economy on an unprecedented scale. The term IoT implies the connection of most devices and objects over time to the Internet's network of networks. Other terms used to describe this process include the "Internet of Everything", the "Industrial Internet" and "Machine-to-Machine (M2M) communication". The term "Internet of Everything" is increasingly accepted as the most accurate because Internet-connected sensors and actuators[1] will not only link to things, but will also monitor the health, location and activities of people and animals, the state of the natural environment, the quality of food and much else besides.

The Internet of Things has profound implications for all aspects and sectors of the economy, including industrial and commercial processes, consumer and home services, energy, transport systems, health care, infotainment and public services. Embedding devices with limited processor, memory and power resources opens up applications everywhere. For example, data could be gathered in buildings, factories and natural ecosystems with applications in urban planning, manufacturing and environmental monitoring. The end result will be combined with the cloud, big data and machine learning to produce autonomous machines and intelligent systems. This section of the *Digital Economy Outlook* investigates how increasing adoption of the IoT will be facilitated or hampered by differing policy and regulatory approaches. In the area of communication, issues range from management of spectrum and numbering through to practices around SIM cards. Broader issues include privacy, security, and consumer protection and empowerment.

6.1 The Internet of Things: Developments, definition and main elements

Visions of smart, communicating objects are not new and existed well before the Internet became a reality 45 years ago.[2] By the early 1990s, ideas about pervasive computing and embodied virtuality were well advanced. For example, at Xerox PARC they imagined that "specialised elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence" (see Weiser, 1991). In spite of this, manufacturers of smart consumer products remain uncertain as to which features will most attract consumers and whether demand exists for some devices to be connected at all (Harwell, 2014).

Predictions regarding the significance of the IoT have also met with scepticism, based in part on the rate of take up of Radio Frequency Identification (RFID), which is slower than anticipated a decade ago. The limited use of RFID is largely the result of a lack of standards, a lack of security and the relatively high cost of both RFID readers and tags.[3] However, the widespread availability of smartphones with near field communication (NFC) capabilities, which allow communication when the device is in close proximity, may help to overcome this hurdle. The passive RFID tag market is now experiencing significant growth, albeit

a decade later than expected, with the majority of growth based on retailer adoption of RFID for shelf-level stock replenishment (Das and Harrop, 2014). Widespread availability of smartphones implies benefits not only for supply chain management, but also for interactions between retailers and customers in stores, for example. The capabilities of smartphones, from NFC to low-energy Bluetooth, and their pervasive adoption within a very short timeframe, mean that devices to read and interact with the IoT are now available at scale for the first time.

Smartphones have brought the IoT to the consumer and function increasingly as a hub linking other devices to the wider network (Yared, 2013), including a number of consumer electrical appliances (Box 6.1). Firms such as Philips and General Electric produce light bulbs that can be controlled over the Internet, while television, radio, sound speakers and telephones can all be purchased with built-in Internet connectivity. Domestic appliances such as ovens, washing machines and refrigerators increasingly come with built-in Internet connectivity, and in 2013-14 major brands such as General Electric, Philips, Samsung and Whirlpool introduced Internet-connected home appliances to the market in wider ranges and larger quantities, first in North America, and then in Europe and Asia. An increasing amount of sporting goods, ranging from equipment for golf to basketball, can also be linked

Box 6.1. **The smartphone as the hub to the Internet of Things**

Smartphones play a prominent role in consumer use of the IoT. Internet-connected smart watches, fitness bracelets, running shoes and heart rate monitors are just some of the products consumers can buy and link to the Internet via their smartphone, enabling them to interact with other users or monitor their own fitness levels. Nearly all IoT-connected products come with an interactive smartphone app.

The development of smartphones and tablets has created an entirely new environment for user interfaces. Historically, user interfaces for all kinds of devices and appliances were limited to LED lights and knobs, which limited how devices could be programmed. Not adding too many functions and keeping the interface simple were among the main requirements. The difficulty experienced by many people in programming their video-cassette recorder is a prime example of the challenges involved in developing such interfaces. The smartphone screen interface now allows formerly difficult choices to be made with relative ease. Search and help functions can further support users in ways that were previously impossible. Smartphones not only make possible more flexible user interfaces, they also allow users to customise them.

The development of smartphones has had tremendous implications for the cost of components needed to make IoT devices. The scale of smartphone production is measured in billions of units, which means that sensors such as GPS, magnetormeters, barometer gyroscopes and cameras also have to be produced in these quantities. As a result, sensors have become smaller and cheaper, which has promoted their use in other products such as toys, remote-controlled helicopters, home weather stations and many other devices. The same trend is visible in screens and communication chips, where smaller screens of low quality have been replaced by higher quality versions, leading to widespread installation in point-of-sale terminals and other devices. The virtual reality glasses “Oculus Rift”, for example, are built using the highest quality smartphone screens available. High-quality screens are also now being fitted into smart watches, thermostats, vehicles and energy consumption appliances.

to the Internet. The International Tennis Federation has already certified an Internet-connected tennis racquet readily available on the market for competition play (Kelly, 2014). The racquet allows tennis players to analyse their game and work on elements such as perfecting their swing.

The above examples monitor people for recreational purposes, however, the first line of certified health-related monitors are now becoming available on the market. In addition, the IoT is increasingly attracting developers. An increasing number of crowdfunded projects on the Kickstarter website have an IoT component, such as Internet-connected locks, sensor tags and lightbulbs (Table 6.1). The entrepreneurs behind these projects ask the general public to fund development by pre-financing their development and production. Funders do not get equity in the company, but do generally buy the finished product or receive promotional material, depending on the level of funding they provide. Kickstarter, as one of the leading platforms for crowdfunding, can provide an interesting indicator of areas being targeted by innovators.

Table 6.1. **A selection of IoT-related projects from Kickstarter**

Name	Description	More information	Funding pledged (USD)
EasyTouch: Turn your world into a touch sensor	EasyTouch is the world's easiest to use capacitive touch sensor. Turn bananas, pencil drawings, water or fabric into a touch button.	*www.kickstarter.com/projects/54060271/easytouch-turn-your-world-into-a-touch-sensor?ref=category*	13 023
Ambi Climate: The smart add-on for your air Conditioner	Ambi Climate learns about your habits and home environment. Auto adjusts AC for ideal temperature and energy savings. Remote access via Android/iPhone.	*www.kickstarter.com/projects/ambi-labs/ambi-climate-the-smart-add-on-for-your-air-conditi*	94 865
Digitsole: The first interactive insole to heat your feet	Digitsole is the first connected insole on the market controlled via your smartphone – warm your feet, track your distance and calories.	*www.kickstarter.com/projects/1308642275/digitsole-the-first-interactive-insole-to-heat-you?play=video_pitch&ref=home_featured*	90 074
Prizm: Turn your speakers into a learning music player	Prizm is a learning device that instantly plays the perfect music on your speakers, based on people in the room and the context.	*www.kickstarter.com/projects/prizm/prizm-turn-your-speakers-into-a-learning-music-pla?ref=category*	105 594
Notti: A more beautiful smart light	This beautifully designed app-controlled light provides highly customised visual notifications and other useful info from your phone.	*www.kickstarter.com/projects/26398080/notti-a-more-beautiful-smart-light?ref=category*	44 727
PLAYBULB color: Smart Color Light and Wireless Speaker 2-in-1	PLAYBULB color is a smart colour LED speaker light bulb with the PLAYBULB X free App. Let colour and music fill up your living space.	*www.kickstarter.com/projects/mipowusa/playbulb-color-smart-color-light-and-wireless-spea?ref=category*	37 446

Source: Kickstarter, 3 November 2014. *www.kickstarter.com*

Defining the Internet of Things

A definition of the IoT is not a simple matter. A previous OECD report on M2M communication found that the term was associated mainly with applications involving RFID (OECD, 2012a). RFID makes use of so-called tags – tiny chips with antennae that transmit data when they come into contact with an electromagnetic field. These are known as passive communication devices, in contrast to active devices that transmit when they have access to a power source, such as a battery. The term "M2M" was used for:

> *Devices that are actively communicating using wired and wireless networks, that are not computers in the traditional sense and are using the Internet in some form or another. M2M communication is only one element of smart meters, cities and lighting. It is when it is combined with the logic of cloud services, remote operation and interaction that these types of applications become "smart". RFID can be another element of a smarter environment that can be used in conjunction with M2M communication and cloud services (OECD, 2012a).*

Since 2011, however, the term "M2M" has lost some of its significance and the term "IoT" has gained prominence for a wide variety of developments where "things" are connected to the Internet. The IoT consists of several elements, such as the cloud, big data, machine-to-machine communication, sensors and actuators, covered later in the chapter. As noted earlier, a more accurate term would be the "Internet of Everything"; however, this term has yet to find common currency and may not be widely used in the future.

The IoT in its purest definition would be limited to objects able to communicate via the Internet. This definition, however, has a number of drawbacks: it is limited to things, does not consider effects and does not consider emerging properties. To start with, by definition, everything that is directly connected to the Internet has to be a thing. People cannot communicate via the Internet except through the mediation of a thing. As such the Internet of *things* would be a misnomer, because all Internet connections occur between things. Many definitions, however, explicitly exclude person-operated/controlled devices, such as smartphones, tablets and other computers. For example, a washing machine that communicates with a smartphone app is it not considered to be part of the IoT because it is operated by a person. This can have practical implications. In Brazil, for example, M2M communication between devices is excluded from certain taxes if the communication occurs without human intervention for the purpose of monitoring, measuring and controlling the device.[4] Given that smartphones and tablets function as the main operating devices for much of the IoT, this definition could prove too narrow. For example, health-monitoring devices such as sports heart rate meters and step counters could fall outside the definition, because they may require a smartphone as a platform in order to function.[5]

Defining the IoT becomes even more challenging when taking into account impact. For example, sensors can be used to ascertain whether a car is parked on a parking spot, but modern vehicles with on-board parking cameras and sensors can also determine the location and size of an empty parking spot just by driving by. This information allows the creation of a real-time overview of city parking spaces, without the need for road-embedded sensors. For users, the parking spots appear to be linked to the Internet. But can a parking spot can be defined as a thing?

When multiple sensors are integrated into systems such as a vehicle, it may prove difficult to state accurately the exact number of things connected to the Internet. Some calculations consider sensors and actuators as individual things, however a vehicle may contain between 30 to 200 different sensors. Should the vehicle be seen as the thing or individual sensors? Furthermore, emergent properties develop from combining different sensors and actuators. In other words, sensors may be repurposed or extended in functionality over time. A smart thermostat may have a motion sensor, which can be repurposed/extended to also act as a light switch or as an element in a burglar alarm. A homeowner may not have bought a burglar alarm, but the combination of sensors, actuators and software in the home could result in the creation of an alarm system.

The other element of the definition – when something is part of the Internet – is equally difficult. According to some definitions, an Internet-connected thing must be capable of operating in an IP communications stack. This would exclude devices such as RFID tags, Bluetooth-enabled devices and connected light bulbs, which can only connect to the Internet through a gateway that acts as a mediator between the device and the Internet. For this report, such devices are considered part of the IoT. Therefore, if a light bulb does

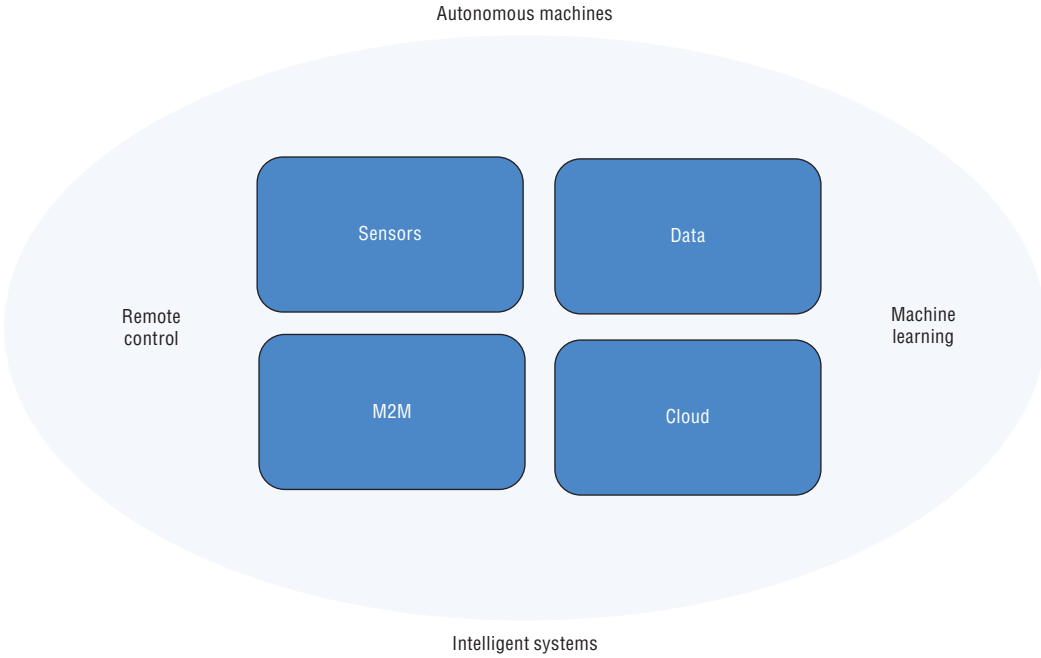
not support the IP protocol but can be addressed via an Internet-connected gateway, it is considered to be Internet connected. The same is true for RFID tags, fitness monitoring bracelets or connected shoes.

This chapter therefore defines the IoT in broad terms including all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, often considered to be part of the "traditional Internet". However, these devices are integral to operating, reading and analysing the state of IoT devices and frequently constitute the "heart and brains" of the system. As such, it would not be correct to exclude them.

The main enablers of the Internet of Things

The evolution of the IoT is underpinned by four main trends in ICT development – big data, the cloud, M2M communication and sensors (Figure 6.1). The combination of cloud computing and big data analytics leads to improved machine learning applications, operating at a new level of artificial intelligence. This combination also leads to further developments in machine learning and remote control. The latter still requires human interaction, but the machine takes care of all main operational functions with human interaction limited to specific actions. Remote-controlled machines and systems combined with machine learning will ultimately lead to autonomous machines and intelligent systems, in particular robotic machines.

Figure 6.1. **Main enablers of the Internet of Things**



A previous OECD report analysed the contribution of sensors and actuators to "Green Growth" (OECD, 2010: 227-256). It stated that sensors can measure multiple physical properties and may include electronic sensors, biosensors and chemical sensors. These sensors can be regarded as "the interface between the physical world and the world of electrical devices, such as computers" (Wilson, 2008). Conversely, actuators function by

converting an electrical signal into a physical phenomenon. Examples include displays for speedometers and thermostats (the data for which is measured by sensors), as well as those that control the motion of machines.

Early sensor and actuator systems such as vehicle engines measured, processed, acted upon and discarded data. Today, generated data are increasingly communicated to other machines and central computers and stored for further correlation and analysis. The data may be communicated via a variety of means – wired and wireless, short or long range, low or high power, low or high bandwidth. Two OECD reports, *Machine-to-Machine communications: connecting billions of devices* (2012a) and *The building blocks for smart networks* (2013a), discuss many of these options.

Communication between sensors controlled by central processing units has allowed machines to become more aware of their surroundings and has stimulated the development of new actuators that execute an increasing range of functions. As a result, remote operation has become possible in ways that were previously unfeasible, where the machine undertakes the majority of tasks and human interaction is limited. In mining, for example, one remote operator can now manage multiple ore transporters.

