**For Official Use** **DSTI/CDEP(2017)2/CHAP6**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **10-May-2017**

**English - Or. English**

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION**
**COMMITTEE ON DIGITAL ECONOMY POLICY**



**Cancels & replaces the same document of 24 April 2017**

**Digital Economy Outlook 2017**

# CHAPTER 6: POLICY AND REGULATION

**17-19 May 2017**

*[This document includes a revised introduction and an updated chapter structure]*

*Attached is chapter 6 of the Digital Economy Outlook 2017.*

*CDEP and CCP delegates are invited to discuss the chapter and provide comments by 31 May.*

*The chapter will be declassified by written procedure.*

Jeremy West, Jeremy.WEST@OECD.org, Tel +33 145241751; Christian Reimsbach-Kounatze, Christian.REIMSBACH-KOUNATZE@oecd.org; Elettra Ronchi, Elettra.RONCHI@oecd.org, Michael.DONOHUE@oecd.org; David Gierten, David.GIERTEN@oecd.org, Tel +33 145249682

**JT03413945**

**TABLE OF CONTENTS**



**Tables**



**Figures**

**Boxes**

# 6. POLICY AND REGULATION

## Introduction

1. This chapter discusses policy and regulation in the areas of access and connectivity, ICT usage and skills, innovation, applications, and transformation, and digital risk and trust. Although these areas might seem rather distinct, policy issues in each of them are increasingly interrelated and need to be considered from an overarching perspective. As underlined in Chapter 1, fully seizing the benefits of the digital economy requires a whole-of-government approach that pro-actively addresses the broad range of policy issues and their relationships across policy areas.

2. For example, the Internet of Things (IoT) may soon be a commonplace of daily life, with many billions of interconnected objects around the world. "Smart" devices, equipment, machines and infrastructure are creating opportunities for automation and for interaction in real time. IoT applications and services, enhanced by data analytics, are expected to help to reinvigorate industry, meet some of the needs of increasingly elderly populations, function as core elements of smart cities, and support the achievement of the sustainable development goals.

3. But to unleash the potential economic and social benefits that are associated with the IoT – and digital technologies more generally – an enabling, comprehensive policy framework is needed. That framework would include interdependent policies for building out the necessary infrastructure and fostering interoperability (Chapter 2 discussed trends in this area), developing the necessary skills for effective use by individuals, firms and governments (Chapter 3), promoting innovation, applications and transformation (Chapter 4), and finally, building trust (Chapter 5) in digital technologies, including the IoT.

4. Governments continue to align digital economy priorities directly with certain socioeconomic objectives, such as improving care for the sick and elderly, giving more career opportunities to girls and women, providing better educations to poor children and those who live in remote areas, and promoting growth and employment. Leading priorities in this context include furthering access to high-speed broadband networks and overhauling laws to improve the speed and coverage of communication services (6.1). Many countries have also focussed on providing training and spurring innovation in the ICT sector (6.1), as well as on encouraging ICT usage through e-government, training programmes and subsidies (6.2). At the same time, countries continue to address the challenges and risks arising from the digital transformation by introducing National Digital Security Strategies, while privacy protection continues to rise on governments' agendas (6.4).

5. It has also become clearer than ever that the digital transformation can be disruptive, and that well-considered policies are needed not only to allow the disruption to occur, but to encourage it so that its benefits can be realised fully and without unnecessary delays. Thus countries have launched initiatives aimed at helping start-ups or young SMEs through accelerators or incubators (6.1) and have promoted digital applications and services with a variety of policy measures (6.3). However, measures are also needed to cushion the blow when the digital transformation displaces workers and to protect consumers in the new commercial settings that are evolving. Consequently, policies in support of vocational training and higher education in ICT are common, may involve partnerships with the private sector, and sometimes aim

to assist specific groups such as the unemployed (6.2). Furthermore, the digital transformation of jobs has triggered reviews of labour laws and sector-specific employment rules (6.3). Meanwhile, as the e-commerce marketplace evolves so do policy responses to protect consumers and ensure trust. For example, policymakers have begun to grapple with the challenge of applying consumer protection frameworks to peer platform markets. They have also taken steps to address consumer protection-related impediments to cross-border e-commerce (6.4).

6. In sum, the digital transformation is an opportunity to be welcomed, but it also brings certain challenges that need to be managed. Generally speaking, the digital transformation is changing the world faster than many rules and regulations have evolved. Governments can benefit from mechanisms to periodically review their regulatory frameworks and, where appropriate, update them to ensure that they are well-suited to the increasingly digitalised world.

7. Much of the information in this chapter is drawn from responses to the 2016 OECD Digital Economy Outlook (DEO) Policy Questionnaire. All OECD countries, as well as seven non-Members, submitted responses to at least one of the eight sections of the questionnaire.

## 6.1 Access and Connectivity

8. The digital economy relies on efficient access and effective use of communication infrastructures and services. In June 2016, discussions at the OECD Cancun Ministerial on the Digital Economy underlined the determination of policy makers to improve high-speed communication infrastructures and services in ways that boost competitiveness and enable greater participation in the opportunities they create. A key challenge in this respect was assessing policies and regulation in light of convergence between formerly distinct sectors such as telecommunication and broadcasting and the need for different parts of government to work more closely to meet challenges and seize opportunities posed by changes in communication markets.

9. This section is based on responses to the telecommunication section of the 2016 OECD DEO Policy Questionnaire by all OECD countries and Colombia. It reviews recent changes in communication policies, communication laws and regulatory frameworks, and then discusses developments in convergence and the associated developments in market structures. It further examines changing responsibilities of communication regulators affected by convergence of the telecommunication and broadcasting sectors, and looks at interconnection between networks and the significant developments in international mobile roaming.

10. The key findings of this section are that convergence in the telecom and broadcasting markets is driving changes in regulatory approaches including a move to more converged regulators and governments undertaking convergence reviews to reform regulation. There is a trend towards removing regulation especially in fixed telecom markets and towards infrastructure-sharing mechanisms and ensuring competition. The market has been found to largely self- regulate peering and transit agreements between internet service providers. In international mobile roaming, regulation is emerging to ensure competition exists through Roam Like at Home (RLAH) offer, while at the same time some technological innovations are emerging as substitutes to regular international roaming services. In terms of developing the ICT sector itself, governments devote the largest focus on encouraging innovation in SMEs and start-ups, followed by supporting businesses to invest and export as ways to further their impact. The most commonly used policies are governmental funding projects or training programmes aimed at giving businesses the tools they need to innovate, followed by incubators and accelerators, which are hybrids, combining both a monetary aspect along with a training component and is primarily directed at SMEs and start-ups.

***Several OECD countries have adapted regulation and promoted infrastructure sharing mechanisms***

11. Over the previous two years, communication policy makers and regulators have been active in furthering access to high-speed broadband networks and adapting regulatory frameworks. The following provides a brief overview of communication reviews as well as changes in policies and regulatory frameworks across OECD countries, the results of which are expected to be positive in spurring competition, innovation and investment in communication markets.

12. Several OECD countries are currently reviewing their regulatory frameworks, public policies and telecommunication laws. Overall, a trend towards revisions that remove some regulation, mainly in the fixed telecommunication market, can be observed. Switzerland, for example, launched a public consultation on a partial revision of its telecommunication law, particularly to *(i)* strengthen the consumer's position in the communication market and to better protect youth, *(ii*) to limit international roaming prices, (*iii*) to render the use of spectrum more flexible, *(iv)* to reduce administrative burdens for telecommunication operators, and (*v*) to improve network access conditions for the different market players. Based on the consultation, the Swiss Federal Council tasked the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to prepare a draft version of the Telecommunications Act (TCS) by September 2017. Denmark has initiated a comprehensive review of public policy on electronic communication with stakeholder workshops and bilateral meetings. The review is planned to be concluded in 2017. The United Kingdom is carrying out a major review of the so-called *General Conditions*, i.e. the rules that all telecommunication companies have to meet in order to operate in the United Kingdom in the aim to make conditions clearer, reduce the cost of compliance, and lift regulation where rules are determined to be no longer necessary. In December 2016, the Swedish regulator PTS passed legislation to deregulate the fixed telephony market, putting in place a 12-month transitory period to fully enact the decision.

13. In September 2016, the European Union published its proposal to overhaul its telecommunications law, the European Electronic Communications Code (EC, 2016a), with the main objectives of increasing speed and coverage in the European Union area. The new proposal foresees adjustments in areas such as next generation access, spectrum licensing and a coordinated approach in the European Union towards spectrum management, regulatory obligations for electronic communications services including Over-the-Top (OTT) services, as well as must carry and electronic programming guides. It further plans to increase the powers of the European regulator BEREC. A further notable proposal in the directive is to amend numbering provisions in the machine-to-machine (M2M) market. The proposal allows "national regulators to assign numbers to undertakings other than providers of electronic communications networks and services", a reform that has been highlighted in several OECD reports as one which could improve competition (OECD, 2012b; 2015b).