Big data, data analytics and cloud computing

Collecting, compiling, linking and analysing very large data flows in real time requires powerful, new analytical techniques and data-sharing models to handle the size and complexity of the necessary data-processing operations. The availability of new techniques and the associated shift in organisation of these operations signal a change towards a data-driven or data-centric socio-economic model commonly discussed under the umbrella term "big data" (Box 6.2). In such a data-driven world, data are a core asset which constitute a vital resource for innovation, new industries and applications, and competitive advantage. The rapid decline in the cost of analytics, including computing power and data storage, as well as the continued expansion of broadband has brought such data increasingly within reach. Storage costs, for example, have decreased to the point where data can generally be kept for long periods of time, if not indefinitely.

Big data is particularly well suited to solutions that favour massively parallel processing (MPP). The data are sliced into smaller units and processed, and the various results are later combined. This is different from traditional computing, where faster processors and memory deliver the required speed increases. Systems that support MPP are essentially large numbers of servers, linked by a common network and a software stack that treats the servers as a common pool for processing and storage. Cloud computing is defined "as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort" (OECD, 2013b).

Sensors, M2M communication and cloud computing generate a vast amount of data, the statistical analysis of which is of enormous value to science, business and consumers. However, big data, M2M and cloud computing also underpin a whole new era of machine learning, otherwise known as artificial intelligence. Previously considered a failed dream of the early age of computing, artificial intelligence has made a comeback through the inclusion of Bayesian statistical analysis. This uses probability distributions based on prior experiences, instead of a priori models, with new tools, better described by the term "machine learning".[6]

Box 6.2. **The difficulty of defining "big data" beyond volume, velocity and variety**

A clear definition of "big data" remains elusive. Initially, the term referred to data sets for which volume became an issue in terms of data management and processing. However, the emphasis on volume alone can be misleading, whether measured in gigabytes, petabytes (millions of gigabytes) or exabytes (billions of gigabytes). In some cases, volume is less relevant than the number of readings, the way the data are used and the resulting complexity. For example, managing a day's worth of data from thousands of sensors in almost real time poses a greater challenge than managing a video collection of equivalent size in bytes. This distinction is captured by the "3Vs" definition of big data, which highlights three main characteristics:

- The **volume** of data as covered by most definitions today (see Loukides, 2010; MGI, 2011; and also McGuire et al., 2012, cited in OECD, 2013c);
- The **variety** of data, which refers to mostly unstructured data sets from sources as diverse as web logs, social media, mobile communications, sensors and financial transactions. Variety also goes hand in hand with the capability to link these diverse data sets;
- The **velocity** or speed at which data are generated, accessed, processed and analysed. Real-time monitoring and real-time "nowcasting" are often listed as benefits that accompany the velocity of "big data".

However, the 3Vs and other similar definitions describe technical properties that depend on the evolving state of the art in data storage and processing, and as such are in continuous flux. Furthermore, these definitions imply that the sole element in big data is data. While this is true for volume, both variety and velocity are based primarily on data analytics – the capacity to process and analyse unstructured diverse data in (close to) real-time. Furthermore, the term "big data" does not indicate how the data are used, the types of innovation they can precipitate, or how they relate to other concepts such as "open data", "linked data", "data mashups" and so on. For these reasons, the OECD KBC2: DATA project has chosen to focus not on the concept "big data", but rather on "data-driven innovation", which is based on the *use of data and analytics to innovate* for growth and well-being.

Source: OECD, 2013c.

The combination of machine learning and remote-controlled machines, such as vehicles, can result in autonomous machines and intelligent systems, able to operate without a human controller. Instead, the machines are controlled either internally or remotely through a computer located elsewhere. The machines and the intelligent system they form part of use a combination of big data analysis, cloud computing, M2M communication, and sensors and actuators, to operate and learn.

Traditionally, robots are used mostly in industries where their speed, precision, dexterity and ability to work in hazardous conditions are valued. However, these capabilities required very precisely defined environments and setting up a robotic plant can take months, if not years, to plan all robotic movements down to the millimetre. This situation is now evolving due to the combination of sensors, machine learning and cloud computing. The IoT allows robots to become more flexible and enables them to learn. Current examples of such developments include fully robotic warehouses that only require people to oversee the robots and load and unload trucks.

The move towards intelligent systems that are not limited to controlled environments, such as factories, but interact with non-technological environments, is still some way off, but is already visible in the area of transport. Many industry experts believe that practical application of these systems will follow quickly, once the technical obstacles are overcome. It remains unclear whether autonomous vehicles will eventually be a common sight on the roads, but industry estimates place implementation at about a decade away. The main benefits foreseen for autonomous vehicles are hard to evaluate at the current time, but a number of advantages present themselves:

- **Utilisation**. Most vehicles are not presently used for the majority of their lifetime. Autonomous vehicles might increase the utilisation of vehicles, for example, through subscription models.
- **Energy efficiency**. Significant energy is used and lost during acceleration and deceleration. Machines would be able to better balance acceleration and deceleration. In addition, autonomous vehicles would be lighter, according to some predictions, due to lower requirements for on-board safety components.
- **Safety**. With millisecond reaction times and communication between vehicles, autonomous vehicles might deal better with sudden changes in situations with greater awareness of dangerous situations ahead.
- **Empowerment**. Industry and academics believe that autonomous vehicles will cost less to own and operate and require less or no skill from the occupant (Lee, 2015).[7] This could provide an alternative to public transport for a larger group of people (e.g. elderly people or those with physical disabilities).

Much of the IoT concentrates in cities and many IoT applications will be useful for urban life, governance, planning, and the management of urban infrastructures and services. For example, intelligent transport systems or smart homes and electricity grids will enable those living in or around cities to save time, energy and money. City governments will have access to increasing amounts of data to plan and invest more wisely and to manage transport, energy, waste and water systems more efficiently. Cities will also foster and benefit from interaction between connected things, machines and systems in areas that have hitherto functioned largely in isolation. For example, synergies could be achieved by connecting water, energy, transport and waste systems with a view to promoting resource reuse and eliminating excess capacity and redundancies in each system. However, interoperability across devices, machines and systems will be essential to optimise the potential of the IoT to transform cities, and technologies, standards, protocols and rules will need to be harmonised across sectors.

6.2 Technical developments in the Internet of Things

The Internet of Things relies upon connectivity with devices and sensors. The different types of connectivity can be described based on the geographic dispersion and geographic mobility they support (Figure 6.2). The higher the geographic dispersion and mobility the application demands, the greater the energy use needed to sustain the application, and the larger the antenna required (if the device is wireless). Energy use and antenna size in turn define the *form factor* (i.e. the size, configuration or physical arrangement of a computer hardware object) and device applications. The smallest sensors and actuators are those that either harvest electromagnetic energy through their wireless circuitry, such as RFID tags, or are connected with a wire to a power source and communications network. Developments

in battery technology unfortunately are linear compared to the exponential advancements in integrated circuits, where increasingly smaller sizes and advances in capabilities are traded off against greater energy use.

Figure 6.2. **Machine-to-machine applications and technologies by dispersion and mobility**

	Geographically fixed	Geographically mobile
Geographically dispersed	**Application:** Smart grid, smart meter and smart city, remote monitoring **Technology required:** PSTN, broadband, 2G/3G/4G, power line communication	**Application:** Car automation, eHealth, logistics, portable consumer electronics **Technology required:** 2G/3G/4G, satellite
Geographically concentrated	**Application:** Smart home, factory automation, eHealth **Technology required:** Wireless personal area networks (WPAN), wired networks, indoor electrical wiring, Wi-Fi, RFID, Near Field Communication	**Application:** On-site logistics **Technology required:** Wi-Fi, WPAN

Short range and home networks

Both wired and wireless networks are essential for the IoT. Wired networks provide capacity, but are inflexible in their location. Wireless networks allow for flexibility in location and motion, but are often limited by bandwidth and energy. Wired networks use standard networking technologies such as Ethernet (for in-company and fibre networks), GPON (for fibre networks), DSL (for public telephony networks) and Docsis (for cable networks). Although some standards exist for Power-line communication, and Power over Ethernet is commonly used in businesses for VoIP phones and other equipment, there has been little development in wired protocols for the IoT. Existing standards are often applicable for situations where a wired connection can be used.[8]

The least mature and, therefore, the most rapidly changing area is short-range wireless standards in the home and factory (lower left corner of Figure 6.2). Technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Zigbee, 6LowPan, Bluetooth and Wi-Fi, in order of complexity, have all been advanced as global standards, and each has its own niche. RFID technology is a one-way communication protocol that allows small chips (tags) to broadcast their location. In 2003, when Walmart announced that it would require its top suppliers to use RFID for all pallets and cases, it appeared that RFID was set for a big future in retailing. Many analysts predicted that every milk carton would soon carry an RFID tag and a refrigerator would be able to scan and provide an inventory of its contents. Some analysts predicted that within a decade 100 billion tags would be used each year. This has not become a reality, in part because the price of tags has not decreased sufficiently, but also because radio frequencies do not easily penetrate packaging made from tin foil or products that consist (partially) of liquids. Therefore, RFIDs have found only limited use in high-volume, low-margin and fast-moving consumables.

By 2014, the RFID market had matured with RFID tags used increasingly in clothing and apparel stores. The benefit of RFID here lies in the ability to scan a stack of clothing and know whether particular sizes are still available or need to be replenished from storage. This reduces the time spent by customers waiting for employees to locate particular sizes in a stack. In addition, RFID is used in aerospace and manufacturing to track the location of

parts and tools, and to ascertain whether the correct part has been used and its exact age. In health care, RFID is used to track goods, medicine and patients, as well as hand-washing hygiene by staff. The use of RFID-controlled soap dispensers has increased the use of soap in hospitals and decreased the amount of infections. In transport, single-use or multi-day tickets are embedded with RFID tags. RFIDs are also used in livestock identification to comply with government requirements regarding the traceability of animals throughout their lives. One analyst company estimates that 5.8 billion tags were sold in 2013 and predicted a rise to 6.9 billion in 2014 (Das and Harrop, 2014).

NFC is a two-way technology developed for interaction, for example, when making payments or entering a facility. Operation requires two NFC-equipped devices to be in very close proximity to each other. NFC is integrated into swipe cards for building access and public transport (e.g. the Parisian *Navigo*, London's *Oyster* card and Japan's *Suica* card). Its use is currently being expanded to contactless payments, with more and more banks introducing credit and debit cards with NFC. With the introduction of Apple's iPhone 6, all major smartphone platforms now support NFC. At the same time, some public transport cards, such as Seoul's *T-card* and Japan's *Suica* card, can be used for payments of groceries, snacks, taxis and other purchases.

The main challenges of NFC concern standardisation. Most systems that use NFC are so-called closed-loop systems. This means that only cards issued by the organisation can be used for the types of transactions it authorises. This limits usage. For example, a public transport authority will only accept transport cards it has issued, but not cards from neighbouring regions or bank cards (the Parisian *Navigo* system cannot be used outside central France). An open-loop system allows customers to use cards issued by other organisations, such as other public transport authorities, banks and mobile phone vendors. The main obstacle to standardisation is willingness among organisations to open access to what they see as their customers. It is difficult to introduce a system that works only when a customer uses bank Q, public transport organisation X and smartphone brand Y provided by mobile operator Z. Such an overlap covers only a small demographic. Many early NFC trials failed because they were limited to one bank and one mobile operator.

Interest in open-loop systems is now increasing. Starting from September 2014, Transport for London began supporting payments through smartphones via "Cash on Tap" from EE and Vodafone Smartpass. The use of a prepaid debit or credit card means that only the co-operation of the bank/credit card company is needed.[9] The Transport for London system has proven popular with 5% of trips being paid through the open-loop card system within the first week of launch. One problem with open-loop systems, however, is the potential for "card clash", which can occur when multiple cards may be used to perform actions such as transport payments. If a user's wallet touches a gate, the system may deduct payment from each card it detects.

Smartphones have also brought NFC technology to other applications. For example, pairing a smartphone with a wireless speaker can be achieved by tapping the phone on the speaker. This functionality is integrated into many Android phones and most Bluetooth wireless speakers and headphones, and is now expanding to keyboards, printers, televisions and other devices. It allows the user to pair devices without needing to know or understand the underlying wireless technologies (Wi-Fi/Bluetooth), and to establish authentication without knowing the keys for the devices. NFC stickers allow users to enable their phones to change configuration automatically when the sticker is tapped, for example, when the phone is docked in a vehicle.

Bluetooth was initially designed as a wireless personal area network (WPA) to connect peripheral devices, such as headsets and keyboards, at short range to mobile phones and computers. Over 90% of phones, tablets and laptops have Bluetooth capabilities, and some vehicles. Compared to NFC it is a higher bandwidth longer range technology, working up to 10-20 metres in a star topology with a central controller, where all devices connect to each other.[10] The latest version is Bluetooth 4.0; however ongoing development for Bluetooth 4.1 is expected to introduce mesh-networking and IPv6. This would allow devices to connect directly to each other and via IPv6 to the Internet, instead of via a central controller. This would make Bluetooth a direct competitor to IEEE 802.15.4-based networks (discussed below).

Bluetooth 4.0 has expanded its IoT capabilities through support for low-energy profiles. This has sparked innovation around a number of low-energy sensors and tags, such as Apple's iBeacon and competing standards. A number of uses have been identified in the home, including sensors that combine temperature, movement, position and other capabilities. These can be used to locate objects such as car keys, but also to signal whether a (liquor or gun) cupboard or window has been opened. Bluetooth has also found uses outside the home, for example, in shops and malls. In the airports of Amsterdam and Miami, Bluetooth beacons guide smartphone owners to the correct gate via a dedicated app. SITA (an organisation specializing in IT and communications solutions for airports) maintains an open index which allows airports to register their beacons and app-makers to interact and develop services.[11] In a few years it may be commonplace for airlines to use beacons to locate passengers and for travellers to find their plane using tags. Beacons with relevant information can be placed at any location, such as a bus stop, and accessed via a smartphone. On a similar note, Microsoft has designed a headset that conveys information vocally for use by the visually impaired among other users.

IEEE 802.15.4 (Low Rate Wireless Personal Area Network) is a networking standard that distinguishes itself by supporting both star topology and mesh topology networking for low power applications. It is designed to use very little power enabling it to work for years in battery-operated situations, even when a device is in sleep mode. It is limited to 250 Kbit/s, which makes it ideal for IoT applications in the home and industrial settings. IEEE 802.15.4 specifies how devices broadcast and connect, but not some of their higher-level interactions which are necessary to allow devices to interact in a meaningful way.[12] A number of other standards both open and proprietary are built on top of IEEE 802.15.4, including WirelessHart, MiWi, ISA100.11A, Zigbee and Thread, each of which addresses different usage cases. IEEE 802.15.4, however, does not work well with a standard IP stack, which has prompted the Internet Engineering Task Force (IETF) to develop the 6LowPan standard to enable native IPv6.[13] The difficulty lies in the packet size, which for IEEE 802.15.4 is too small to hold a standard IP packet, and the energy consumption associated with the Internet's always-on assumption. Unlike Bluetooth, however, 802.15.4 is rarely supported on mobile phones, tablets and laptops, and therefore needs a dedicated gateway to function.