14. To further spur competition in communication markets and reduce costs, many countries are increasingly working on infrastructure sharing provisions. For example, European Union member states must transpose the European Union Broadband Cost Reduction Directive (2014/61/EU) into national law (European Parliament and European Council, 2014). The directive addresses infrastructure sharing, information sharing and co-ordination of civil works between communication operators and utility operators to facilitate the roll-out of high speed broadband networks. It enables ISPs to get access to passive infrastructure of any network provider. In this respect, for example, Finland, Hungary, Ireland, Spain and Sweden have already enacted national legislation. The Czech Republic, Latvia and Slovenia are currently in the process of transposing the Directive into national law.

15. In mobile markets, OECD countries continue to open their 700 MHz spectrum band. Chile opened the band for commercial LTE ("long term evolution", a standard for high-speed mobile communications) services in May 2016. The three operators that won the spectrum license are obliged to

cover 1281 localities as well as 13 highways on a length of 850km. In 2017, Australia auctioned an additional 30 MHz of 700MHz spectrum that was left unsold in a 2013 round. Finland is preparing the auction for the 700 MHz band for the end of 2016. The auction will be a simultaneous multi-round auction whereby all spectrum blocks will be auctioned at the same time. It will be carried out over the Internet.[1] A total of six frequency pairs of five MHz each will be auctioned and no more than two frequency pairs of 5 MHz can be allocated to any individual organisation. Mexico licensed the 700 MHz band in the context of the creation of a mobile wholesale access network - the *Red Compartida*. Altán Redes was the auction winner, with a bid to cover 92.2% of the Mexican population. The company signed a Public-Private partnership with Promtel (*Organismo Promotor de Inversiones en Telecomunicaciones),* formally initiating work toward establishing the wholesale broadband network. . The United Kingdom plans to make the 700 MHz spectrum band available for use across the entire country by 2022, at the latest, and the EU plans to make the 700 Mhz band available for wireless broadband by 2020.

***Convergence contributes to revisions of regulatory frameworks and institutions***

*New players are offering audio-visual content delivery, spurring convergence in the telecommunication and broadcasting sectors*

16. New services have blurred the contours of the telecommunication and broadcasting sectors, which were previously distinct. In turn, this has tested existing (legacy) regulatory and policy settings and encouraged a reconsideration of these frameworks. The emergence of OTT video service providers and the popularisation of triple- or quadruple-play service bundles, for example, have made decisions on issues such as must-carry/must-offer obligations and copyright and retransmission harder to allocate between formerly distinct regulatory realms.

17. There is an increasing diversity of distribution channels for audio-visual content in OECD countries. Most countries now have offers from public and commercial television broadcasters that include the option to watch broadcast content via the Internet, both in real time (linear online streaming) and in an on-demand, non-linear fashion (e.g. catch up television). The offers vary in nature. While some provide real-time streaming only for subscribers, many offer linear streaming to the general public over the Internet (although these are often geo-restricted to the country or region of origin for copyright-related reasons). Regarding on-demand broadcast content, providers usually make it available for a limited time only and some require users to have a subscription for access.

18. Non-traditional players are also offering audio-visual content, especially through on-demand Internet platforms. However, as most OECD countries either do not regulate these services at all or regulate them very lightly[2], most regulators have not systematically collected data on these services and rely mostly on data from private sources. Intellectual property is another changing factor for audio-visual content. Historically, content developers have tried to segment these rights to different delivery platforms or performance windows. Acquisition of content by platforms (via recent or planned mergers or through deeper distribution agreements) may result in more innovative and flexible modes for consumers to enjoy content.

19. Many countries are considering how well regulation is adapted to the new environment. In December 2014, the FCC released a Notice of Proposed Rulemaking (NPRM) seeking comment on a proposal to modernise its interpretation of the term "multichannel video programming distributor" (MVPD) in the United States. This definition has been further refined in November of 2016, and expands the definition of MVPD to no longer be tied to a specific technology of distribution, such as television (FCC, 2016). This technical adjustment would give MVPDs that use the Internet (or any other method of transmission) the same access to programming owned by cable operators and the same ability to negotiate

to carry broadcast television stations that Congress gave to satellite systems to ensure competitive video markets. Additionally, this definition would still include video distributors should they change their delivery method from television to via the internet.

20. In Europe, as part of the Digital Single Market Strategy (EC, 2015), the European Commission adopted an amendment to the European Audio-visual and Media Services (AVMS) Directive in May 2016 and in September 2016 submitted a legislative proposal for an European Electronic Communications Code. That proposal would revise the five European Directives[3] and two European Commission regulations and turn them into one single instrument. The revised AVMSD sets a new approach to online platforms (including those without editorial responsibility for content, such as video-sharing platforms) by prohibiting hate speech, protecting minors, promoting European works across all content platforms and proposing rules for more responsible video-sharing platforms (EC, 2016a). It further proposes that OTTs would be subject to regulation only if they use numbering or are connected to the public switched telephone network (PSTN), congruent with BEREC's taxonomy (BEREC, 2015). Regulators in European Union member states would also be able to request information from OTTs.

21. Currently, most OECD countries have little regulation concerning audio-visual content provision by OTTs (which do not provide a licensed or authorised audio-visual service). Definitions of video-on-demand (VoD) services within legal frameworks in the OECD usually encompass services provided to consumers via a licensed broadcasting undertaking. In Canada, for example, VoD licensees are required to adhere to various programming codes that also apply to broadcasters and there are provisions preventing vertically integrated broadcasters from making television programming available on an exclusive or otherwise preferential basis. In Europe, consistent with the current AVMS Directive[4], notification from VoD providers can also be required, as in the United Kingdom and Hungary, which maintain national directories of all notified VoD service offerings.[5, 6]

*Convergence in the telecommunication and broadcasting sectors is a driver for mergers and acquisitions*

22. This convergence between previously distinct parts of the communication industry is the main driver for mergers and acquisitions (M&A) in OECD countries. Between 2014 and 2016, mergers or acquisitions between cable network operators and mobile network operators featured prominently among the transactions with a market value of around USD 500 million or above (Annex 1). However, as the case of Spain indicates, the trend towards convergence makes it harder for policy makers and regulators to assess outcomes (Box 1). Operators such as Vodafone purchased a number of fixed network operators while operators, such as BT, Liberty Global and Shaw Communications purchased mobile network operators (MNOs). In all cases the firms aim to offer a bundle of services, to benefit from the complimentary nature of the networks and to compete more effectively against rivals.

23. In October 2016, AT&T announced its intention to buy Time Warner for USD 85 billion. If approved by authorities, this will be one of the biggest upcoming M&As. Cable networks continue to merge with regional operators in countries such as Germany and the United States, while MNOs competing in the same market merged in Germany, Ireland and Italy. Meanwhile, in 2016, MNO mergers did not proceed in countries such as Denmark and the United Kingdom, where new entrants did not emerge from remedy negotiations.

**Box 1. Mergers and market developments in Spain**

Between 2014 and 2016, there were several mergers at the core of the digital economy in Spain. The largest were between Vodafone and ONO, which was approved in July 2014, as well as between Orange and Jazztel, in May 2015. In the first case, Vodafone, the second largest mobile operator, acquired ONO, the third largest fixed network operator with its own cable network in most parts of Spain and an MVNO. In the second case, Orange, the third largest

MNO and third largest fixed network operator, acquired Jazztel, the fourth largest fixed network operator. While both Orange and Jazztel primarily used unbundled local loops from Telefónica, they had also started significant investments in their own fibre networks. Jazztell also had an MVNO. This merger was approved by the European Commission with remedies that included:

- A bitstream wholesale offer to a competitor, using Orange's ULL access to Telefónica's fixed copper network, with cost-orientated prices, for a period of 4+4 years.
- The sale to a competitor of a fibre network in five Spanish cities, which covered nearly 800 000 homes or commercial units.
- Ensuring that the competitor has wholesale mobile access in attractive commercial conditions (including 4G), for a period of 4+4 years.

Subsequently, in 2016, a merger was announced between MasMovil, which has the fibre assets divested by Orange and Jazztel, and Yoigo, the fourth largest MNO, which was approved by the Spanish Competition Authority (CNMC) without imposing any commitment on the merging parties. Additionally, in 2015 Telefónica acquired DTS, the main satellite pay-TV operator in Spain. As a result of this acquisition, Telefonica increased its already high market share in pay-TV, as their premium content is the key to selling bundles in Spain. The agreement to an increased concentration of ownership was subject to several commitments to promote competition, such as the provision of a premium channel offer.