Zigbee is the most well-known standard to make use of IEEE 802.15.4. However, a number of incompatible implementations of Zigbee exist on the market, which has slowed adoption. Zigbee can be found in light bulbs by GE and Philips and Comcast's new set-top box. Most variants of Zigbee do not support IP-based networking natively, although some do. One reason for lack of native support for IP is the power requirements. For example, Zigbee Green Power allows the use of Zigbee networking in devices that have no permanent power source, such as a battery or other electrical connection. Instead, these devices can harvest energy from motion, such as by pressing a light switch.

In 2014, Google Nest, Samsung, ARM and a number of other companies announced "Thread", a standard for in and around the home, launched as an alternative to Zigbee. Thread makes use of 802.15.4 and comes with native 6LowPan support. While incompatible with Zigbee, it is designed in such a way that the same chips and radios can be used. Whether it will be successful remains to be seen.

A number of alternative proprietary technologies to IEEE 802.15.4-based technologies exist, such as ANT, Peanut and Z-Wave. Of these, Z-Wave is the most widely implemented. GE, for example, offers a wide range of Z-Wave-based products. As proprietary technologies, they are controlled by a company or group of companies, unlike open standards which allow everyone to make use of the standard (under certain conditions). A limited number of vendors provide the chips and radios, although more vendors may be building packages around the technology.

Wi-Fi (IEEE 802.11x) is the final networking protocol in this quadrant that deserves attention. It forms the basis for a great many IoT devices in and around a home, with almost every ISP supplying its customers with a modem/switch with Wi-Fi on board. Despite using unlicensed spectrum, Wi-Fi has become the preferred way for many consumers to connect to the Internet. It was optimised for use by computers in local area networks and as a result can attain speeds of up to 1 Gbit/s, instead of prioritising energy efficiency, as does IEEE 802.15.4.[14] This makes Wi-Fi the technology of choice for higher bandwidth and low latency applications, such as voice and video applications. As a result, Wi-Fi requires more energy and does not support battery-operated technologies well. Wi-Fi is therefore used to connect all kinds of devices that are (regularly) connected to the mains supply.

Short-range networking technologies are the most contentious area for networking the IoT, as the conflicting requirements of technologies make it hard to predict a winner. Where a technology needs to work for years on a single charge, IEEE 802.15.4 or Bluetooth-based technologies win out. Where high speeds are needed, Wi-Fi is a likely choice. However, no matter what technology is chosen, a trade-off needs to be made. A possible solution is for some manufacturers to put multiple networking technologies in some of their chipsets aimed at IoT solutions. This might increase the costs of the chipsets, but also increase the flexibility with which they can be deployed, and potentially avoid lock-in.

Long-range and mobile networks

For geographically dispersed networks wired options are only viable in locations where wired connectivity is already present, or for certain organisations such as those managing roads and railroads as part of an overall infrastructure. For others, the costs associated with the civil works necessary often make wiring remote locations too expensive. For this reason the use of mobile wireless networks is essential to the IoT for geographically dispersed IoT applications. Whether used to control traffic lights or remotely monitoring pumps or vehicles, the only cost-effective way to connect them is through wireless networks.

2G/3G/4G networks, as developed by the 3GPP2, are the primary networks for the deployment of the IoT:

- 2G (GSM) networks offer worldwide coverage, both indoors and outdoors, and as such are considered future proof. Some mobile operators plan to retire their 2G networks (e.g. AT&T in 2017), but their coverage is often superior to that of 3G and 4G networks and the installed GSM base is so large, particularly in Europe, that retirement will prove challenging.

- 3G (UMTS/HSDPA) is considered by some in the industry to be less useful because it makes use primarily of the 2 100 Mhz band, which does not offer good indoor coverage. Nevertheless, some countries use 3G in other bands and some M2M modules support 3G.
- 4G networks are increasingly prized because of their potential for use in a wide range of frequencies, including below 1 GHz, and their high throughput and low latency. 4G networks can also work in bands that currently support 2G and 3G. 4G IoT modules are still considered expensive, although prices are decreasing. Analysts predict that by 2022, 70% of M2M modules for M2M applications will use 4G. However, this would still leave 30% of the market based on 2G modules. Given the 10 to 20-year lifespan of M2M, this effectively means that 2G networks would need to remain operational well after 2030 (Connected World, 2014).
- There are, however, drawbacks to using 2G/3G/4G networks for large-scale IoT roll outs. The primary obstacle is SIM card lock-in. It is difficult if not impossible to switch mobile operators during the lifetime of the device, as any change in operator requires the physical replacement of the SIM card, which locks the device to a single operator. This hinders competition. In addition, it creates difficulties in achieving coverage, because even in dense cities no one network can claim full (indoor) coverage. If competitors' networks cover a location, then large-scale users may opt to use multiple networks at the same time. Moreover, mobile networks are not static and change their operating characteristics based on demands from network load and operations such as maintenance. Research in Norway has shown that up to 20% of devices are offline for at least 10 minutes a day, even in dense cities, without counting major network failures (Kvalbein, 2012).[15] In addition, some sites may face congestion during busy hours. This may not be a problem for smart electricity meters, which can reschedule data shipments, but it does pose a problem for recharging an electric vehicle, traffic lights and payment terminals that require direct interaction. Some have suggested that additional quality-of-service mechanisms are necessary to deal with the best-effort nature of the Internet, in order to support critical IoT applications such as autonomous vehicles or eHealth. However, others argue that the inherent unreliability of the underlying network and the inability of higher networking protocols, such as IP, to effect change, calls for a more fundamental approach. This would involve making applications more resilient and allowing the fast switching of the underlying network using operator-independent SIM cards. In addition, international mobile roaming, though well supported, is expensive and no mobile network operator or alliance of operators has a wide enough footprint to offer good coverage and rates for some customer requirements.

One option is for governments to change regulations to allow private companies (not public telecommunication networks) to hold the numbers necessary for use in mobile networks, such as IMSIs for SIM cards, telephone numbers and mobile network codes. This would make the market for 2G/3G/4G connectivity competitive without long-term lock-in to a single network. Instead, customers could choose one or more networks per territory, based on their needs. They might even opt to use alternative networks, such as Wi-Fi networks, and employ their SIM card as an authentication mechanism. In the Netherlands, the government has changed the existing regulations in part at the request of its energy sector for the roll-out of smart meters. Enexis, a regulated utility managing an energy network, is the first private virtual network operator in the country to use its own SIM cards.[16] It chose this solution to avoid lock-in and ensure flexibility in the future.

The governments of Belgium and Germany are also consulting on a possible rule change. The European Conference of Postal and Telecommunications Administrations (CEPT/ECC) working group on naming and numbering concluded in a report on IMSI numbers for SIM cards that:

CEPT countries should review the assignment criteria for E.212 Mobile Network Codes (MNCs) and consider introducing more flexibility regarding the assignment of MNCs for:

a. Traditional market players such as MVNOs, MVNEs and Resellers; and

b. Emerging business models such as M2M service providers and SMS Service Providers (ECC, 2014).

Some governments are of the opinion that changes to the relevant ITU recommendations are necessary to grant private networks access to IMSI numbers and related numbers. In 2015, the ITU Study Group 2 will discuss proposed changes to the relevant regulation.

As a result of potential lock-in with mobile networks and the challenges in achieving coverage, large-scale suppliers and users of the IoT have been looking at alternative networking options. It is instructive to examine various solutions used for automatic meter reading/smart grids. Telefonica together with Connode from Sweden won a 15-year contract to supply smart metering solutions in the United Kingdom, using a combination of 802.15.4 IPv6-based mesh networking and cellular connectivity. The mesh networking allows smart meters to use other smart meters to reach a hub that has cellular connectivity. If coverage is lost on one node, another node can act as a hub. In the Netherlands, Alliander (a regulated utility managing an energy network) purchased a CDMA450 license from an existing licensee to offer network services to its own operating companies for smart grid purposes, but also to third parties. CDMA450 offers better coverage than higher frequency networks and is used by some companies to deploy wireless telephony in rural areas. The technology has limited capacity for voice calls; however, CDMA450 or LTE450 may deliver data communication with better coverage than existing wireless technologies. In other countries, energy companies have opted to use power-line communication, which can take up to a day to relay messages. While too slow for real-time services, this option often proves reliable and falls under the control of the energy company. In some cases, metering companies have opted for a short-range drive-by system, where the meter is not permanently connected but communicates when a meter company vehicle passes nearby.

In the United Kingdom, a company called Neul (recently purchased by Huawei) advocates the use of whitespace spectrum – unused frequencies in the television bands. Its technology works on spectrum between 470 Mhz to 790 Mhz. In France, Sigfox aims to use unlicensed industrial, scientific and medical (ISM) bands (868 Mhz in Europe and 902 Mhz in the United States) with Ultra Narrow Band networks. A device can send up to 140 messages per day of 12 bytes payload. Although currently available in only a few countries, it received USD 115 million in funding in 2015 to expand locations. Another French company, Semtech, is promoting LoRa for long-range (up to 15 km) communication at low bit-rates with IoT devices.

These developments underline the need on the part of many users for communication over a widely dispersed area with large coverage. Alternative solutions to 2G/3G/4G are being developed, however only a few can make use of globally standardised spectrum bands and the available spectrum bandwidths are narrow, limiting their use.

IPv6 and the Internet of Things

IPv6 and the IoT are often perceived to be strongly aligned, to the extent that they are mutually reliant. The IoT needs the massively expanded protocol address space that only IPv6 can provide, while IPv6 needs to provide a substantive foundation to justify the additional expenditures associated with widespread deployment of this new protocol. Some argue that use of IPv6 would also alleviate shortages in telephone numbers and IMSI numbers. However, these are still necessary to identify a device in a mobile network over which IPv6 is run.[17]

However, the evidence to date on device deployments does not provide a compelling justification. Existing deployment of sensor networks, mobile devices and other forms of microware all use the IPv4 network. This is viewed as a pragmatic choice dictated by availability. While estimates vary, the consensus indicates that between 8 billion and 10 billion devices were connected to the Internet in 2012. At that time the Internet comprised about 2.5 billion addresses, indicating that the majority of these devices were located behind conventional Network Address Translation (NAT) units that allow one IPv4 address to be shared across multiple devices simultaneously.

This raises the question of whether the IoT requires IPv6 as an essential precondition, or whether an ever-expanding population of micro devices can continue to be deployed on the present address-sharing framework on IPv4, or a mix of IPv4 and IPv6 with translation between parts of the same network. This question also relates to the nature of the embedded device and the way in which it communicates within its external environment.

"Polled model" devices collect and retain data in local memory, then pass the data back to a controller when polled. In this data collection model the device is the target of connection requests and generally needs its own uniquely assigned public IP address. Given the large volume of devices contemplated in the IoT, the polled model would require the greater volume of addresses supplied by IPv6, and could not be sustained on IPv4.

An alternate sensor-reporting model is the "report to base" model, in which the device collects data and periodically initiates a connection to its controller to pass the data back. This second model functions adequately in an environment of IPv4 and NATs, as the device initiates connection requests and is assigned the use of a public address only for the duration of the connection. At the same time, this model essentially "hides" the sensor device from the external Internet, as the NAT function effectively prevents external agents from initiating any form of communication with the device.

Much of the work to date in sensor networks and similar application environments for embedded automated devices uses this "report to base" model of connection, which permits the devices to be located behind NATs and use the existing IPv4 network. Such devices do not add to the impetus for broad IPv6 deployment. However, when continuous sensor models (e.g. video streams or continuous environmental sensors) are considered, as well as forms of "just in time" opportunistic data collection, then the ability to poll sensors as and when needed becomes a significant asset and NATs become an impediment. In this case, using IPv6 is generally thought to be a necessary precondition. However, not using a NAT will expose unattended micro devices to the Internet. This has attendant issues relating to security and abuse, including the risk of such addressable devices being co-opted into various forms of high-volume distributed Denial of Service (DOS) attacks. The question of whether the larger address space of IPv6 effectively prevents the

opportunistic discovery of sensor devices, or whether operational prudence requires that such exposed sensors be equipped with robust security and continual monitoring and maintenance, is at present an open issue for the sensor industry.

Predictions and measurements of the size of the Internet of Things

There have been numerous predictions about the size of the IoT in the near future. The most widely cited is that of Ericsson, which stated in 2010 that there would be 50 billion connected devices by 2020. Prior to this, Intel estimated in 2009 that 5 billion devices were already connected to the Internet and predicted that this number would rise to 15 billion by 2015 (GigaOm, 2014). Cisco's Visual Networking Index 2014 also predicted 15 billion devices connected, although for 2018, while in 2013 the Cisco Internet Business Group estimated 50 billion connected things by 2020.[18] These numbers could be judged to be excessive, and the timing could also be off by a few years. However, when the OECD evaluated the underlying calculations for the number of devices, they appeared sound. The main determining factors are the roll-out of fixed and mobile broadband and the decreasing cost of devices.

In 2012, the OECD produced its own estimates of the size of IoT usage in people's residences, with a view to verifying some of these claims. Today, in OECD countries, an average family of four with two teenagers has ten Internet connected devices in and around their home. Estimates indicate that this figure could rise to 50 by 2022 (Table 6.2). As a result, the number of connected devices in OECD countries would increase from over 1 billion today to 14 billion by 2022.[19] This calculation only covers homes in OECD countries and does not evaluate growth in the number of connected devices outside OECD countries or in industry, business, agriculture and public spaces. It is not an unreasonable assumption that the market for the IoT outside of OECD countries is at least as big as for OECD countries.

Measuring the actual size of the IoT is harder, however. A device connected via Bluetooth or Zigbee, such as a light bulb, fitness bracelet or other device, may not show up on the network. These work via gateway devices, such as smartphones and dedicated home gateways, and the gateway devices themselves may operate behind firewalls, proxies and home routers that perform network address translation. In practice, this means that it is hard to look beyond the router into the home or to look across the mobile network and the smartphone to connected devices. However, the OECD and regulators have found a number of ways to measure the growth of the IoT.

One way of measuring the IoT is to look at the number of SIM cards and phone numbers allocated to M2M communication devices on mobile networks (Figure 6.3). Increasingly, governments require mobile operators to report the number of M2M devices on their networks. Some countries have gone further mandating that any device not used for telephony has to be assigned a (longer) M2M number rather than a traditional telephone number.[20] Current data show brisk market growth in SIM cards and phone numbers in many countries. Most countries report double digit growth between 2012 and 2013, although most lack data for 2011, so it is hard to analyse trends. Some operators are also reporting on the number of connected devices. AT&T in the United States, for example, reports that it connected 1.3 million devices on its mobile network in the second quarter of 2014, of which 500 000 were vehicles.