24. Regulatory authorities have applied remedies or required conditions on many of these mergers. Sometimes approvals were subject to a divestment of part of the newly merged entity, such as in Belgium for the Liberty Global and Base case. In other cases, such as the one in Canada involving Shaw Communications, the fact that Shaw did not previously own a mobile network meant that authorities assessed there was no need to oppose the transaction. It was also noted that approval would not result in any change in spectrum concentration and accordingly no remedies were applied to this transaction.

25. In approving MNO mergers, authorities imposed a number of conditions including the divestment of spectrum or facilities (e.g. towers) to open possibilities for new MNOs or an undertaking from the merged player to offer wholesale access to MVNOs and so forth. In OECD countries, remedies applied in more recent mergers appear to be more pro-competitive in terms of their goals than the remedies applied in earlier cases. This may indicate that remedies applied in earlier cases did not meet initial expectations in terms of emergence of MVNOs in merged markets, or of developments in prices and investment.

26. In the area of fixed networks, regulatory authorities also applied a number of different conditions before approving mergers. In Portugal, authorities required divestment of network operators. In the United States, as a condition of approving the AT&T and DirecTV merger, the new entity was required by the FCC to deploy fibre to the premises (FTTP) network facilities to 12.5 million mass market locations within four years of the merger closing date.

27. Post a merger or acquisition approval, OECD countries take a number of different approaches to assessing or monitoring market developments. When specific conditions are imposed, the merged entity will generally have to report on fulfilling those remedies. While not all authorities conduct specific post-merger reviews, they are common in a number of countries. For example, Austria's Federal Competition Authority BWB and the Austrian Regulatory Authority for Broadcasting and Telecommunications RTR published two reports assessing the effects of the merger between Hutchison 3G Austria and Orange Austria that took place in 2012.

28. One question that arises in a post-merger case or in general monitoring of market developments is whether regulatory authorities have the information they need to assess outcomes. Assessing compliance with a precise remedy may be less challenging than assessing general outcomes such as effects on prices and investment, even though proponents of mergers often hold out more effective competition and incentives for investment as a reason for requesting approval. A further consideration for assessments is the increasing use of shared network facilities between MNOs and its potential influence on investment, particularly when this is combined with MNO mergers.

*Several countries are undertaking convergence reviews to reform regulatory frameworks in light of the changing market*

29. As communication services continue to evolve and the use of OTT services grows, a number of governments have been carrying out convergence reviews to evaluate whether different services should be brought under the same frameworks. In some cases specific units have been created to ensure that policy makers have the necessary information to take informed decisions. In Australia, the government created a Bureau of Communications Research (BCR), a unit of the Communications Ministry responsible for assessing new convergence trends in the communication sector. In October 2016, the BCR released a report analysing recent communication trends in that country, such as the increased demand for faster Internet services, the disruption of traditional broadcasting business models by increased demand for OTT services and local content costs, and a growth in content produced in Australia due to new entrants and platforms. The Australian Competition and Consumer Commission (ACCC) also announced a study on the communications market in Australia, which will examine network capacity, access to dark (unused) fibre, and OTT services development. The results will be issued in 2017.

30. In Spain, the CNMC released a report in 2015 on the use of OTT services which found that the main exceptions were a more frequent use of messaging applications on mobile connexions (76% use in mobile against 43% in fixed) and for downloading of audio-visual content (38% of those using fixed connexions and 21% using mobile) (CNMC, 2015). Similarly, the Danish Agency for Culture published a Media Development Report in 2015 with data and analysis on the use of media on different platforms over time in that country (Danish Agency for Culture, 2015). In 2015, New Zealand commenced the implementation of a cross-government work programme on convergence. The programme entailed an exercise to increase the understanding of issues such as content standards, taxation and the development of creative industries (MBIE and MCH, 2015). As a result of the exercise, certain programmes were designed, some of which are part of New Zealand's Business Growth Agenda (MBIE, 2015). In the United Kingdom, Ofcom is conducting a Digital Convergence Review, which led to an interim report in February 2016 that set out the focus of the United Kingdom's future convergence strategy and defined the process of de-regulation in some cases (Ofcom, 2016).

31. In some countries, proposals for upcoming work on the issues around convergence are set out in the work programmes of relevant agencies. For example, Canada's CRTC strategic plan for 2016-19 revolves around the main pillars of connecting Canada with accessible, innovative and quality communication services, creating more local content and protecting users (CRTC, 2016). Korea is undergoing a similar process through the development of KCC's overall plan for 2017-19.

*Some countries have created converged regulators who have a responsibility for both the telecommunication and broadcasting sectors*

32. To encourage a more coherent regulatory approach, an increasing number of countries have reformed their communication authorities and adopted a converged structure that integrates both telecommunication and audio-visual sectors.

33. Some of the benefits of establishing a converged regulator have included:

- One-stop shop for the industry and consumers;
- Better enforcement and coherence among the different regulatory areas (e.g. audio-visual services, networks, communication services);
- Ability to examine the full value chain from networks to content, undertake comprehensive competition analysis, identify possible leverage of market power in neighbouring markets (bundling issues) and evaluate concerns from content standards to exclusive dealing, whereby upstream providers foreclose competing companies downstream;
- Cost savings, with the caveat that actual savings are dependent on the resulting structure and functioning of a converged regulator.

34. Most recently, Mexico (2013), Slovenia (2013), and Spain (2013) have reformed their communication regulatory authorities to introduce a converged structure. These countries add to the list of those that previously adopted some features of a converged structure, such as Australia, Austria, Canada, Estonia, Finland, Hungary, Italy, Korea, Switzerland, the United Kingdom and the United States. The so-called, 'converged regulators', which vary substantially in their structure and capacity, now total 13 among OECD member countries (Annex 2).

***Interconnection rates and approaches to Internet traffic exchange remain areas of interest***

*Termination rates have declined in recent years, though there have been exceptions*

35. Interconnection rates such as mobile termination rates (MTRs) and fixed termination rates (FTRs) apply to telecommunication operators providing telephony service. In OECD countries, mobile termination rates for all mobile operators (MNOs and MVNOs) generally apply. In some countries, such as Korea, however, MTRs are differentiated by operator. In the case of fixed operators, MTRs can apply to all of them, as in Germany, Spain and Finland, or only to operators holding significant market power, as in Belgium, Denmark and Ireland.

36. The interconnection rates and the methodology used to update termination rates are dependent on the regulatory authority. In the United States, interconnection rates vary by carrier and area served. In Europe, some countries use a market analysis and national consultation to elaborate a proposal for changes in the termination rates. For EU member states, such proposals must be submitted to the European Commission. Alternative methods are used in other countries: in Canada, termination rates are adjusted manually using an (i-x) factor where ‘i’ is the annual rate of inflation and ‘x’ is a productivity factor determined by the regulator. In Colombia, interconnection rates are negotiated by operators in their contracts but need prior approval of an initial reference offer by the regulator (CRC). In Korea, termination rates are determined biennially and applied to each operator.

37. Outside the OECD area, international termination rates continue to be a concern in countries where the government establishes a cartel and applies a uniform surcharge on incoming telephone calls (OECD, 2014a). International termination rates have also drawn attention among OECD countries, with some concerned that the rates do not reflect a cost oriented approach. In the European Union, since 1st January 2016 some regulators have begun to allow mobile operators to treat the international termination rate differently from national termination. Subsequently, prices change frequently (e.g. almost on a monthly basis) and this has led to tensions between European mobile operators and their counterparts. As

Swiss operators, for example, are no longer offered the 'European Tariff', this has been said to have undermined relations between MNOs.

38. Outside of Europe these developments have drawn the attention of the Office of the United States Trade Representative (USTR). According to the USTR, several operators within the European Union are charging higher rates for the termination of international traffic originating from outside that area than they are for traffic that originates within Member States. This creates a two-tiered approach for termination, which the USTR says does not appear to reflect incremental costs for termination of such traffic.

39. The questions raised by USTR were familiar ones between OECD countries in the days when the international accounting rate system was used between operators in different countries, most of which had monopolies. This system was largely superseded once telecommunication markets were liberalised and competition was able to drive rates closer to cost. Nonetheless, as regulators around the world recognise, every network operator potentially has a degree of monopoly power in terminating traffic to their own customers and, as such, the same vigilance applied to domestic rates should also apply to international rates.

*Peering and transit between Internet service providers is largely self-regulated by the market*

40. The interconnection of Internet service providers and the terms in which traffic is exchanged among them is an area largely self-regulated by market players. Recent market developments, in particular peering and transit disputes between market players, such as the Netflix-Comcast cases in the United States, have led to the debates becoming a matter of public record. In 2015, the regulatory agency in the Netherlands analysed seven prominent international disputes and concluded that in all cases except one, some form of actual restrictive interconnection behaviour caused the dispute to arise (ACM, 2015). It further noted that consumer harm only arose in the situations where there was not enough interconnection capacity between the parties involved.

41. Communication regulators do not generally collect information on IP interconnection agreements because they are not subject to direct regulation. In most countries, the operator's decision on whether and how to connect is driven by competitive market forces rather than by government regulation. However, national regulators have, by law, the authority to request such information in most cases. Some countries have specific requirements to send interconnection agreements to the relevant Ministry or regulator, as in the Czech Republic and Korea.

42. Recent developments related to mergers and acquisitions have highlighted the importance given by regulators to interconnection. In the Charter Communications acquisition of Time Warner Cable and Bright House Network in the United States, the FCC imposed an obligation to the resulting operator to make interconnection available on a non-discriminatory, settlement-free basis to companies that meet basic criteria. Other conditions include addressing data caps, usage-based pricing for residential broadband, residential broadband build-out and more. In the same case, the Justice department also examined whether the merger would allow the resulting company to become an unavoidable gatekeeper for Internet-based services, including online video distribution, that rely on a broadband connection to reach consumers.

***International mobile roaming is evolving, influenced by innovation, competition and regulation***

*Technological innovations are emerging as partial substitutes to regular international mobile roaming services but competition is driving the greatest change*

43. The international mobile roaming (IMR) market continues to be transformed in OECD countries. Key factors include technological change, commercial responses to increased demand, and regulation (where competition has been determined to be insufficient). Furthermore, there is an ever-increasing range

of technologies that allow consumers to bypass traditional IMR if they are willing to accept a degree of imperfect substitution. These technological paths, in one way or another, substitute the services of a home country provider, such as the complete substitution of an operator specific SIM by one from an intermediary, such as Apple (OECD, 2016a).

44. Over time, some of the technological alternatives to the use of conventional IMR services are overcoming aspects of imperfect substitution. An example is the Interphone sticker, which was introduced in September 2016. It enables the use of virtual SIMs from operators in participating countries but critically enables the retention of a home country mobile number for incoming calls.[7] That being said, while the rates in such an approach may be far lower than regular roaming, they tend to be much higher than obtaining a local SIM. On the other hand, if a user is willing to forego his or her mobile number and rely on data-only services, the emerging options are more propitious. Users of the Apple SIM on an iPad, for example, can select and pay local rates from two or more operators when visiting countries such as Japan and the United States without the need to insert a local SIM from the country. At the end of the day, however, all substitutes for SIMs from either the origin or the destination country rely on competitive markets. In other words, SIMs need to be unlocked for foreign use and there need to be participating operators in the visited country (i.e. without direct access to local rates, charges are higher than local rates via intermediaries).

45. The most widely used technological substitution for regular international mobile roaming services is Wi-Fi. In the past, while this option enabled access to data services and use of OTT telephony, it still had limitations in terms of the use of a regular mobile number. This is also changing; in March 2016, AT&T began to allow customers to use Wi-Fi when calling from abroad. These calls do not incur international mobile roaming charges but rather the charges associated with the customers' regular service plans. Offers called 'roam like at home' (RLAH), appearing in an increasing number of countries, go a step farther. RLAH offers are now commonplace in countries such as France, Israel, the United Kingdom and the United States, though they are conspicuously absent in many countries (Annex 3).

*Regulation is emerging to ensure competition in international mobile roaming and affordable prices to the end user*

46. The other substantial developments in international mobile roaming have been in the area of regulation. In Mexico, for example, the emergence of RLAH offers coincided with new market entry enabled by a lifting of foreign investment barriers. A further notable feature of the Mexican market, though believed to be nascent in its potential use, has been the introduction of MVNOs and the ability of those players to directly negotiate their own direct international roaming agreements. In many countries MVNOs do not have this ability and action to overcome such barriers could provide an additional option for countries that find insufficient competition is developing in the IMR market.

47. The highest profile regulatory changes have undoubtedly been those in the European Union. In November 2015, the European Parliament and Council reached agreement on the 'Telecoms Single Market' (TSM, Regulation EU 2015/2120 - European Parliament and European Council, 2015)), which set out a timetable for further reductions in intra-EU retail roaming caps in April 2016 (to EUR 0.05 per minute for outgoing calls, EUR 0.02 per SMS and EUR 0.05 per MB of data). It also required RLAH to be subject to fair use criteria (to ensure that only periodic roaming would have to be covered) and sustainability criteria (to allow in exceptional cases a derogation from RLAH if roaming costs were not covered. The EU approved a Fair Use Policy in December 2016, which details regulations to ensure the effective application of RLAH offers and to make certain that the most competitive domestic offers remain competitive (EC, 2016b). In January 2017 the EU agreed upon a set of wholesale roaming rules defining the rates which European Union operators can charge one another for use of their respective networks abroad, a final step to ensure the introduction of RLAH for periodic roaming by 15 June 2017 (EC, 2016c).

48. The TSM regulation followed three years after the previous roaming regulation (Roaming III), which came into force on 1 July 2012. In summary, that regulation had extended anti-bill shock and transparency mechanisms (including the EUR 50 data cap) to European Union roamers travelling beyond the European Union's borders and introduced retail caps for data for the first time, as in other countries like Canada. In Canada, the CRTC's 2013 Wireless Code placed an automatic cap on international data roaming charges at USD 76 within a single billing cycle unless the customer explicitly agreed to pay additional charges. The TSM also established a mechanism for introducing structural solutions to decouple regulated mobile roaming services from domestic services, which were set out in European Union Implementing Acts following a consultation of BEREC and also provided for BEREC guidelines on wholesale access.

49. The European Union regulatory initiatives in the IMR market have provided a benchmark for many countries and have shown the role that regional bodies can play in significantly reducing prices and creating competition in IMR services. Israel, for example, has used the European Union prices for bilateral agreements with Poland and the Russian Federation. Regional regulatory bodies are also active in this area though they generally do not have the powers available to the European Union

50. In the future, bilateral agreements should lead to price reductions and provide a paradigm for other countries to follow suit where there is insufficient competition (OECD, 2016a). Some of these bilateral agreements have been undertaken between countries with free trade arrangements (FTA) and could provide a framework to follow for other regions with FTAs and could help alleviate some concerns that bilateral or regional agreements may have to be opened up to third parties as part of most favoured nation obligations. Australia and Singapore updated and signed their FTA in October 2016.[8] A key element of this agreement deals with IMR between the two countries. Notably, the agreement provides that either country, if it sees fit, may regulate wholesale rates and make these rates available to mobile operators from the other country. That being said, both countries subsequently had spectrum auctions that will lead to the introduction of a fourth MNO in each of their respective markets. Moreover, the same company (TPG) won the auctions to provide the new MNO in both countries. As such, the new entrant, looking to attract customers, is well placed to differentiate their services by offering improved roaming between these markets. If so, the tools available via the FTA may not be required. On the other hand, if competition did not address the high IMR rates between the two countries, authorities now have a regulatory mechanism to address this issue.

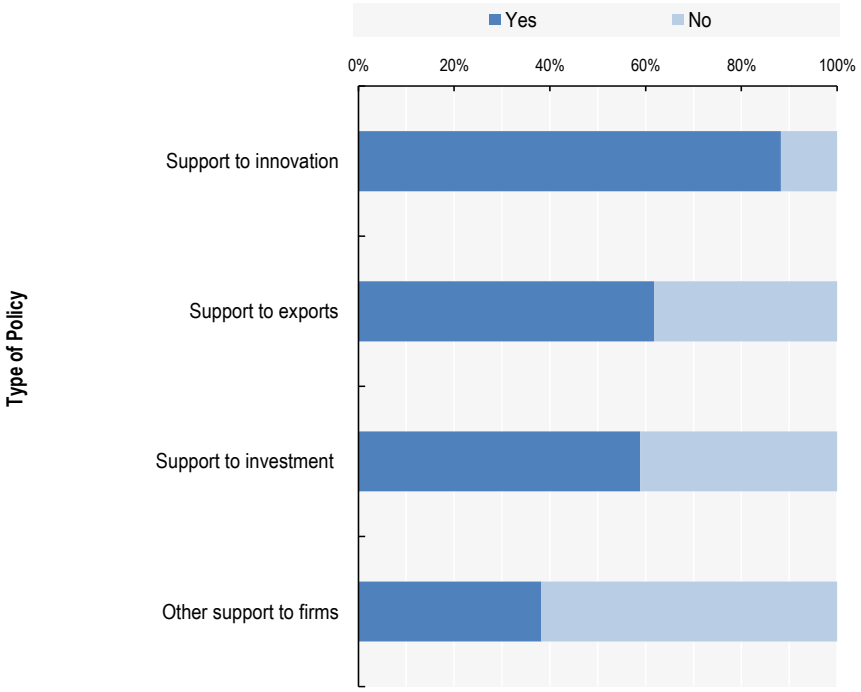
***ICT sector development support is focused on training programmes and measures to spur innovation***

*The most commonly used policies are government funded innovation measures and training programmes*

51. All countries surveyed for this edition of the DEO have policies to support the growth of the ICT sector. Most target innovation, investment, or exports. 30 of the 34 countries[9] that responded to the ICT sector development section of the 2016 DEO OECD Policy Questionnaire reported having at least one policy that specifically supports innovation, compared to 21 with measures directed at expanding firm exports, 20 with policies that promote ICT sector investment, and 13 with policies related to other ICT sector development (Figure 1). Comparatively, innovation policies seem to hold greater importance as countries had 84 distinct policies to promote innovation in the ICT sector, as opposed to investment and exports, which had 46 and 40 policies, respectively[10].