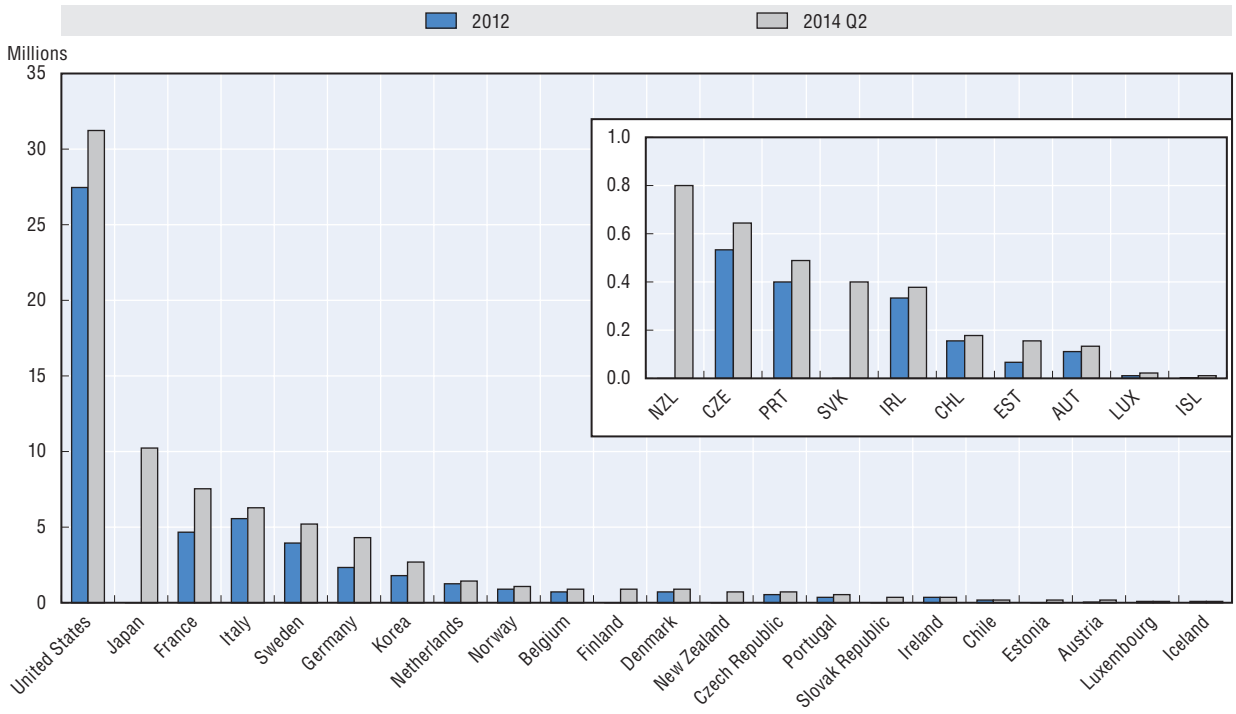
Table 6.2. **Number of devices per household**

2012	2017	2022
2 smartphones	4 smartphones	4 smartphones
2 laptops/computers	2 laptops	2 laptops
1 tablet	2 tablets	2 tablets
1 DSL/Cable/Fibre/Wi-Fi modem	1 connected television	3 connected televisions
1 printer/scanner	2 connected set-top boxes	3 connected set-top boxes
1 game console	1 network-attached storage	2 e-Readers
	2 eReaders	1 printer/scanner
	1 printer/scanner	1 smart meter
	1 game console	3 connected stereo systems
	1 smart meter	1 digital camera
	2 connected stereo systems	1 energy consumption display
	1 energy consumption display	2 connected cars
	1 Internet-connected car	7 smart light bulbs
	1 pair of connected sport shoes	3 connected sport devices
	1 pay-as-you-drive device	5 Internet-connected power sockets
		1 weight scale
		1 eHealth device
		2 pay-as-you-drive devices
		1 intelligent thermostat
		1 network-attached storage
		4 home automation sensors
Devices that are likely, but not in general use		
e-Readers	weight scale	alarm system
sportsgear	smart light bulb	In-house cameras
Network-attached storage	ehealth monitor	connected locks
connected navigation device	digital camera	
Set-top box		
smart meter		

Some caution is necessary in interpreting the data, as these numbers are allocated to mobile operators of particular countries, however the devices may be used outside the country. This issue is notable in European countries where multinational corporations may purchase connectivity from one operator to cover all or part of Europe. An example is Sweden, where Telenor Connexion has a large M2M business, with a large proportion of the numbers used outside of Sweden. In addition some mobile operators will assign a number from a small country, such as Luxembourg or Malta, so that the device can, in principle, roam on all networks in other European countries. These countries will be overcounted, whereas other countries will see an undercount for the number of devices.

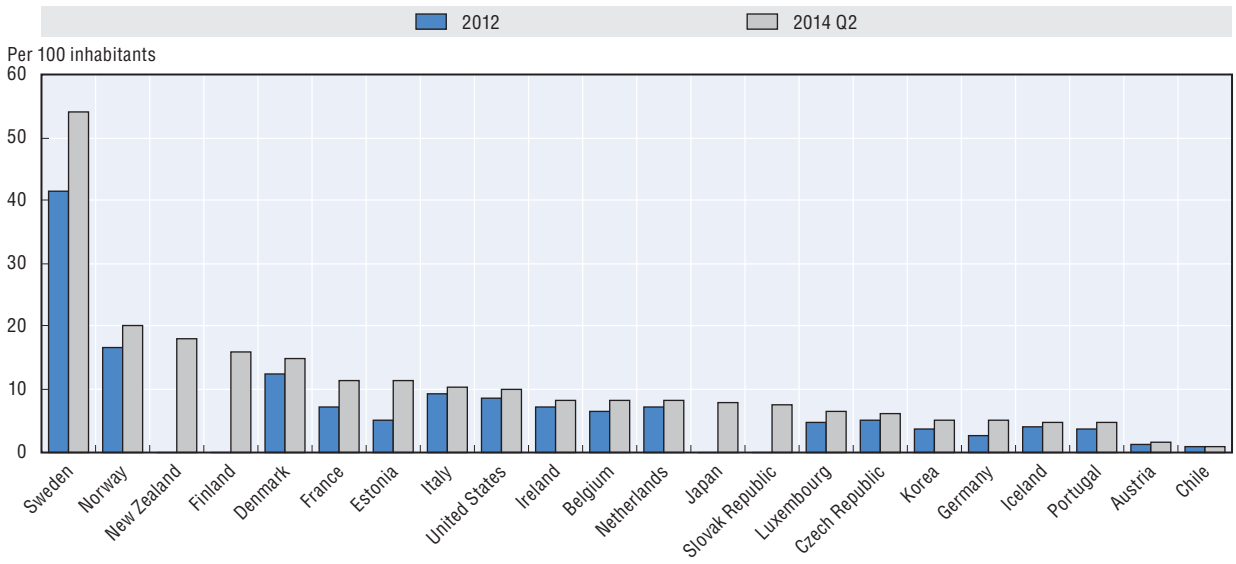
Across the OECD, regulators report that there are at least 83 million M2M numbers in use. There are 12 countries for which data are not available. Even if no growth between 2012 and 2013 was assumed for countries for which no data for 2012 were available, then the growth in number of M2M connections at 21%, or 12 million devices, can still be viewed as robust. These data do not capture all M2M devices connected through mobile networks, as an unknown number of users connect using consumer subscriptions. While the United States leads in absolute number of devices connected, Sweden leads on the basis of number of devices connected per capita. However, not all these devices may be located in Sweden (Figure 6.4).

Figure 6.3. **Number of M2M SIM cards per country**



StatLink http://dx.doi.org/10.1787/888933225289

Figure 6.4. **Number of M2M/embedded mobile cellular subscriptions, per 100 inhabitants**



StatLink http://dx.doi.org/10.1787/888933225295

An alternative way of measuring the size of the IoT is to scan IP addresses for the types of devices connected to the Internet. Data from companies such as Shodan can be used for this exercise. Devices themselves often provide data on the brand and type of

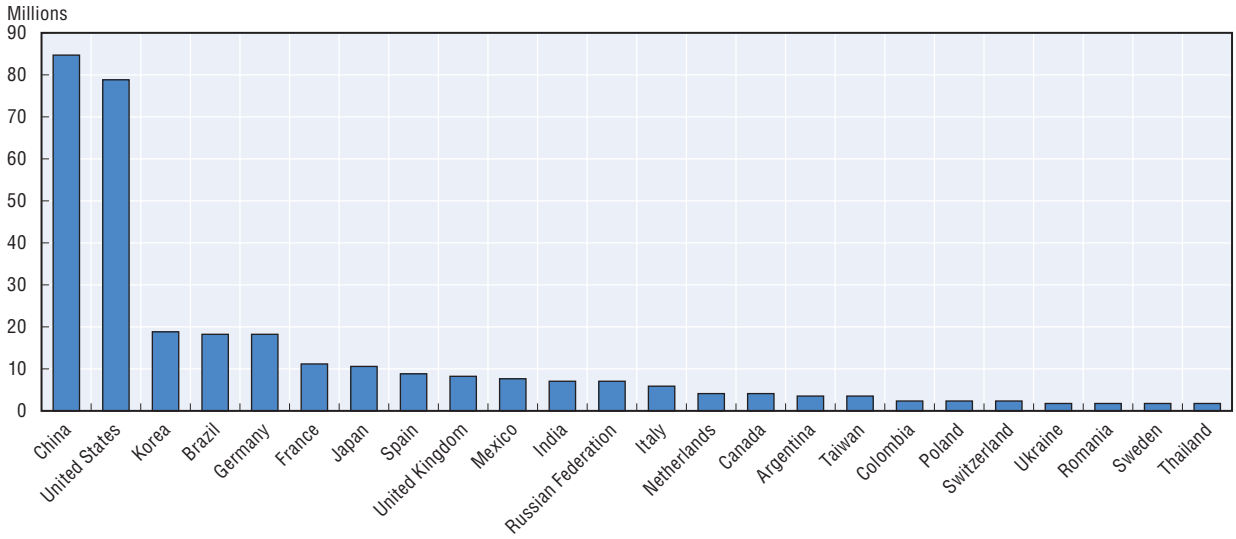
device, or this can be inferred from the type of response they give. Although this approach is promising, the lack of a classification for devices producing the raw data hinders its use as a means to measure the size of the IoT. Security researchers have created profiles for specific devices, such as SCADA systems that control factories and energy plants, but as yet there is no general classification of devices. A more encompassing framework that will allow analysis of data received through scanning the Internet is likely to be created in the near future.

Even if all IPv4 addresses are scanned there are some limitations to the data. Not every device connected to the Internet will respond to every request to identify itself. System administrators may limit the types of requests a device will respond to and a large number of devices are located behind home and business DSL routers, cable modems and corporate firewalls that use Network Address Translation (NAT), which may not respond to random requests. In the case of Carrier Grade NATs used in mobiles, it is often impossible to reach individual devices.[21] If networks switch to IPv6 this might become even harder, as it is impossible to scan all IPv6 addresses in a meaningful manner. While it may take a few hours to a day to scan all 4 billion IPv4 addresses, the IPv6 space is 4 billion times 4 billion times 4 billion times larger. Registration of IP addresses to countries can also be problematic. If the data from regional Internet registries (RIRs) are used some countries may be over-represented. For example, the network of Liberty Global, which spans multiple countries in Europe, is considered an Austrian network according to some IP location mappings. This is because the address space was registered by RIPE NCC to the Austrian branch of Liberty Global, but the space is used across all European subsidiairies of Liberty Global.

Even with these limitations the data provide an approximate overview of device locations on the Internet. Shodan finds 363 million devices online (Figure 6.5) with some 84 million registered to China and 78 million to the United States. Korea, Brazil and Germany follow with 18 million connected devices, and Japan, Spain, the United Kingdom and Mexico make up the rest of the top 10 with 8 million to 10 million devices. Efforts to rank devices per capita are hindered by data limitations, but an experimental top 10 is provided (Figure 6.6). For example, Luxembourg does not rank high in terms of this approach because some operators use Carrier Grade NAT for their FTTH implementation, effectively shielding all devices behind the NAT.

Other approaches could be based on the number of Bluetooth, Ethernet, IEEE 802.15.4, Wi-Fi and 2G/3G/4G chips shipped. Estimates for shipments can be obtained from industry analysts, although the methodologies may not be transparent. Difficulties can arise, however, in combining the data as some devices will have multiple chips and chipsets on board. The Wi-Fi-alliance states that in 2013 an estimated 2 billion Wi-Fi-enabled devices were shipped. Over 2 billion Bluetooth chipsets were shipped in 2013, with smartphones making up 61% of that market. It is likely that there is an almost complete overlap between smartphones, laptops and tablets that integrate both Wi-Fi and Bluetooth, but it is unclear whether sales figures distinguish correctly between the two if Bluetooth and Wi-Fi form part of the same chipset. With sales of laptops, tablets and smartphones close to 1.5 billion units, this would indicate that up to 1 billion other wireless connected devices were sold. Data for sales of 802.15.4 chips are unfortunately not available.

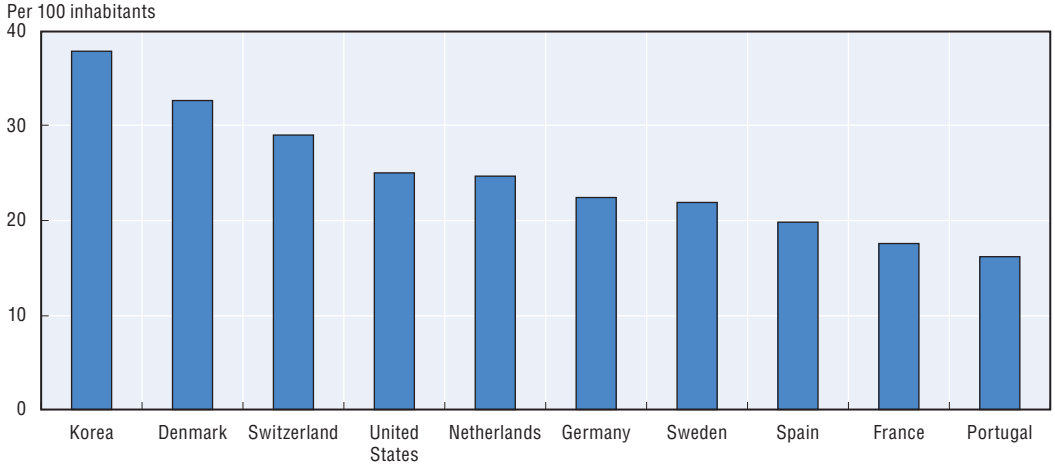
Figure 6.5. **Devices online, top 25 countries**



Sources: Based on Shodan, *www.shodanhq.com*.

StatLink http://dx.doi.org/10.1787/888933225304

Figure 6.6. **Devices online per 100 inhabitants, top OECD countries**



Sources: Based on Shodan, *www.shodanhq.com*.

StatLink http://dx.doi.org/10.1787/888933225312

6.3 Fostering public policy goals with the Internet of Things

A number of governments have introduced regulations that rely on data from the IoT. For example, remotely monitoring traffic lights and dykes allows governments to optimise traffic flow and better understand flooding risks. The IoT also allows governments to achieve policy goals in new ways. For example, some governments now use GPS and mobile communication to calculate road pricing based on time of day and distance travelled, with a view to reducing congestion. This represents a shift from conventional road-pricing systems, which relied on a toll booth or digital moat around a city to charge all incoming traffic a flat congestion charge.

eHealth

Analysts and governments have high expectations of eHealth devices that will allow remote monitoring of patients at home or work. However, only a few certified devices are available on the market. This appears to be due not to a lack of research or government commitment, but rather to difficulties in implementation. One example is created by the use of portable eHealth equipment in conjunction with near real-time data streaming to a central server. Users of portable Electro Cardiogram (ECG) equipment have reported an increase in anxiety as a result of calls from carers resulting from anomalous readings, possibly caused by a user moving out of range, compounded by an inability to distinguish between an emergency call and a service call.[22] Regulators also have to certify the equipment and the associated applications. In the case of a radiology application, regulators also needed to verify the quality of the iPad screen to ensure it can display the images at the correct quality and luminescence. Such problems are not easily rectified by a simple change in policy. Instead they require the consistent evaluation of each new application with a view to minimising the risks to users, while maximising the benefits.

Transport

Road toll systems in most OECD countries are based on RFID technology, activated when a user drives through a toll-gate. The drawback of this system is its inflexibility. It works only on main highways and equipping new roads with the system can be expensive as this necessitates a redesign of the road. GPS-based systems that use wireless networks to communicate can function on any road and do not require physical infrastructure. However, implementation has proven more challenging than expected in countries that have tried. The reasons for this include a failure to reach agreement among stakeholders and issues relating to technology and price.[23] Germany and Hungary have GPS-based tolls in operation for trucks above 12 tonnes and 3.5 tonnes respectively. Belgium will use the same system as Germany for trucks as of 2016. Germany uses an integrated system where the on-board unit and back-office systems are provided by one company, Toll-Collect. Hungary's system is more modular and relies on a number of manufacturers and service providers for the on-board unit. These companies can also provide fleet-management (location, fuel consumption) solutions to hauliers, which has allowed the Hungarian system to acts as a platform for additional services to the industry.

The European Commission has proposed eCall in all vehicles sold in the European Union. This initiative is designed to bring rapid assistance to motorists involved in a collision anywhere in the European Union. The EC proposals for legislative acts foresaw full implementation and seamless functioning of eCall throughout Europe by end-2015. However, the adoption procedure for these legislative acts by the European Parliament and the Council is still ongoing, so the deadlines for implementation will most likely be delayed to end-2017 or early 2018. In Brazil, a similar system (Denatran/SIMRAV) will become mandatory and is targeted for release during 2015. This system is designed to prevent vehicle theft, but will also enable other services. Manufacturers of vehicles also expect the eCall system to become a platform for other on-board services.

Online on-board services using inbuilt mobile communications are currently more popular in North America, where examples such as OnStar of General Motors, Bluelink of Hyundai and BMW Assist, provide emergency services, theft protection and similar services. Most manufacturers choose a hybrid system that incorporates a mobile communications unit on-board for emergency services, but uses the driver's mobile phone

for other services. It is also possible to connect to the vehicle using a smartphone and read its location, tyre pressure and other mechanical properties, or heat up the vehicle prior to departure. Accurate numbers across the North American market are difficult to obtain for all manufacturers. This type of service is becoming a standard feature on new vehicles and AT&T reports connecting to 2 million vehicles per year. OnStar has over 6 million users in Canada, China and the United States, while BMW Assist has over 1 million users.

The IoT can also be used to connect data about road usage with vehicles and traffic lights. Several navigation providers, such as Garmin, Google and TomTom, make use of data from governments and mobile networks on the speed of vehicles in certain locations to provide their customers with real-time traffic updates. Transport for London has gone one step further and connected data on road usage with real-time control of traffic lights in the city. The collected data are fed to a machine-learning algorithm, which aims to optimise traffic flow. The system known as SCOOT is said to deliver on average a 12% improvement in traffic flow. It is likely that other large cities will aim to introduce similar systems to improve in-city traffic flows.

Energy

Smart grids are another area where countries expect the IoT to benefit their economies. Smart grids will allow two-way communication between the home/business and the energy grid. This will increase consumer awareness of their energy consumption, which policy makers expect to result in reduced energy consumption, but will also deliver energy back to the grid, which could promote the use of renewable energy sources such as solar and wind power. Accordingly, the European Commission required all European Union member states to conduct a cost-benefit analysis of smart meters, with countries implementing smart meters in 80% of positively assessed locations by 2020. In 16 European Union member states the cost-benefit analysis was positive and smart meter roll-out will commence. In seven countries the analysis was negative or inconclusive, but in some of these, such as Germany, roll-out will commence for certain groups of customers (EC, 2014).

In the United Kingdom, consumers with smart meters will be offered an in-home display (IHD) which will let them see how much energy they are consuming and its associated cost. In addition, the communications hub in the meter will allow users to connect third-party devices and services to the meter and develop services around it.[24] The smart meter is expected to function as a platform on which the IoT can be built. Expected benefits include:

- near real-time information on energy use, expressed in pounds and pence
- the ability to manage energy use, save costs and reduce greenhouse gas emissions and other harmful gases and particles
- an end to estimated billing with customers charged only for the energy they actually use, helping them to budget better
- smoother and faster switching between suppliers to obtain better deals
- supplier access to accurate data for billing, removing the need to manually read meters.

The energy crisis in Japan, resulting from the 2011 Tōhoku earthquake and tsunami, prompted the Tokyo energy company Tepco to accelerate its plans for smart metering. The company intends to roll-out a network by 2018 to cover 80% of its customers. The innovative network will be based on IPv6 over wireless mesh networking, cellular network and power-line communication. It will transmit meter data every 30 minutes – much more

frequently than most existing systems. In addition, it will act as a two-way system that supports push messaging demand response and energy management capabilities, all the way to individual devices in the home. To ensure security Tepco have adopted an end-to-end security model. The result should be a system that can support the future of electric vehicles, solar cells and building energy management systems (St. John, 2014).

In the United States, a federal stimulus programme designed to counter the global economic crisis aimed to promote the roll-out of smart grids to promote energy efficiency. As a result, two-way communicating smart meters were installed in 50 million households (43% of the total) by September 2014 (IEI, 2014). Over 8 million customers can participate in a variety of "smart pricing" programmes, which reward participants for voluntarily reducing energy consumption when demand for electricity and prices are expected to be particularly high. In some cases, customers make use of connected thermostats and other devices to automatically change their usage in line with smart pricing programmes.

Cities

In addition to the above examples for transport and electricity, city governments increasingly use the IoT to pursue policy goals. For example, the city of Boston has developed a mobile app, StreetBump, that sends data from the smartphones of citizens driving through Boston. Making use of the accelerometer (motion detector) and GPS, StreetBump identifies potholes and bumps and communicates their location. Other examples include Barcelona's app 2.0 incidències, which reports on commuter rail service interruptions or delays in the metropolitan area of Barcelona, or San Francisco's Cycle Track app that informs transport planners about bicycle trips in the city and thus on the actual use of existing bike lanes and the need for new ones. Several cities are currently looking into upgrading public rubbish cans to communicate how full they are, which would allow trash collectors to optimise their routes and stops. The increasing amount of real-time, fine-grained IoT data enables more targeted and cost-effective infrastructure maintenance, service improvements and investment decisions in cities.

Public policies that promote or affect use of the Internet of Things

The potential benefits of the IoT feature in a growing number of public policies, either as a means to achieve goals or an area targeted for research. There is no consistent approach among governments to the IoT, but some examples can be provided.

The European Union has made the IoT an essential part of its Digital Agenda for Europe 2020, which focuses on applications, research and innovation, and the policy environment. The European Union has been particularly active in promoting research and innovation:

> *The Internet of Things European Research Cluster groups together the IoT projects funded by the European research framework programmes, as well as national IoT initiatives. The requirements of IoT will also be fed into the research on empowering network technologies, like 5G Mobiles. The Future Internet public private partnership will develop building blocks useful for IoT applications, while Cloud Computing will provide objects with service and storage resources. On the application side, initiatives like Sensing Enterprise and Factory of the Future help companies use the technology to innovate, while experimental facilities like FIRE are available for large-scale testing.* [25]

In February 2014, the Korean government published its plan for building the IoT with the aim of launching a hyper-connected "digital revolution" to address policy goals. One of the aims was to promote IoT-driven economic development, existing examples of which

include Songdo Smart City and smart eel farms (Box 6.3). The plan aims to commercialise 5G mobile communication by 2020 with Gigabit Internet achieving 90% of national coverage by 2017. In addition, a total of 1 GHz of spectrum will be freed by 2023 and IPv6 infrastructure further expanded into the subscriber network by 2017. The plan also emphasises the development of low-power, long-distance and non-licensed band communication technologies for connecting objects in remote areas (Ministry of Science, ICT and Planning, 2014).

Box 6.3. **IoT advances in Korea**

Smart farm projects

In January 2014, SK Telecom introduced an IoT technology-based eel farm management system. Farmers can monitor their fish tanks in real time through smart devices including smartphones. In general, each eel farm has 20 to 60 water tanks breeding about 10 000 eels, which are worth over USD 100 000 per tank. Eel farming is a high value-added business, but the farming requires farmers to frequently monitor a variety of indicators as even minor environmental changes are fatal to eels. Under the IoT-based fish farming management system, three sensors are installed on each fish tank to measure water temperature, quality and oxygen level. The farmer can operate the sensors and machinery remotely when intervention is needed.

Songdo Smart City

"Songdo" city is a new city built on a peninsula off the coast of Seoul, which will become home to 200 000 people. The whole city is wired with fibre optics to connect the different systems that keep Songdo city running. Telepresence is installed in homes, offices, hospitals and shopping centres to allow people to make video calls wherever they want. Sensors are embedded in streets and buildings to monitor everything from temperature to road conditions. These sensors also monitor fire and safety in many towers. The wireless sensor networks used in Songdo are designed specifically to create smart cities. The aim is to build a distributed network of intelligent sensor nodes that can measure a variety of parameters for more efficient management of the city. Data are delivered wirelessly and in real time to citizens and the appropriate authorities. Citizens can monitor the pollution concentration in each street of the city. The authorities can also optimise irrigation of parks or lighting throughout the city. Water leaks can be easily detected and vehicle traffic can be monitored in order to modify street lights. Systems that detect and transmit the location of available parking spots will reduce traffic congestion and pollution, and save time and fuel.

When rolling out IoT services nationwide, conflicts with existing regulation and regulatory uncertainty may act as bottlenecks. For example, existing medical regulations may hamper innovative services by requiring the presence of a doctor on both ends of a tele-medicine consultation. Such regulations undermine a key advantage of tele-medicine – the ability to consult a medical practitioner when factors such as distance would make this otherwise impossible. With this in mind, the Korean government has established a "telecommunication strategy council" which will aim to improve general regulations. It will also establish an IoT testbed as a regulation-free zone and aim to improve the legal system.

The German government has launched innovation clusters directly tied to the IoT. For example, the "Cool Silicon" innovation cluster in the south of Germany aims to develop low-energy and energy self-sufficient processors and sensors. Another innovation cluster called

"IT's OWL", located in central Germany, focuses on creating intelligent and autonomous industries through the use of robots. Also in Germany, Microtec Sudwest aims to develop new sensors, microsystems and flexible, bendable chips. A fourth cluster focuses on software for new industries. Each of the research clusters is tied to a large number of businesses, universities and research centres in the region that combine to deliver the output.

Other countries have acknowledged the future of the IoT in their policies, and its underlying and accompanying developments in the cloud, big data, sensors and actuators and the aims of autonomous machines and systems. Some have started to assess whether current policies are still in alignment with the perceived future (Box 6.4). Ofcom in the United Kingdom, for example, has started a consultation on the implications of IoT for spectrum and numbering policy (Ofcom, 2014). The Netherlands, the first country to liberalise access to IMSI numbers for SIM cards, is consulting on further policies regarding signalling point codes needed for routing traffic in mobile networks.[26] Liberalising access to IMSI numbers has enabled Enexis, a Dutch energy network, to deploy 500 000 SIM cards (not tied to a mobile operator) to its smart meters. The Belgian government has indicated its support for this approach (BIPT, 2014). Some countries are of the opinion, however, that a change of the ITU E.212 recommendation is required – something that is being discussed in 2015.

Governments will also have to re-evaluate a large number of policies. These include policies surrounding naming and numbering, particularly with regard to numbers used in mobile networks, where further liberalisation and access for private networks could bring great economic benefits. Numbering policies surrounding IPv4 and IPv6 do not appear to need fundamental changes, as these numbers are already available to all interested parties, although the number of available IPv4 addresses is limited.

Policies surrounding the use of "national" numbers on an international scale will also need discussion. For example, does it matter when "national" numbers are used outside the national territory? Conversely, does it matter when a device with a foreign IMSI number or foreign E.164 (telephone) number is used within a territory? Although this practice is common for IP addresses, which have no strict link to a country, these questions are now being asked by national telecommunication regulators. There are already cases where governments and incumbent operators have declined to allow "foreign" devices roam in their country permanently, despite the payment of all applicable charges and taxes.

Spectrum is necessary for the IoT, although it is unclear how much. Globally harmonised ranges would be best, but may be unattainable. In and around people's residences and businesses, unlicensed bands have proven to be of great value. Lack of competitive offers that fit their circumstances has pushed some large-scale IoT users to try to obtain access to their own dedicated spectrum or to find alternatives. Others have sought to create dedicated bands for IoT communication, sometimes with service providers that have monopoly power.

Standardisation has proved difficult. Because the IoT encompasses everything from the technical level upwards, it also affects business processes and even political decisions. As such, there is no single standard and as a result standards are fragmented. Large manufacturers often back multiple competing standards at each level, thereby failing to ensure consumer confidence by choosing one particular standard. There is a chance that countries and economic sectors will decide to use different and competing sectors, thus creating a situation of inoperability and fragmentation. However, it is equally possible that flexible frameworks will develop where devices can interoperate with multiple standards at the same time.

Box 6.4. **IoT policy in the United States**

At the Federal Communications Commission, the Technological Advisory Council (a group of academic and industry experts appointed by the FCC Chairman) is studying issues surrounding how the IoT will effect communications networks in the next 10 to 20 years. In December 2014, the IoT Working Group made the following recommendations to the TAC:

- The FCC should programmatically monitor consumer IoT network traffic impact on WLAN and WWAN with a focus on new high bandwidth consuming applications.
- The FCC should focus on availability of unlicensed spectrum suitable to a range of PAN/WLAN services without making spectrum allocations unique to IoT, and ensure there is enough short-range spectrum to meet growth in PAN/WLAN requirements and sufficient network capacity upstream from IoT devices and proxies.
- The FCC should define its role within the context of an overall cybersecurity framework, dedicating resources and participating in IoT security activities with other government stakeholders.
- The FCC (in collaboration with other agencies) should conduct a consumer awareness campaign related to IoT security and privacy.
- The FCC should conduct internal periodic scenario exercises to determine appropriate response to widespread consumer events related to the IoT.

In February 2014, the United States National Institute for Standards and Technology (NIST) released a "Framework for Improving Critical Infrastructure Cybersecurity," which provides a structure that organisations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programmes. Designers of ICT systems (including those with IoT components) in any country can utilise this framework to enhance their systems security. In August, NIST convened its first meeting of the Cyber-physical Systems Public Working Group to develop and implement a cybersecurity framework for IoT with the goal of establishing an integrated and interoperable system across all economic/industry sectors. NIST plans to produce a draft "reference architecture" by early 2015.

In November 2014, the National Security Telecommunications Advisory Committee (NSTAC, a group of representatives from large information and communications corporations that reports to the President) released a draft report on IoT, urging the US government to take actions to secure the IoT. The report identifies risks associated with the IoT with a focus on critical infrastructure, concluding that, "there is a small and rapidly closing window to grasp the opportunities of the IoT in a way that maximizes security and minimizes risk. If the nation fails to do so, it will be coping with the consequences for generations". The report further states that, "there are only three years – and certainly no more than five – to influence how the IoT is adopted". While the report highlights the benefits of the IoT, it warns that "the rapid and massive connection of these devices also brings with it risks, including new attack vectors, new vulnerabilities and perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction".