52. This support is delivered through a variety of conduits, including tax incentives, loans, R&D subsidies, export subsidies, block grants, and educational training programs. Of all the policies reported by countries in the survey, 39 percent targeted SMEs and start-ups, while 25 percent were focused on companies in the ICT sector, 17 percent were open to all companies and the remaining 19 percent had other firm requirements.

**Figure 1. Policies to support ICT sector growth**

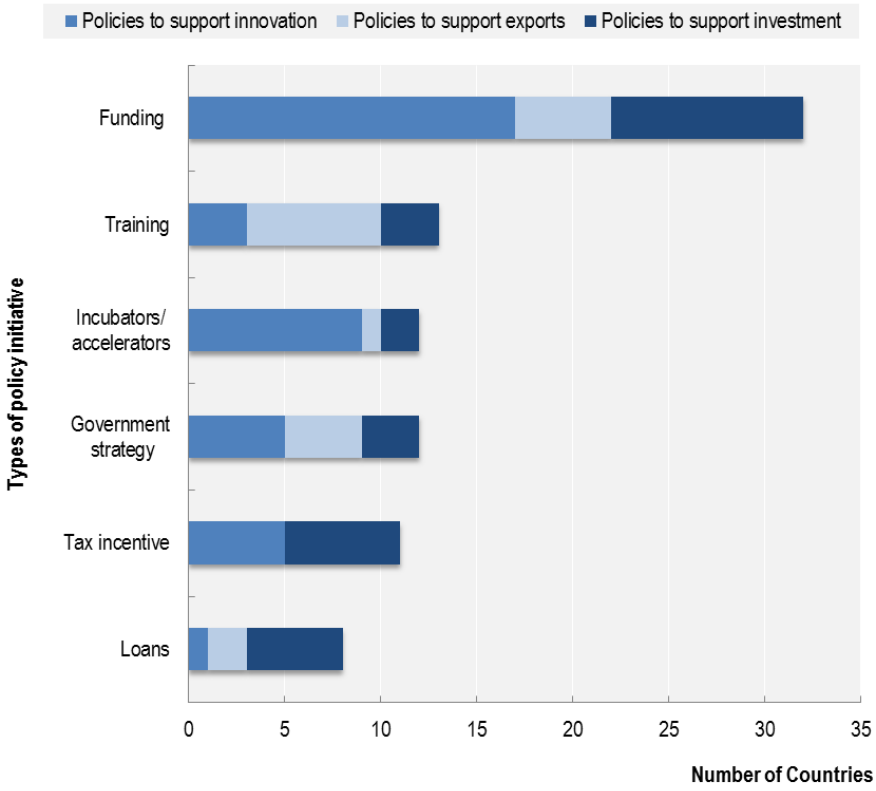



Source: OECD Digital Economy Outlook Policy Database.

53. The most prevalent governmental policy measure to strengthen the ICT sector is funding, which may include subsidies for companies to undertake further investment in infrastructure or research and development (R&D), or to encourage exports (Figure 2). Governmental funding programmes are used frequently to encourage innovation and investment, and are employed by 97 percent, or 33 out of the 34 surveyed countries. As an example, Austria's ICT of the Future programme provides financial support to companies that explore new ICT research topics and possible associated applications, and to encourage development based on these topics.[11] Turkey and Mexico also offer subsidies to specific industries to encourage exports. Another form of governmental funding is through a venture capital fund, as is seen in the Czech Republic and Estonia.[12]

54. Government sponsored training programmes are also commonly seen as a way to develop expertise in ICT and thereby to promote innovation. These projects may be aimed at developing knowledge, sharing experiences and creating best practices, or providing expertise on a subject so that local firms can better compete in the market. For instance, the UK offers education materials on social media sales to businesses to improve their social commerce skills, while the Switzerland Global Enterprise and Spain's Tech Center both advise companies on export promotion. Finland, Colombia, and China are other countries who have implemented training programmes directed to the development of the ICT sector. 15 countries in the survey had some form of training programme, making it the second most common ICT policy after funding. Additionally, 12 countries offer a mixed policy approach which often includes a training component in conjunction with other types mentioned above, like grants, subsidies, loans or tax exemptions.

**Figure 2. Policy initiatives to support ICT sector growth**




Source: OECD Digital Economy Outlook Policy Database.

*Incubators and accelerators are popular tools to promote innovation in ICT start-ups and SMEs*

55. Several governments, in an effort to promote innovation, have launched initiatives aimed at helping start-ups or young SMEs through accelerators or incubators. Fourteen of the 34 respondent countries have such initiatives, making it the third most common ICT policy. While both accelerators and incubators share the same aim – to help starting businesses grow – their methods differ. Both types of institutions rely on a network of entrepreneurs to promote synergies and learning from other members, as well as some sort of mentorship, but accelerators also provide intensive education along with seed funding for the selected businesses in exchange for taking ownership of a share of the business. Given this initial investment, the competition is fierce for a spot in an accelerator's portfolio, and the intensive period of education and mentorship usually culminates in a "Demo Day" after a few months (Hathaway, 2016). Among the governments that have taken this approach, for instance, the United Kingdom has set up the HutZero programme, which is an early stage accelerator focused on cyber security. The programme offers an intensive period of business education and mentorship.[13] Another example is Luxembourg's Fit4Start programme, which accepts start-ups to make up a cohort two times per year with the winning start-ups having access to EUR 50 000 in funding in addition to "lean start-up" training and coaching to prepare the cohort for a final pitch at the end of four months. [14] Brazil, France and Israel have similar programmes for start-ups and early stage SMEs.

56. Other governments have adopted the approach of hosting an incubator in their country. An incubator usually charges its members a fee for access to shared office space, educational services and mentorship opportunities. The duration of the membership, from one to five years, is often longer than with

an accelerator and the selection process is much less competitive (see Table 1). In Denmark, the Danish Agency for Science, Technology and Innovation, together with the Ministry of Higher Education and Science, has launched the Innovation Incubator Scheme to help encourage start-ups early in their business development.[15] Latvia, Portugal, and Hungary have similar projects. Some governments, like Singapore and Israel[16], have recognised the value of these organisations for start-ups and have offered support. The Singaporean government's Incubator Development Programme provides grant support of up to 70 percent of costs to enhance the capabilities of incubators and venture accelerators to assist and grow innovative start-ups in the country. However, the "business models" of these government-sponsored initiatives differ from their private sector counterparts. For instance, a government's seed investment often does not result in partial ownership in the company once it has "graduated", nor do chosen companies usually have to pay membership fees to partake in the incubator scheme.

**Table 1. Main characteristics of incubators and accelerators**

| | **Incubators** | **Accelerators** |
|---|---|---|
| **Duration** | 1 to 5 years | 3-6 months |
| **Cohorts** | No | Yes |
| **Business Model** | Rent; non-profit | Investment; can also be non-profit |
| **Selection** | Non competitive | Competitive, cyclical |
| **Venture Stage** | From early to late | Early |
| **Education** | Ad hoc, human resources, legal | Seminars |
| **Mentorship** | Minimal, tactical | Intense, by self and others |
| **Venture Location** | On-site | On-site |

Source: Hathaway, I. (2016), "What start-up accelerators really do", 1 March 2016, Harvard Business Review, https://hbr.org/2016/03/what-startup-accelerators-really-do (accessed on 15 March 2016).