The NSTAC report made several recommendations for the Obama Administration to work on. The Department of Commerce, specifically NIST, was tasked to develop a definition of the IoT for departments and agencies to use during assessments related to the IoT. NSTAC recommended that the White House Office of Management and Budget (OMB) require all federal departments and agencies to conduct an internal assessment of IoT capabilities that currently or could potentially support national security and emergency preparedness (NS/EP) functions. Furthermore, it stated that OMB should direct federal departments and agencies to develop contingency plans to identify and manage security issues created by current and future IoT deployments within the United States Government. These plans should anticipate an environment that cannot be fully secured because of the dynamic nature of the IoT and the potential threat. NSTAC recommended that the President create an inter-agency task force to coordinate with existing organisational bodies to foster balanced perspectives between security, economic benefits and potential risks. Participants should include, at a minimum, the Departments of Commerce, Homeland Security and Defense, and set milestones for the completion of a set of activities relevant to NS/EP.

As the IoT is pervasive, it will touch much of government policy. Policy makers should not just identify the potential benefits from IoT, they should also identify where the data and functionality offered by IoT could be leveraged and combined with other data elsewhere. The above-mentioned Hungarian case of creating an open system for road tolls, where data are also available to hauliers for their logistical processes, constitutes such an example.

Building the Internet of trust

In order to ensure that the IoT works to the benefit of people, some have argued that it should be thought of as the "Internet of Trust", as trust will be fundamental to enhancing user experience and addressing key legal challenges such as user privacy. Another pertinent factor is that while the "IoT is global .. the law is not" (Capgemini, 2014). The OECD has typically considered security, privacy and consumer protection as key elements for building trust in new technologies such as the IoT (OECD, 2015). This means prioritising security for devices connected to the IoT against cyber-attacks and ensuring the confidentiality and integrity of data communicated between devices. As already mentioned, this will require a shift in mindset from a traditional to a risk-based security approach (OECD, 2015).

Addressing the protection of personal data is more complicated. Broadly speaking, the privacy challenges raised by the IoT are not new. However, the enormous increase in the collection and use of data, its new and unanticipated uses, and the increased complexity and all-pervasive nature of the IoT present new challenges to traditional principles such as data minimisation, notification and consent. This complexity will make it more difficult for individuals to control and police data collection, especially when they are not actively involved or aware that it is occurring (OECD, 2015).

Individual preferences with respect to the use of personal data are nuanced and contextual, and are influenced by factors such as trust in service providers, perceived value exchange and other attitudinal, demographic and cultural factors. Acceptable practice is therefore subjective and may evolve (WEF, 2014). Data-use policies that treat all data equally and have universal application are neither appropriate nor sufficiently flexible. However, the difficulty of building context-related nuances with appropriate safeguards into regulations should be recognised.

One possible way forward is to learn from the experience of security risk management. Risk management could be adopted as an approach to privacy protection in a context-dependent environment that is rapidly evolving. This could be achieved in particular through the development of privacy management programmes to implement accountability (OECD, 2013a). This would take into account data sources and quality, as well as the sensitivity of the intended uses with a view to mitigating the risks of misuse. Such an approach would need to consider the wide range of harms and benefits, and be simple enough to be applied routinely and consistently. Privacy-enhancing technologies also have a role to play in reducing the identifiability of individuals, and in improving traceability and accountability.

The third element in building trust is consumer protection and empowerment, whose basic tenets revolve around adequate information disclosure, fair commercial practices including quality of service, and dispute resolution and redress. In increasingly complex environments involving a number of devices and parties, it will become more difficult for

consumers to know where a problem lies when it arises, and who is responsible for its resolution. Take, for example, the case of devices with firmware and software supporting an app for health monitoring. If the app ceases to work following a software update, who is responsible? Assuming the user can identify the issue, who should they turn to for assistance? Furthermore, for how long should such hardware or software be expected to function?

How well existing consumer protection frameworks address these challenges (or will be adapted to do so) is yet to be determined – a point recently discussed by the Committee on Consumer Policy in the context of its revision of the OECD's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce*.[27] Some consumer organisations such as Consumer Action in the United States have already spken at conferences on the subject of consumer protection frameworks in light of the IoT.

Managing security risks

Management of digital security risks has long been an issue in communication networks, and the commercialisation of the Internet has seen security concerns grow in scope and scale. Critical infrastructure increasingly depends on ICTs and communication networks, and guarding against accidental or malicious interference is becoming ever more important. End-to-end security is paramount for the IoT and must be built into networks and devices. Moreover, effective management of security risks will be essential.

Take, for example, a smart metering system with a network of electricity meters that measure consumer usage and send data to an electricity company's servers. There are a numerous ways that such a system could be compromised: a fake meter could transmit false data, a genuine meter could be tampered with to send incorrect data, data from a meter could be intercepted and modified by a network eavesdropper, and malicious users could install a fake server or compromise a genuine one to issue malicious commands or upload malicious firmware to meters on the network (Rubens, 2014).

Successfully hacking approaches such as this could have potentially devastating consequences. In 2012, the US Federal Bureau of Investigation reported that several smart meter hacks had occurred over the previous few years, costing hundreds of millions of dollars a year (KrebsOnSecurity, 2012). One commentator has identified three likely forms of attack (Baudoin, 2014):

- Eavesdropping on data or commands could reveal confidential information about the operation of the infrastructure.
- Injecting fake measurements could disrupt control processes and cause them to react inappropriately or dangerously, or could be used to mask physical attacks.
- Incorrect commands could be used to trigger unplanned events or to deliberately send physical resources (water, oil, electricity, etc.) to unplanned destinations.

The United States Federal Trade Commission (FTC) has also taken enforcement action. In 2013, the FTC charged TRENDNet, a maker of video cameras designed to allow consumers to monitor their homes remotely, with lax security practices that exposed the private lives of hundreds of consumers to public viewing on the Internet. In its complaint, the FTC alleged that, from at least April 2010, TRENDnet failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement. Under the terms of its settlement with the FTC, TRENDnet is prohibited from misrepresenting the

security of its cameras or the security, privacy, confidentiality or integrity of the information that its cameras or other devices transmit. In addition, TRENDnet is required to establish a comprehensive information security programme designed to address security risks that could result in unauthorised access to or use of the company's devices, and to protect the security, confidentiality and integrity of information that is stored, captured, accessed or transmitted by its devices. The settlement also requires TRENDnet to notify customers about the security issues with the cameras and the availability of the software update to correct them, and to provide customers with free technical support for two years to assist them in updating or uninstalling their cameras (US FTC, 2014).

The OECD is currently undertaking a review of its *2002 Guidelines for the Security of Information Systems and Networks*, in line with the changing context (OECD, 2012b):

- The threat landscape has evolved in scale and in kind. Since 2002, cyber criminality has considerably increased and the exploitation of vulnerabilities in information systems provides an opportunity for economic, social and political disruptions of all kinds ("hacktivism").
- The perimeter of information systems is increasingly blurred. In a hyper connected world – where every process, device and infrastructure is in some way interconnected – it is becoming difficult to define the perimeter of information systems or corporate networks.
- IT and the Internet have evolved from being useful to individuals and organisations to being essential to society.
- Cybersecurity policy making is at a turning point. Responding to cybersecurity challenges has become a national policy priority in many countries.

A risk-based approach recognises that guaranteeing end-to-end security in the IoT is impossible and that it is up to everyone, including consumers, to assess the likelihood of problems occurring and the potential impact, and to take responsibility for their actions. The key message is that you cannot secure your digital environment and that you cannot expect "suppliers" to do everything for you. It therefore becomes a matter of assessing and managing the risk. Governments have a particular role to play in educating consumers and citizens in this regard. However, this is quite a sophisticated and subtle message and making intelligent decisions may be beyond the capability of many consumers. Perhaps a new class of trusted intermediaries will emerge to manage interactions with the IoT on consumers' behalf.

Governments also have a role to play in fostering the development of a common set of standards, which would become a benchmark for the required level of security expected from a device. The goal is not to guarantee absolute levels of security. Instead it is necessary to instil confidence and trust among consumers that, in the event the security of their device is breached (especially as new vulnerabilities emerge), the problem will be addressed. Cross-country adhesion to a similar set of standards would avoid creating trade barriers by requiring different standards.

Privacy

Data protection and privacy are key concerns associated with the IoT. However, ever since the invention of the telephone and the camera, the adoption of new technology has challenged privacy. With billions of connected devices in the IoT transmitting and receiving

huge amount of data, much of it sensitive personal data, a key question is: "To what extent is it necessary to rethink approaches to data protection and privacy?" According to US FTC Commissioner Brill, "We should all be concerned that questions about privacy will keep consumers away from the IoT because they do not trust it" (Brill, 2014).

A key privacy issue relates to consent, particularly regarding possible onward use of data outside the intial terms of an agreement. Will consumers in the IoT retain control of their data or will they be unwitting participants in a system that neither respects nor needs their consent? This fear is compounded by the enormous number of organisations that might be able to use personal data and benefit from the nascent potential of data analytics.

Devices connected to the IoT will send and receive frequent, sometimes continuous, data streams. If collection of this data were to rely on traditional notification and consent, people would be prompted hundreds or thousands of times a day. In addition to the inconvenience to individuals it might slow the IoT to a grinding halt (Wolf and Polonetsky, 2013). Adhering to a traditional approach of notification and consent to protect privacy might lead consumers to just give up or to turn down requests as a default option. Providing effective information disclosure to consumers as a basis for privacy protection is already a challenging issue. The IoT will compound the difficulties.

Some have argued that the scale and complexity of the IoT signals the death of privacy (Rauhofer, 2008). Others respond that there is nothing fundamentally new about the IoT in terms of its implications for privacy (Pasiewicz, 2008). Nevertheless, there are several emerging approaches, such as the proactive "baking in" of privacy to the IoT at the design stage.[28] Some think that the IoT will stimulate the emergence of trusted intermediaries (or infomediaries), such as OpenPDS, who will manage the use of data on the behalf of consumers (Co.Exist, 2014). Others believe that these approaches will be insufficient to resolve the challenges and argue that data ownership should be rethought completely. Tim Berners-Lee, the inventor of the World Wide Web, for example, believes that the data people create about themselves should be owned by each individual, not by large companies that harvest data (Hearn, 2014; see also *Edge*, 2012).

Instead of focusing on the collection and communication of information, Wolf and Polonetsky, co-chairs of the think tank Future of Privacy Forum, argue that it is more important to focus on how personal data is used (Box 6.5). Whether a use model would provide more effective protection in practice is disputed, and remains a topic of ongoing discussion and debate among experts (OECD, 2014).

Box 6.5. **A use-focused privacy paradigm for the Internet of Things**

- "Use anonymised data when practical."
- "Respect the context in which personally identifiable information is collected."
- "Be transparent about data use."
- "Automate accountability mechanisms."
- "Develop Codes of Conduct."
- "Provide individuals with reasonable access to personally identifiable information."

Source: Wolf and Polonetsky, 2013.

Consumer protection and empowerment

As mentioned above, the key consumer issues subject to considerable policy attention in the e-commerce environment (e.g. privacy protection, the need for adequate information disclosures, fair commercial practices, and dispute resolution and redress) are likely to be amplified in an IoT context, where multiple parties engage in a complex set of transactions with consumers.

As regards disclosure, a charter developed by the Alzheimer's Society (2014), provides people with dementia and their carers with a list of questions to consider prior to purchasing or accessing technology used to deal with the consequences of this illness (Box 6.6).

Box 6.6. **What to consider when purchasing IoT equipment related to dementia**

Questions for professionals working in dementia

- What are the limitations of the technology to be used?
- Does the technology connect to other devices? If so, is compatibility an issue?
- Does the use of the technology match the intended use of the manufacturer?
- Is battery life an issue? Who will be responsible for battery management?
- Does the product need to be waterproof?
- What can go wrong with the chosen technology?
- If the technology fails, what are the associated risks of the failure?
- What are the maintenance arrangements for the product and is it covered by a warranty?
- Who is responsible for equipment testing and how often will this take place?

Questions for individuals, families and carers

- How does it work? Who will show me how to use it? Are the instructions easy?
- Do I need a phone line or an Internet connection to use the technology?
- Who do I contact if something breaks or if I have a problem?
- Do I need to change or charge batteries, and how often do I need to do this?
- Who will install the equipment and will I experience any disruption to my life?
- If my needs change, will the technology still support me?
- What evidence or information is there to help me decide what technology I need?
- Is there a helpline I can call if I have any concerns?
- Is there a response service that will come if a particular alarm is triggered?

Source: Based on Alzheimer's Society (2014).

While not all the questions in Box 6.6 may be appropriate for every IoT product, they provide an interesting overview of the type of information passed on to consumers at an early stage, so as to engage in an IoT transaction in an informed manner. Such information should help consumers to:

- access and use devices and related services in an easy manner and at all times
- determine the level of interoperability of the IoT devices
- identify who to turn to when problems with such devices arise.

One of the major drivers of consumer adoption of the IoT is likely to be the desire to make life simpler. But even one device such as a smart heating controller can be quite complex to programme and manage, and anyone with several devices may need guidance on ways to access and use them. A related issue is the need to ensure that consumers can access and use their devices and associated services within the IoT network, on any Internet connection, in an effective and uninterrupted manner. This will help to address situations where access to devices is prevented when part of the network goes offline. Likewise, the lifetime of IoT devices will need to be explored. This will mean examining conditions for updating software and the continued functioning of devices in an IoT network. In recognition of the need for enhanced consumer understanding of IoT device functionality and limitations, and for trusted compliance processes that will operate along the IoT supply chain, the United Kingdom Information Economy Council has developed a voluntary consumer-focused framework of recommendations. This aims to help address consumer expectations and to provide consumers with adequate disclosures about their rights and obligations in an IoT ecosystem (BT, 2014).

Ensuring a greater level of interoperability for connected devices and providing consumers with adequate information will be key to building a trusted and reliable IoT ecosystem. Exploring ways to overcome software update management challenges will also be essential to maintain interoperability between older and newer consumer IoT devices. In the area of payments, this will involve addressing problems associated with the range of diverse NFC systems in operation, as pointed out in a study of NFC in public transport (Liebenau et al., 2011). Proprietors of those systems currently have no incentive to make their payment cards interoperable with other systems, however convenient this might be for consumers.

However, the complex structure of the IoT market may not only obscure which provider is responsible for a particular problem in the value chain, but also which authority can help consumers and be involved in the policy decision-making and enforcement process. In the NFC area, regulatory responsibilities for both the development of NFC-related rules and their enforcement are quite fragmented in some countries. One example of this is Australia (Box 6.7), although it is likely other countries have similar structures.

The ongoing development of separate responses to emerging technology developments risks an overall loss of regulatory coherence, with consequences for industry participants in terms of increased compliance costs. For consumers, increased complexity and regulatory fragmentation can make it more difficult to manage their communications experience. A single regulatory framework, or at least a joint approach, for addressing the changing dimensions of IoT activities would offer a more coherent arrangement for both businesses and consumers engaging in such activities.

Undoubtedly, much of the unease that surrounds the IoT stems from a lack of consumer understanding and awareness. A recent survey found that although mass adoption of connected technology is likely in the long term, the majority of consumers (87%) had not even heard of the term “The Internet of Things” (Aquity Group, 2014). The study concluded that the highest barrier to mass adoption of the IoT was not so much price or concerns about privacy, but a lack of both awareness and value perception of the new ecosystem among consumers. This strongly suggests that improving customer experience in this area, and educating consumers about the key functional characteristics

(e.g. connectivity, interactivity, telepresence, intelligence, convenience and security) and benefits (e.g. personalised offers and cost savings) of connected technologies, should be a high priority in building consumer trust and stimulating demand for the IoT (YaPing et al., 2014). Moreover, in situations where a household will have tens or even hundreds of connected devices, overall systems for managing these devices will become essential. As IoT apps proliferate, and in the face of the growing potential complexity of the market, integrated consumer interfaces will be essential to ensure that the desired simplicity of the IoT is maintained.