57. Other governments, such as Lithuania and Norway, have programmes where the government acts as a guarantor for start-up companies or SMEs to facilitate access to finance in their early development stages. For example, France, Italy, Mexico, Latvia and the Czech Republic offer governmental loans, some of which have preferential grace periods and interest rates, to companies. Tax incentives are another tool used by policymakers and 12 of the countries surveyed use them. Brazil, for instance, offers tax breaks to investors who have bought debt issued by telecom operators to finance broadband infrastructure projects, as well as to the operators themselves who have investment projects to expand or modernise telecom networks. Other countries allow companies to depreciate the value of goods above the normal rate of depreciation; in Italy, for example, companies can depreciate new capital goods at a rate of 140 percent and high-tech purchases such as nanotechnologies, big data, and smart materials up to a rate of 250 percent. Sweden, Turkey, Costa Rica, and Lithuania also offer various forms of tax exemptions. Finally, many governments establish high-level strategies as a way to support ICT development at a broader scale, for instance in digital or innovation strategies.

### 6.2 Usage and Skills

58. This section provides information on policies and regulation for increasing ICT usage by individuals, firms and governments, as well as for enhancing ICT skills. In this section the discussion on usage is based on responses to the usage section of the 2016 OECD DEO Policy Questionnaire by 35 countries[17], and the discussion on skills is based on responses to the skills section by 34 countries[18]. There is strong evidence that the use of ICTs drives innovation, which can enhance productivity and competitiveness (OECD, 2016b). ICTs help reduce transaction costs and enhance the scope of communication with the different stakeholders of an organisation. That enables, for instance, faster creation and diffusion of ideas and knowledge both within and between organisations, which can translate into benefits such as enhanced collaboration during R&D activities. The use of ICTs can also enable greater product differentiation, enhance customer relationships and improve supply chain management. All of that can ultimately lead to an increase in productivity and higher market shares (OECD, 2016b).

59. ICT-related skills are another key enabler of digital innovation. This is confirmed by business innovation surveys showing that firms using internal or external skills related to ICTs and data are more likely to innovate.[19] In most countries for which data is available, around 60 percent of the innovative firms employ software developers and around 40 percent employ mathematicians, statisticians and database managers (compared to around 30 percent of non-innovative firms that employ software developers and 20 percent that employ mathematicians, statisticians and database managers) (OECD, 2016b).

***ICT usage is being promoted through e-government, training programmes and subsidies***

60. Most of the potential value brought by digitalisation lies in the adoption and use of ICTs. For companies, ICTs connect businesses to digitally managed global value chains and offer a platform for selling to customers worldwide. That allows firms to scale up quickly and in some cases to compete on a national or even a global level. In areas where there are obstacles to accessing knowledge, such as in some rural areas, the Internet is an important source of information supporting business innovation and knowledge accumulation. ICT applications, ranging from basic accounting or inventory applications for smaller companies, to more complex services such as customer relationship management software or enterprise resource planning systems, for larger companies, render business processes more efficient. Overall, the Internet and ICTs drive firm productivity and reduce barriers to market entry.

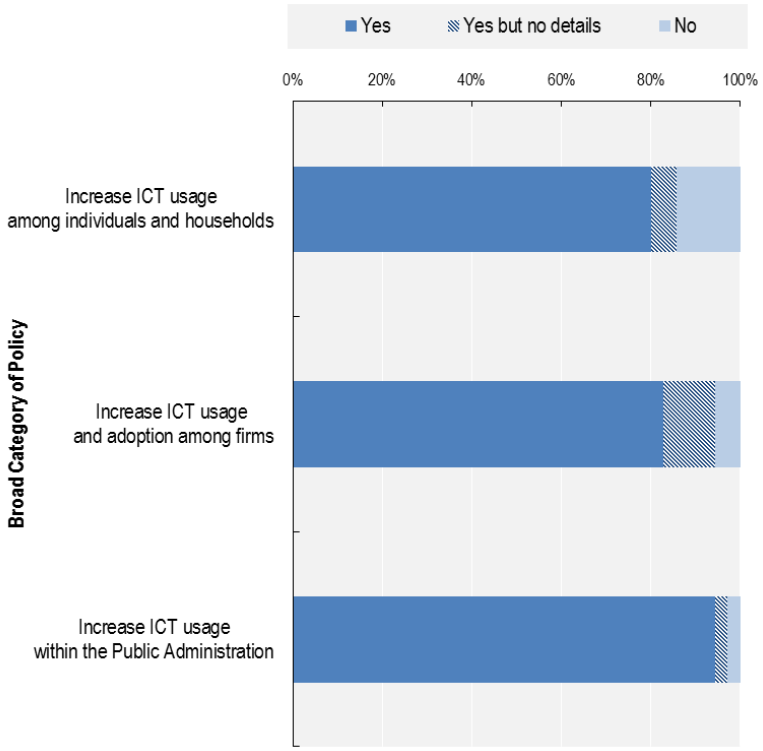
61. Several studies have analysed the link between ICT adoption, firm performance and contribution to economic growth and have been able to demonstrate the positive effects of greater ICT adoption on firms' productivity, performance and the economy as a whole (e.g. Gaggle and Wright, 2014; Grazzi and Jung, 2016; Haller and Siedschlag, 2011). Grazzi and Jung (2016) were also able to demonstrate that firms that adopt broadband are more likely to innovate.

62. The following examines policies to promote ICT use by individuals and firms, including, for example, financial support to households and individuals for purchasing ICT goods or services, support to firms for ICT investment and expenditures, and the promotion of e-government services.

63. Of the 35 countries that responded to the ICT usage section of the questionnaire, almost all had at least one policy in place to increase the use of ICT tools in the public administration and governmental services, reflecting governments' priority to become more digital. Thirty-three governments reported having policies to encourage the use of ICTs in businesses, along with 30 that had policies directed at increasing usage among individuals. However, when analysing the actual policies themselves, the priority for governments seemed to be increasing the use of ICTs within their own administrations, rather than encouraging businesses and individuals to use ICTs. This is exemplified by the total number of policies reported for each target group: over 300 policies were reported to improve ICT use within governmental

bodies, in contrast to 74 for individuals and households, and just over 60 directed to businesses. One point that must be acknowledged is that many of the policies reported as encouraging usage among businesses were actually focussed on aiding innovative ICT companies (which was detailed in the part of Section 6.1 that discusses ICT sector development support), rather than encouraging all types of companies to adopt the use of ICTs in their work processes. Therefore, since such policies have already been explored earlier in this section, they are omitted from the analysis here, leaving only those policies directly related to increasing ICT usage by businesses more generally. As said above, given the volume of policies in support of ICT usage in public administration, governments seem to place slightly less priority on encouraging households and businesses to incorporate ICT technology more systematically. Alternatively, it is possible that governments are seeking to achieve higher uptake of ICTs by households and businesses through more general business, framework and investment policies.

**Figure 3. Policies to support ICT usage**



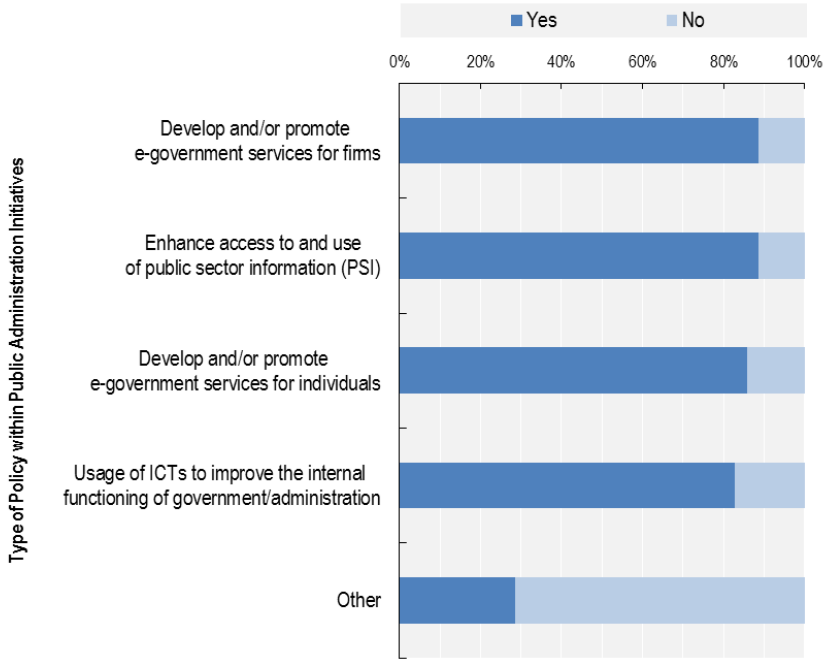

Source: OECD Digital Economy Outlook Policy Database.

64. The key findings for this section are that governments are focussing on becoming digital by incorporating ICT tools internally as well as offering services online for individuals and businesses. Online handling of governmental administrative requests is the most common e-services offered, and include tax declarations, update of personal information and the civil registry, and consular services. Many governments also have policies to share public sector information through open data portals. Policies aimed directly at individuals and firms to increase their usage of ICT tools are secondary to improving ICT usage in the public administration, however among those offered, training and subsidies are most commonly used for both individuals and businesses.

*Governments are offering their services online and focussing on becoming more efficient through use of ICT tools*

65. Policies to promote the adoption of ICTs in Public Administrations can be split broadly into three categories: the first is directed to creating or promoting e-government services for individuals, the second towards firms, and the third is focussed on improving the internal functioning of the governments themselves and making the government more transparent through the public availability of information. All of these categories carry roughly the same weight in terms of number of policies.

**Figure 4. ICT Policies by Public Administration Breakdown**




Source: OECD Digital Economy Outlook Policy Database.

66. Policies to develop or promote e-government services for individuals and households are aimed overall at bringing governmental services for citizens online. This includes allowing citizens to pay their taxes, submit various forms, and update their personal information online. Over 80% of the countries surveyed have a policy of this type. By way of example, Colombia has several initiatives to migrate paper-based forms online; these include having a digital registry to track and update civil registration, medical records, and electronic documentation of education and military service. Colombia also has made some consular services available online, including for the issuance and renewal of passports. Switzerland has implemented an electronic voting system for voters abroad, and a few cantons have recently begun to offer this option for Swiss residents living in the country. Austria, Israel, Korea, and Portugal are other examples of countries who offer various e-services for citizens. Along the same line of making governmental services more efficient by going digital, many governments have converted to solely digital media to communicate with citizens. Norway has adopted a "digital-by-default" approach, forcing citizens to actively choose to receive paper mail in lieu of receiving communication digitally via a secure digital mailbox. Lithuania and Austria have similar programmes for digital communication.

67. Given that many of these e-services include the transfer of personal data, around a quarter of the countries surveyed have developed e-ID and e-authentication services to make these online services more

secure, including Brazil, Finland, Poland and Sweden. However, policies specifically related to digital security and privacy are discussed in more detail in Section 6.4, as well as in OECD (2016b). Therefore, the policies represented here may not be fully representative of all the security initiatives that countries have put in place.

68. Over half of the countries who responded to the survey have created a website to communicate relevant information related to the e-services provided by the government. Information dissemination and awareness of available e-tools is integral to stimulate further use of e-government services among citizens. Similarly, it is also important that the site is easily navigable and that users can find related information on services. Spain, Turkey, and Mexico are just a few examples of countries that have "one-stop" websites, and some like Korea and Slovenia even offer their websites in multiple languages to be accessible to foreigners living in the country.

69. There are similar policies directed towards firms as those discussed above. For instance, web portals for a "one-stop" point for e-government information, and online submission of forms are also offered for businesses. Given that they often reduce the governmental administration burden both for firms as well as for governments, it is no surprise that these services also be available to businesses. Online submission of forms, including online tax services, is by far the most common policy directed towards businesses with 28 of the 31 countries having such policies. Specific to businesses, many countries allow all paperwork to be completed electronically in order to officially register as a legal entity; Spain, Russia and Latvia have such programmes. Other examples of e-forms specifically for firms include e-invoicing for government suppliers, which Norway, Colombia and Belgium have done; online licensing systems which can be found in Singapore and the Czech Republic; and online tax declaration, including VAT and customs declaration, which Korea, Switzerland, Mexico and Israel, among others, offer to firms. Many countries have "one-stop" portals directed towards business users which contain more specialised information related to the establishment and registration of a legal business entity, and provide links to access the required online forms. Austria, Denmark, Finland and Spain are among the one-third of the countries surveyed which offer such online business portals.

70. Unique to e-services for businesses is the large number of governmental processes directed toward a single online platform for public procurement. Such portals integrate all of a government's buying and selling across governmental entities in one place. By making all government procurement specifications available via the Internet, companies have equal access to information, making the public procurement system more transparent. Japan's "Government Electronic Procurement System" provides a good example of the various digital procedures incorporated within the e-public procurement process including the public notice of specification, bid, open bill, conclusion of contract, performance evaluation on contract, and lastly payment. Just under half of the countries surveyed have such public procurement processes online, including many EU countries, Costa Rica, Singapore, Turkey, and Korea.

71. Approximately one-third of governments are also reviewing the e-services available to firms in an effort to make internal processing of business administration more efficient and to reduce the regulatory burden where possible. This often entails sharing information among governmental offices more seamlessly, offering integrated services for business, and allowing firms to comment and file complaints with governmental services as a feedback loop to drive further improvements. Slovenia has established a Single Business Point, which aims to reduce the number and volume of data required of firms for reporting purposes and is in the process of a review to further reduce administrative burdens and simplify regulatory procedures. Canada has a number of initiatives to make internal processing more efficient for businesses. The Canada Revenue Agency is establishing a standard identifier for businesses to be recognized across the government to increase information exchange within governmental agencies and is also implementing several service transformation initiatives such as single sign-on, real-time status updates and e-payments.

Singapore, the Netherlands, and Brazil are other examples of countries that are reforming their internal processes.

*Open Data portals and legislation for access to public sector information aim to improve transparency*

72. The theme of governments "going digital" is central to policies aimed at improving internal governmental functioning, with around 80% of the country respondents reporting at least one policy to support the digitalisation of governmental functions. While related to the digitalisation efforts highlighted in the paragraphs above, these policies are more focused on bringing governmental documents and registries online, keeping them up to date and easy to find and access, and promoting zero paper policies through digital communication. Some examples of such processes include the Czech Republic's electronic legislative library which enables tracking of legislative documents, monitoring of comments and the secure storage of all versions. China and Costa Rica have implemented zero paper policies, while Poland, Canada and Japan have put in place electronic documentation management for the exchange, update, and version control of electronic documents, as well as the disposal of obsolete documents within the public administration.

73. Sharing information between governmental ministries is also a common theme. Approximately 60% of governments have policies to increase internal information-sharing and collaboration, which includes ensuring interoperability between governmental platforms. By way of example, Colombia's Interoperability Framework is an effort to help the state function as a single institution, and establishes a common interoperable platform for the seamless exchange of information. The Information Management Framework in Norway defines the data responsibilities of each agency, and is establishing a common framework to integrate the data from various agencies to create a common data directory. Russia, Luxembourg, Finland and Israel are other countries that have similar policies in place.

74. Almost all of the governments surveyed reported having at least one policy in place to increase public access to governmental information. These open data programmes have a dual aim: the first is to promote transparency and accountability within the government by making information available to the public. Chile offers an example of an open data initiative with such an aim, as it allows access to the public sector budget through its "Open Budget" platform. Brazil publishes all governmental expenditures online on its Transparency Portal. Both of these programmes are a step towards transparent governments. The second aim of open data initiatives is to promote access to and effective reuse of data, so that the data may be used for research or innovation towards the benefit of society. The objectives of the open data campaigns in Israel and Canada are indeed to increase public access to information to encourage innovation in the public sector and the society more broadly. However, that is not to say that open data initiatives cannot accomplish both aims; they can simultaneously encourage the effective reuse of data and increase the transparency of the public administration.

75. About two-thirds of governments in the survey have legislation establishing public access to information and defining parameters on which information is publicly shared. The EU Directive on the re-use of public sector information provides a common legal framework for public access to government-held data (EC, 2017). The directive is built to promote transparency and competition in the market and focuses on the economic benefits of the re-use of information. EU member governments were obliged to transpose the directive into national law by 2015, which all EU respondents in the survey have done at the time of writing. Brazil, Costa Rica, Japan and Mexico also have such legislation to define the public sector information to which the public should have access.

*Training programmes and subsidies are the most common types of policy to encourage the use of ICTs by individuals and households*

76. A number of different policy configurations, both financial and non-financial, encourage individuals and households to use ICTs in their daily lives, with non-financial programmes being slightly more prevalent. Training in the use of ICTs is the most common non-financial policy, with over half of the countries reporting a policy of this type. Of these, over 80% target specific disadvantaged groups who may lack basic ICT skills due to the digital divide resulting from income disparity, disability, or age. Singapore and Norway have digital literacy programmes for seniors, while China targets rural communities, and Israel and Brazil target low-income households and individuals. Latvia and Canada both have training programmes to give jobseekers the skills needed in the current market; Latvia has allocated over EUR 100 million to training programmes under its national digital strategy, to be disbursed from 2014 to 2020. Among the countries that responded to the questionnaire, Latvia, Poland and Hungary reported the highest budgets for training programmes. The "Enable IT" programme in Singapore aims to train persons with a disability to use assistive technology to better meet the demands of their daily lives, both personally and professionally. Several countries have programmes to "train the teachers" as a more effective way of disseminating ICT skills; China, Estonia, and Poland have adopted this approach.