Box 6.7. **NFC regulation in Australia**

The Australian Communications and Media Authority (ACMA) requires industry to develop codes and standards to ensure that consumer protection is maintained in the telecommunications industry, and in a range of different areas, including privacy, maintenance of service standards and appropriate redress measures.

The ACMA, in its role as spectrum regulator, is responsible for planning and managing radio frequency spectrum as a public resource. Growth in the take-up and use of NFC-enabled services will also need to be accommodated in future spectrum demand planning and the management of spectrum interference.

The ACMA further provides consumer protection by requiring active devices, such as readers at a cash register or a mobile phone with an NFC chip, to meet relevant electromagnetic compatibility and emissions standards.

The Australian Securities and Investments Commission (ASIC) administers the e-Payments Code and related measures under the *Corporations Act 2001*. These regulate electronic payments, including internet/online payments and mobile banking.

The Australian Competition and Consumer Commission (ACCC), along with state and territory fair-trading agencies, enforce Australian consumer legislation, and provide consumer with guarantees for faulty NFC transactions in cases where consumers were incorrectly charged by a merchant or the contactless payment terminal was not operating properly.

The Attorney-General's Department, supported by the **Office of the Australian Information Commissioner (OAIC)**, administers the *Privacy Act 1988*, which outlines National Privacy Principles (NPPs). Organisations that facilitate NFC transactions need to comply with the Privacy Act regarding the information they hold.

Source: ACMA (2013).

6.4 Autonomous machines and public policy

The IoT will affect remote-controlled machines, machine learning and autonomous machines. The economic implications and the implications on sectoral regulations could be a topic for future research. Some of the main implications are related to employment and to the growth of autonomous machines. Furthermore, current regulations especially in transport assume human control of vehicles, which is not the case with remote-controlled and autonomous vehicles. At present, there is therefore an absence of regulation that explicitly allows the use of remote-controlled and autonomous machines and/or regulates their use.

Policy implications of autonomous machines on employment and growth

A question that arises around the IoT is its implications for employment. Brynjolffson and McAfee (2011) mention in their book *Race against the Machine* a possible future, where machine learning allows robots to replace humans in many "lower skilled" jobs. Their book aimed to bring technology into the discussion on unemployment and the global financial recession. The "End of Work", as this hypothesis is known, after a book by Jeremy Rifkin, has been proposed by many economists, but has received only minor attention as technological changes have generally been accompanied by increases in employment in other parts of the economy, such as the services economy and the IT industry. To many economists, the proposition is therefore also known as the Luddite fallacy (*Economist*, 2011). John Maynard Keynes used a different term as early as 1930, stating:

> *We are being afflicted with a new disease of which some readers may not yet have heard the name, but of which they will hear a great deal in the years to come-namely, technological unemployment. This means unemployment due to our discovery of means of economising the use of labour outrunning the pace at which we can find new uses for labour. But this is only a temporary phase of maladjustment (Keynes , 1930).*

Economist Alex Tabarrok's summary of the concept states that "[if] the Luddite fallacy were true, we would all be out of work because productivity has been increasing for two centuries" (Tabarrok, 2003). Robert Gordon states:

> *In setting out the case for pessimism, I have been accused by some of a failure of imagination. New inventions always introduce new modes of growth, and history provides many examples of doubters who questioned future benefits. But I am not forecasting an end to innovation, just a decline in the usefulness of future inventions in comparison with the great inventions of the past (Gordon, 2012).*

This last statement evokes a general pessimism regarding the extent to which much new technology can add to the growth of the economy.

While there are different views on the implications of technological change for employment, the IoT promises to increase their scale and reach. Brynjolffson and McAfee point to the introduction of mechanisation at the start of the twentieth century, which led to an almost complete replacement of the use of horses in only two decades. In many ways, the world is today at the dawn of machine learning, similar to its position in 1994 with respect to the Internet. Practical commercial examples are now available, but much is still to be learned. Technology has moved quickly and the integration of low-cost electronics, large-scale processing power and ubiquitous networking has made possible new generations of autonomous and semi-autonomous machines. These machines are moving into every part of the economy and are displacing work in various sectors. This could theoretically lead to workerless factories. Even if it causes only temporary friction problems in the economy, as Keynes once suggested, it is a development that policy makers need to consider. Machine learning is as much about the competitiveness of the economy as it is about labour policy.

The competitiveness of the market of an economy is dependent upon having the most efficient tools and processes. It is, therefore, likely that countries that invest more in the development of machine learning and autonomous systems will benefit to a greater extent from them. Whether this will lead to economic growth and/or influence jobs is food for debate among economists. What is likely, however, is that if robotic warehouses perform as well as argued by those responsible for their implementation, then jobs in the warehouse sector will decrease and companies will compete to build more efficient warehouses. This

will lead to greater efficiency, which in turn lead will lead to greater purchasing power for consumers. It could also lead to job loss and friction problems in the economy that cost society economic growth. That the market is moving in this direction is exemplified by Wehkamp.nl, a Dutch online retailer, which announced in October 2013 that it would build the world's largest robotic distribution centre to replace its traditional warehouse. This centre will permit order-to-package times of 30 minutes and same-day delivery, which customers will likely appreciate.[29] Robots will manage the warehouse, pick goods, and move to and from picking stations, where employees will pick and pack the goods.

In the area of manufacturing, robots will likely replace many labour intensive tasks that are presently too difficult or too expensive to execute by robot. For policy makers keen to repatriate manufacturing to their countries from low-cost labour countries, the resultant effect might not produce the number of jobs traditionally associated with the sector. For the least developed economies, the traditional development path from assembly of low-cost clothing and goods, via low-cost electronics, to high tech will be cut off because the assembly of higher value goods will be performed in developed countries by robots.

Many other "routine" jobs may also disappear in the coming years. If autonomous vehicles are a success, then autonomous taxis, buses and trucks would be likely candidates. Some jobs that in the past absorbed unskilled or low-skilled workers may no longer exist. Jobs will still be associated with providing these functions; however, many of them will require higher skills, for example, repair and programming of robotic functions. Having a skilled labour force is therefore crucial. On the other hand, there are also cost savings associated with autonomous machines, which may allow re-employment of people in other parts of the economy.

Autonomous machines, whether in transport or manufacturing, are dependent upon reliable infrastructures. Autonomous technologies can only provide their full benefits when countries have dependable transport, energy and communications networks. The vision of an entirely robotic production process can only exist if each element fits well with the next, because despite its increased flexibility, machine learning will not have the ability to deal with adversity. For example, a human factory worker may be able to reorganise some of the work in the event of an electricity failure. Similarly, failing communications systems may be detrimental to the functioning of autonomous taxis, which might not be able to find new passengers, but a human driver will still be able to identify a waiting passenger. Therefore, a well-functioning infrastructure will be essential.

Policy implications of autonomous machines for regulation

Autonomous and remote-controlled machines are used mainly in controlled environments at present. However, they will form a major part of the IoT. Regulation in controlled environments consists mostly of adequate health and safety measures, which often translates into a switch that turns the robot off when an employee enters the operations area. This will change with the newest generation of autonomous machines, where humans and machines will interact and co-operate. The legal context of these machines will as a result change, dramatically.

A number of countries and companies are actively testing driverless cars on public roads. Google in the United States is the best-known example, but every major car manufacturer has a prototype programme that deals with autonomous vehicles. For the near future, companies are focusing on near-autonomous vehicles. The first applications can be found in driver assisted systems, some of which are already available, for example,

to allow autonomous driving in low-speed traffic jam environments or to allow automatic parking. These applications will expand over time to allow automatic cruising on highways. Some automobile manufacturers, however, expect to bring near or fully autonomous vehicles on the market between 2017 and 2020.

The legality of use of automated vehicles, be they airborne or on the road, is much more complex. Existing international treaties, as well as national and local regulations, were not written with autonomous or remote-controlled vehicles in mind. International treaties to which the majority of OECD countries are signatories include the 1949 Geneva Convention on Road Traffic and the 1968 Vienna Convention on Road Traffic. These require a driver to be present. Some countries disagree on the definition of "driver" and on whether an automated function would fit the treaty definition.

Stanford University's Cyber Law Center assumes that as long as a human operator can take over control, the treaties do not prohibit automated vehicles (Smith, 2012). "Possibly the condition is also satisfied if that vehicle operates within the bounds of human judgment. These interpretations may not require a human to be physically present" (Smith, 2012). It is therefore important that the definitions be clarified or modified for autonomous vehicles to become a possibility in all signatory countries.

In the United States, some states including California, Florida and Nevada have now enacted legislation that allows the use of autonomous vehicles. These laws do not resolve all legal issues surrounding their use, but they do explicitly recognise the existence of autonomous vehicles and authorise their use in the state. According to the analysis of Stanford University, areas that will require attention include: vehicle standards, general tort liability, insurance, data collection, transportation planning and environmental impact assessment.

The United Kingdom held a consultation in 2014, with a first trial to be conducted in 2015 in Greenwich. The government plans to publish a Code of Practice in early 2015 for those who want to test driverless vehicles on the roads of the United Kingdom. Officials have said that they want "a light touch/non-regulatory approach" to testing self-driving cars in order to get such automobiles on the road faster. "A Code of Practice will be quicker to establish, more flexible and less onerous for those wishing to engage in testing than the regulatory approach being followed in other countries" (Mlot, 2015). In the Netherlands, the government has stated that it wants to become a testbed for the use of autonomous vehicles and has approved their use on the road. In Korea, however, despite research at national research institutes, the Road Traffic Act requires a driver to be present in the vehicle.

(Light) unmanned remote-piloted aircraft systems (RPAS), also known as Unmanned Aerial Vehicles (UAV) or drones, are allowed in some OECD countries. In Japan, for example, remote-controlled helicopters are used to spray 40% of the rice crop. A roadmap for RPAS prepared for the European Commission states that the Czech Republic, France, Ireland, Italy, Sweden, Switzerland and the United Kingdom currently have national rules and regulations in place. National regulations are also being prepared in Belgium, Denmark, the Netherlands, Norway and Spain (EC, 2013). In Korea, RPAS above 150 kilograms are forbidden, whereas those under 150 kilograms need to file 18 documents seven days prior to a flight. Only RPAS under 12 kilograms are exempt from these rules. In the United States, the FAA is working to produce regulations. However, at this moment commercial use of RPAS is restricted. Autonomous piloted aircraft systems are not yet part of the regulatory roadmap because the International Civil Aviation Authority is currently limiting itself to RPAS. RPAS are also used in many military applications and, as a result, are listed on the

export control list of Wassenaar Arrangement countries, to which many OECD countries adhere (category 9.A.12). This means that farmers in Australia cannot buy remote-controlled helicopters from Japan, but have to hire them as a service from the manufacturer, complete with a pilot. Future work could examine possible regulation of this sector in greater detail.

That regulation is necessary was demonstrated by an incident in Sweden, where all traffic to and from Stockholm's Bromma airport was halted because of a commercial, but unauthorised drone flight in the airport's control zone over central Stockholm.[30] The airport remained closed for an hour until the drone operator was located. In the United Kingdom, the pilot of an Airbus 320 on approach for a landing at Heathrow airport reported a drone passing 7 metres over the left wing. The Airbus was at that time 213 metres above the ground. An investigation was held, but the operator of the drone was not found. These are not the only episodes known to involve RPAS, but they serve as an indication of the seriousness of possible future incidents.

Notes

1. Merriam-Webster defines an actuator as "a mechanical device for moving or controlling something". While a sensor can be used to ascertain the state of a system, an actuator can be used to change that state.
2. For a list of milestones in the evolution of the blending of the physical with the digital, see Gil Press (2014).
3. For information on the cost of RFID readers, see: *www.rfidjournal.com/site/faqs#Anchor-If-36680*.
4. Decree 8234 of 2 May 2014, found at *http://leisonline.blogspot.fr/2014/05/decreto-n-8234-de-2-de-maio-de-2014.html#!/2014/05/decreto-n-8234-de-2-de-maio-de-2014.html* (accessed 15 April 2015).
5. For a further discussion of definitions of the Internet of things see Evans (2011). For a more academic evaluation of definitions, see Atzori, Iera and Morabito (2010).
6. This is not a fully accurate depiction of the changes machine learning is undergoing as a result of advances in Bayesian analysis and might be too negative of prior work in the field of machine learning. However, a discussion of the nuances involved would be too technical for the present report.
7. Similar predictions have been made by researchers and engineers of vehicle manufacturers in conversations with OECD staff.
8. Power-line communication carries data on a conductor that is also used simultaneously for AC electric power transmission or electric power distribution, while Power over Ethernet (PoE) passes electrical power along with data on ethernet cabling.
9. Transport for London, "What is a Contactless Payment card?", *www.tfl.gov.uk/fares-and-payments/contactless/what-is-contactless?intcmp=8610* (accessed 15 April 2015).
10. A star network is a computer network topology which consists of one central switch, hub or computer, which acts as a conduit to transmit messages.
11. SITA's website is here: *www.sita.aero/about-us*.
12. 802.15.4 is a layer 2 protocol, which defines modulation, power output, frequencies used and a number of other elements necessary to make communication possible. Zigbee, Thread and 6LowPan are layer 3 and higher protocols that define how the network will organise itself, how addressing is done, how routing becomes possible and data is packaged. An 802.15.4 wireless device that uses one layer 3 protocol can make itself heard, but is not understood by devices that use a different layer 3 protocol.
13. The term "native" is used when the infrastructure supports IPv6 from the bottom up and each device receives an IPv6 address. Non-native use describes when there are translation mechanisms to move from IPv6 to another underlying protocol.
14. See *http://en.wikipedia.org/wiki/IEEE_802.15.4*.
15. Time periods can be brief lasting only seconds, or longer lasting minutes.

16. Energy network operators in the Netherlands manage the physical connections to the electricity and gas grid network. They are structurally separated network operators, who cannot generate electricity, sell retail services to end users or operate the national high voltage distribution grid.

17. The OECD has published a number of reports on IPv6. For an overview, see: *www.oecd.org/sti/ieconomy/telecomandinternetreports.htm#Internet*.

18. Cisco Visual Networking Index 2014 states: "The number of devices connected to IP networks will be nearly twice as high as the global population in 2018. There will be nearly three networked devices per capita by 2018, up from nearly two networked devices per capita in 2013. Accelerated in part by the increase in devices and the capabilities of those devices, IP traffic per capita will reach 17 GB per capita by 2018, up from 7 GB per capita in 2013" (Cisco, 2014). The UN estimates the world population to be 7.5 billion in 2018. The estimate from Cisco Internet Business Group is found in Evans (2011).

19. The calculation adjusts the initial estimate for a family of four to an average household size.

20. Mobile networks currently still require each SIM card to be assigned at least one e.164 telephone number. This may change in the future, but so many systems now expect a phone number for billing and management purposes, that moving to other types of numbers may take considerable time.

21. Carrier Grade Network Translation is the term used when the Network Address Translation (NAT) is performed at the core of the network instead of at the edge. Millions of devices may simultaneously share the same pool of addresses, requiring a much higher throughput and reliability then NAT in a home DSL router. Carrier Grade NAT is the only way to perform NAT in a mobile wireless network, because the network translation cannot easily be handled by devices at the edge.

22. Online posts regarding such concerns can be found at: *www.medhelp.org/posts/Heart-Rhythm/Why-does-cardionet-event-monitor-record-when-nothing-is-wrong/show/1393291* and *www.medhelp.org/posts/Heart-Rhythm/30--day-Cardionet-Monitor-going-off-by-itself/show/1089961*.

23. Several countries have examined GPS-based road pricing, but so far have not moved forward. A lack of support from rule makers or complex demands, for example, by allowing pre-booking of slots and so forth, can create delays in their introduction. See, for example: *http://roadpricing.blogspot.nl/2011/08/uk-concludes-gps-based-distance-road.html*, *http://en.wikipedia.org/wiki/Road_pricing* and *www.nce.co.uk/news/transport/government-collapse-scuppers-dutch-road-pricing-plans/5216811.article*.

24. A leaflet entitled "The Smart Metering System", published by the UK Department of Energy and Climate Change, can be found at: *www.gov.uk/government/uploads/system/uploads/attachment_data/file/336057/smart_metering_leaflet.pdf*.

25. See *http://ec.europa.eu/digital-agenda/en/internet-things*.

26. See *Besluit van de Minister van Economische Zaken van 3 maart 2014, nr. ETM/TM/14024019, houdende wijziging van het Nummerplan voor identiteitsnummers ten behoeve van internationale mobiliteit (IMSI-nummers) in verband met het gebruik van IMSI-nummers door besloten netwerken* (in Dutch), *https://zoek.officielebekendmakingen.nl/stcrt-2014-6781.html*.

27. See *www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm*.

28. For more information, see the "7 Foundational Principles" on the Privacy by Design website, *www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/*.

29. A clip of the announcement and the new distribution centre can be seen at *www.youtube.com/watch?v=Q5eie0IgccY* (in Dutch).

30. For the Heathrow incident the official Air Proximity report (no. 2014117) can be found at *www.airproxboard.org.uk/docs/423/2014117.pdf*. The Swedish incident was described in the press, for example, at Airscoc (2014).

References

ACMA (2013), *Near-field communications. Emerging Issues In Media and Communications*, Occasional Paper, No. 2. Australia Communications and Media Authority, Canberra, *http://165.191.2.87/~/media/Regulatory%20Frameworks%20and%20International%20Coordination/Information/pdf/Near%20field%20communications%20Emerging%20issues%20in%20media%20and%20communications%20Occasional%20paper%202.pdf*.

Airsoc (2014), "Airspace around Stockholm-Bromma briefly closed following drone sighting", *Airsoc* webpage, *http://airsoc.com/articles/view/id/5480fa8d31394477768b456a/airspace-around-stockholm-bromma-briefly-closed-following-drone-sighting* (accessed 15 April 2015).

Alzheimer's Society (2014), DementiaFriendly Technology: A Charter That Helps Every Person With Dementia Benefit From Technology That Meets Their Needs, Alzheimer's Society, London, *www.telecare.org.uk/sites/default/files/file-directory/Publications/Dementia%20Friendly%20Technology%20Charter.pdf*.

Aquity Group (2014), *The Internet of Things: The Future of Consumer Adoption*, *www.acquitygroup.com/news-and-ideas/thought-leadership/article/detail/acquity-group-2014-internet-of-things-study* (accessed 15 April 2015).

Atzori, L., I. Antonio and G. Morabito (2010), "The Internet of Things: A survey", *Computer Networks*, Vol. 54/15, pp. 2787-2805, *www.sciencedirect.com/science/article/pii/S1389128610001568*.

Baudoin, C. (2014), "The Internet of things: Automation heaven or security hell?", *Cutter Consortium* website, *www.cutter.com/content/bia/fulltext/updates/2014/biau1403.html* (accessed 15 April 2015).

BIPT (2014), Raadpleging op vraag van de raad van het BIPT van 25 november 2014 met betrekking tot de herziening van het beleid inzake het beheer van het nummerplan (*Consultation at the request of the board of BIPT of 25 November 2014 in relation to the policy review on the management of the numbering plan)*, Belgisch Instituut voor Postdiensten en Telecommunicatie, Brussels, *www.bipt.be/public/files/nl/21394/Consult_review_KB_Nummering_NL.pdf*.

Brill, J. (2014), "The Internet of Things: Building trust to maximize consumer benefits", speech at The Internet of Things: Roundtable with FTC Commissioner Brill, Center for Policy on Emerging Technologies, Washington DC, 26 February 2014, *www.ftc.gov/system/files/documents/public_statements/203011/140226cpetspeech.pdf*.

Brynjolfsson, E. and A. McAfee (2011), *Race Against the Machine*, Lexington, MA, Digital Frontier Press.

BT (2014), *Promoting Investment and Innovation in the Internet of Things*. Ofcom Internet of Things Consultation – BT Response, British Telecom, London, *http://stakeholders.ofcom.org.uk/binaries/consultations/iot/responses/BT.pdf*.

Capgemini (2014), "Internet of Things = Internet of trust", *Capping IT Off* blog, 19 September 2014, *www.capgemini.com/blog/capping-it-off/2014/09/internet-of-things-internet-of-trust*.

Cisco (2014), *Cisco Visual Networking Index: Forecast and Methodology, 2013–2018*, Cisco Systems, Inc., *www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html* (accessed 15 April 2015).

Co.Exist (2014), "7 tools that let you control your own data", *CoExist* website, *www.fastcoexist.com/3024857/world-changing-ideas/7-tools-that-let-you-control-your-own-data* (accessed 15 April 2015).

Connected World (2014), *Two Views: Is It Too Soon to Move to 4G/LTE?* Aug/Sept 2014, *http://connectedworld.com/two-views-is-it-too-soon-to-move-to-4glte/* (accessed 15 April 2015).

Das, R. and P. Harrop (2014), *RFID Forecasts, Players and Opportunities 2014-2024*, IDTechEx, *www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2014-2024-000368.asp* (accessed 15 April 2015).

EC (2014), *Benchmarking Smart Metering Deployment in the EU-27 with a Focus on Electricity*, EC Report, No. COM(2014) 356 final, European Commission, Brussels, *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0356&from=EN*.

EC (2013), *Roadmap for the Integration of Civil Remotely-Piloted Aircraft Systems into the European Aviation System*, Final Report from the European RPAS Steering Group (ERSG), European Commission, Brussels, *http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf*.

ECC (2014), *Evolution in the Use of E.212 Mobile Network Codes*, ECC Report, No. 212, CEPT Electronic Communications Committee, *www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP212.PDF*.

Economist (2011), "Difference engine: Luddite legacy", *The Economist*, 4 November 2011, *www.economist.com/blogs/babbage/2011/11/artificial-intelligence* (accessed 15 April 2015).

Edge (2012), "Reinventing society in the wake of big data: a conversation with Alex (Sandy) Pentland", *Edge*, 30 August 2012, *http://edge.org/conversation/reinventing-society-in-the-wake-of-big-data* (accessed 15 April 2015).

Evans, D. (2011), *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper, CISCO IBSG, *www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf*.

GigaOm (2014), "Ericsson CEO predicts 50 billion Internet connected devices by 2020", *GigaOm*, 14 April 2014, *https://gigaom.com/2010/04/14/ericsson-sees-the-internet-of-things-by-2020/* (accessed 15 April 2015).

GigaOm (2009), "Intel inside becomes Intel everywhere", *GigaOm*, 2 March 2009, *https://gigaom.com/2009/03/02/intel-inside-becomes-intel-everywhere/* (accessed 15 April 2015).

Gil Press (2014), "A very short history of the Internet Of Things", *Forbes*, 18 June 2014, *www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/* (accessed 15 April 2015).

Gordon, R.J. (2012), "Why innovation won't save us", *Wall Street Journal*, 21 December 2012, *http://online.wsj.com/articles/SB10001424127887324461604578191781756437940* (accessed 15 April 2015).

Harwell, D. (2014), "Whirlpool's 'Internet of Things' problem: No one really wants a 'smart' washing machine", *The Washington Post*, 28 October 2014, *www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/whirlpools-internet-of-things-problem-no-one-really-wants-a-smart-washing-machine/* (accessed 15 April 2015).

Hearn, A. (2014), "Sir Tim Berners-Lee speaks out on data ownership", *The Guardian*, 8 October 2014, *www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership* (accessed 15 April 2015).

IEI (2014), *Utility-scale Smart Meter Deployments: Building Block of the Evolving Power Grid*, Institute for Electric Innovation, The Edison Foundation, Washington DC, *www.edisonfoundation.net/iei/Documents/IEI_SmartMeterUpdate_0914.pdf*.

Keynes, J.M. (1963), "Economic possibilities for our grandchildren", *Essays in Persuasion*, W.W.Norton & Co., New York, pp. 358-373, *www.econ.yale.edu/smith/econ116a/keynes1.pdf*.

KrebsonSecurity (2012), "FBI: Smart meter hacks likely to spread", *KrebsonSecurity*, 12 April 2012, *http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/* (accessed 15 April 2015).

Kvalbein, A. (2012), *Measuring Mobile Broadband in Norway*, Simula Research Laboratory, RIPE 64, *https://ripe64.ripe.net/presentations/172-Mobile_Broadband_Measurements.pdf*.

Lee, T.B. (2015), "5 reasons self-driving taxis are going to be amazing", *Vox*, 17 March 2015, *www.vox.com/2015/3/17/8231401/self-driving-taxis-amazing* (accessed 15 April 2015).

Liebenau, J. et al. (2011), *Near Field Communications: Privacy, Regulation & Business Models*, A white paper of the LSE/Nokia research collaboration, *www.lse.ac.uk/management/documents/LSE-White-Paper_-_Near-Field-Communications-Privacy-Regulation-Business-Models.pdf* (accessed 15 April 2015).

Kelly, S.M. (2014), "World's first connected tennis racquet will perfect your swing", *Mashable*, 7 January 2014, *http://mashable.com/2014/01/07/connected-tennis-racquet/* (accessed 15 April 2015).

Ministry of Science, ICT and Planning (Republic of Korea) (2014), *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, Ministries of the Republic of Korea, Seoul, *www.iotkorea.or.kr/2013_kor/uploadFiles/board/KOREA-%20IoT%28Internet%20of%20Things%29%20Master%20Plan%20-%202014.pdf*.

Mlot, S. (2015), "Driverless cars hitting U.K. roads this summer", *PC Magazine*, 11 February 2015, *www.pcmag.com/article2/0,2817,2476609,00.asp* (accessed 15 April 2015).

OECD (2015), *Trust in a Data-Driven Economy: Data and Analytics: Prospects for Growth and Well-being*, OECD, Paris.

OECD (2014), *Summary of the OECD Privacy Expert Roundtable on Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, OECD Publishing, Paris, *www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en* (accessed 15 April 2015).

OECD (2013a), "Building blocks for smart networks", *OECD Digital Economy Papers*, No. 215, OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/5k4dkhvnzv35-en*.

OECD (2013b), "Cloud computing: The concept, impacts and the role of government policy", *OECD Digital Economy Papers*, No. 240, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5jxzf4lcc7f5-en*.

OECD (2013c), "Exploring data-driven innovation as a new source of growth: Mapping the policy issues raised by 'big data'", *OECD Digital Economy Papers*, No. 222, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5k47zw3fcp43-en*.

OECD (2012a), "Machine-to-machine communications: Connecting billions of devices", *OECD Digital Economy Papers*, No. 192, OECD Publishing, Paris, *http://dx.doi.org/10.1787/5k9gsh2gp043-en*.

OECD (2012b), "Terms of Reference for the Review of the OECD Guidelines for the Security of Information Systems and Networks", *OECD Digital Economy Papers*, No. 210, OECD Publishing, Paris, *http://dx.doi.org/10.1787/5k8zq92zhqhl-en*.

OECD (2010), *OECD Information Technology Outlook 2010*, OECD Publishing, Paris, *http://dx.doi.org/10.1787/it_outlook-2010-en* (accessed 15 April 2015).

Ofcom (2014), *Promoting Investment and Innovation in the Internet of Things*, Ofcom, London, *http://stakeholders.ofcom.org.uk/consultations/iot/* (accessed 15 April 2015).

Pasiewicz, M. "On people, the death of privacy, and data pollution", interview with Bruce Schneier, *Schneier on Security*, *www.schneier.com/news/archives/2008/03/on_people_the_death.html* (accessed 15 April 2015).

Rauhofer, J. (2008), "Privacy is dead, get over it! Information privacy and the dream of a risk-free society", *Information & Communications Technology Law*, Vol. 17/3, *www.tandfonline.com/doi/abs/10.1080/13600830802472990#.VDWAHUvgp5k* (accessed 15 April 2015).

Rubens, P. (2014), "Internet of Things a potential security disaster", *eSecurity Planet*, 4 September 2014, *www.esecurityplanet.com/network-security/internet-of-things-a-potential-security-disaster.html* (accessed 15 April 2015).

Smith, B.W. (2012) "Automated vehicles are probably legal in the United States", *The Center for Internet and Society*, *http://cyberlaw.stanford.edu/publications/automated-vehicles-are-probably-legal-united-states* (accessed 15 April 2015).

St. John, J. (2014), "4 ways Tokyo's smart meter plan breaks new ground", *Greentechgrid*, 19 March 2014, *www.greentechmedia.com/articles/read/4-ways-tokyos-smart-meter-plans-break-new-ground* (accessed 15 April 2015).

Tabarrok, A. (2003), "Productivity and unemployment", *Marginal Revolution*, 31 December 2003, *http://marginalrevolution.com/marginalrevolution/2003/12/productivity_an.html*.

US FTC (2014), *In the matter of TRENDnet. Docket no. C-4426. Decision and Order*. United States Federal Trade Commission, Washington DC, *www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf*.

WEF (2014), *Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems*, World Economic Forum, Geneva, *www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf*.

Weiser, M. (1991), "The computer for the 21st century", *Scientific American*, Vol. 265/9, pp. 66–75.

Wilson, J. (2008), *Sensor Technology Handbook*, Newnes/Elsevier, Oxford.

Wolf, C. and J. Polonetsky (2013), "An Updated Privacy Paradigm for the 'Internet of Things'", *Future of Privacy Forum*, 19 November 2013, *www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf*.

YaPing, C. et al. (2014), "Influence of characteristics of the Internet of Things on consumer purchase intention", *Social Behavior and Personality*, Vol. 42/2: 321-330.

Yared, P. (2013), "2013: The Internet of things, delivered via smartphone", *VentureBeat*, 2 January 2013, *http://venturebeat.com/2013/01/02/internet-of-things-via-smartphone/* (accessed 15 April 2015).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(93 2015 04 1P1) ISBN 978-92-64-23227-3 – 2015

OECD Digital Economy Outlook 2015

Contents

Chapter 1. An overview of the digital economy
Chapter 2. The foundations of the digital economy
Chapter 3. The growing and expanding digital economy
Chapter 4. Main trends in communication policy and regulation
Chapter 5. Trust in the digital economy: Security and privacy
Chapter 6. Emerging Issues: The Internet of Things

Consult this publication on line at ***http://dx.doi.org/10.1787/9789264232440-en.***

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases. Visit ***www.oecd-ilibrary.org*** for more information.

OECD*publishing*
www.oecd.org/publishing

ISBN 978-92-64-23227-3
93 2015 04 1 P