77. In addition to training programmes, governments also frequently conduct communication campaigns to promote digital technologies, e-services and ICT tools. These campaigns are generally directed towards a broad audience, with only around one-quarter being targeted to a specific group. Most of the campaigns, which are largely sponsored by governments in European countries, have the goal of promoting the safe use of the Internet. Finally, a smaller proportion of countries have projects to build telecommunication infrastructure to increase broadband access to previously underserved areas. Poland, Slovenia, Lithuania, Hungary, and Luxembourg have projects of this sort, often incorporated within their respective national digital strategies. As these countries are all members of the EU, these initiatives are likely related to meeting the EU's broadband targets of enabling access to all households at a speed of at least 30 Mb/s, and to half of all households at 100 Mb/s by 2020 (EC, 2017). Costa Rica and Turkey both have similar initiatives; though these have more varied aims, like establishing public Wi-Fi access points or mobile telecommunications infrastructure.

78. Over two-thirds of policies that use financial incentives to support usage are specifically directed at disadvantaged groups of the population who historically have had less access to ICT equipment or training, such as senior citizens, people in rural and remote areas without access to the internet, or people from disadvantaged, low-income areas. Roughly 70% of financial based policies come in the form of a grant or stipend to either purchase ICT equipment or services, like establishing broadband and paying for the service, or to be used towards classes in ICT skills. Israel offers a subsidy for low-income households to purchase personal computers as well as a three year warranty on ICT equipment and optional ICT training. Other countries offering similar programmes are Austria, Canada, China, Colombia, Costa Rica, Hungary, and Singapore. One-fifth also offer a tax incentive for an ICT purchase, as in Brazil, which grants an exemption on the purchase of smartphones, or in Poland and Denmark who offer tax advantages for the installation of a broadband connection.

*Policies supporting ICT usage in firms overlap with policies to develop the ICT sector overall*

79. Encouraging the use of ICT tools in businesses can be done through both financial and non-financial means. Financially-based schemes are slightly more common with 23 countries reporting 31 distinct financial policies, compared to 18 countries answering that they have 25 non-financial initiatives. Of the policies based on financial schemes, monetary support for the purchase of ICT equipment or towards ICT development is the most common with 16 countries out of 23 using this method. Turkey and Spain both have programmes to encourage SMEs to adopt cloud computing solutions, while Singapore's

iSPRINT Programme enables SMEs to use smart technology as a way to boost productivity and growth. Other countries such as Estonia, Poland, Hungary, and Belgium support investment in R&D infrastructure and the integration of ICT and e-business tools for the optimisation of business operation and management. France, Japan, Mexico have similar policies.

80. Roughly a quarter of the respondents to the questionnaire reported having a tax incentive for ICT purchases or for R&D, including Canada, Singapore, Japan, Italy, Israel and China. However, other OECD work shows that 29 of the 35 OECD countries have an R&D tax credit (OECD and European Commission, 2017, p. 4). For example, Canada offers a tax incentive to any Canadian business conducting research and development and Japan offers various tax incentives for companies to increase investment in digitalisation and in facilities designed to increase productivity. Meanwhile, Singapore's Productivity and Tax Credit allows eligible businesses to deduct up to 400% on expenditures incurred on prescribed activities that promote innovation and productivity, and China offers a VAT exemption and income tax reductions for SMEs.

81. Policies that are not directly financial are more concerned with increasing business ICT use by offering targeted training. Training accounts for over half of the individual policies reported by countries, with 10 of the 18 countries having at least one such training programme. The training itself is mostly focused on the digitalisation of business services, e-commerce, or on the effective use of digital media. Germany's "Trusted Cloud" training programme helps SMEs gain an understanding of cloud computing, and its possible applications within their business. Switzerland and Australia offer training courses and information related to effective digital business management: Australia's "Digital business kits offer tailored tips for operating online, as well as case studies and support to businesses. Meanwhile Switzerland provides information on IT infrastructure, IT security, e-commerce and advises SMEs on the potential steps to make businesses more digital on its digital.swiss and SME portals.

82. The policies listed here, both for financial and non-financial initiatives, have a strong overlap with policies directed at the overall development of the ICT Sector. This is perhaps unsurprising, as increasing firms' use of ICT and incentivising them to purchase ICT goods and conduct R&D is linked to increasing ICT sector development overall. However, only policies aimed at increasing ICT use in firms were used for this discussion; others related to supporting the overall development of ICT businesses through innovation and support of ICT industries, start-ups and SMEs were not included in the analysis as they already have been discussed. For a more detailed description of the policies to encourage overall ICT sector development, please see the end of section 6.1.

***ICT skills development policies target vocational training and primary or secondary education***

83. Digitalisation is bringing many opportunities, but it is also bringing new challenges and policy makers need to understand how digitalisation can help boost productivity and create new jobs. Digitalisation is often viewed as a source of new job growth, both in the ICT sector and more broadly due to its role as a catalyst for business innovation across all other sectors of the economy. It is also important, however, to acknowledge and address the net impact on employment and skills. It is clear that digitalisation is driving a significant reorganisation of businesses around the world, and that this is affecting labour demand as well as, ultimately, employment. The net effects of digitalisation on jobs are complex and still poorly understood. What is known, though, is that when any significant new technology emerges, workers and users need new skills to capture the potential productivity gains.

84. ICT skills have become an important requirement for employment across the economy, but a significant portion of the population still lacks the basic skills necessary to function in this new environment (OECD, 2012a). PIAAC (Programme for the International Assessment of Adult Competencies) data shows that the demographic factors most commonly associated with a lack of core

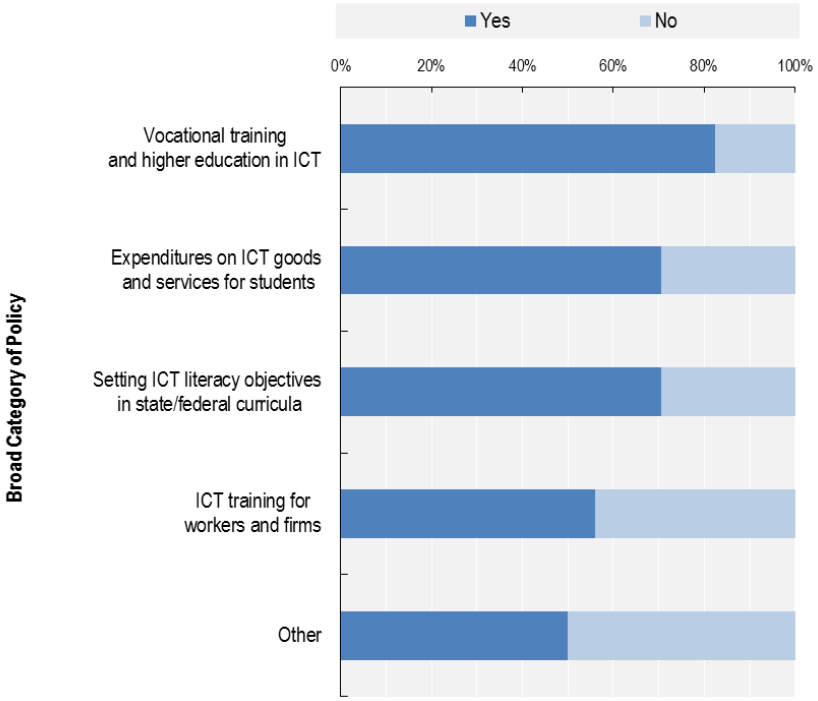
skills and no computer experience are people aged 55-65, people with less than an upper secondary level of education, and people in semi-skilled occupations. This lack of ICT skills in the adult population is of particular concern for policy makers because the groups with the lowest ICT skills tend to be among the demographic groups at the highest risk of losing their jobs in the current technological transformation of the workforce. Labour market disruptions will affect some workers more than others, and often these people will be those with the lowest levels of ICT skills and those who are the least prepared to update their skills.

85. Furthermore, a scarcity of ICT specialist skills may hinder adoption of ICTs. For instance, surveys point to the shortage of skilled data specialists as one of the biggest impediments to the use of data analytics in business. In the United States, since 1999, occupations for those with advanced ICT skills have been among those with the fastest growth in relative wages, suggesting (combined with other evidence) a possible shortage of such skills (OECD, 2016c).

86. Policies for improving ICT skills typically include ICT literacy objectives in state/federal curricula, vocational training and higher education programmes in ICT, and support to firms for providing ICT training to workers.

87. More specifically, all 34 countries that responded to the skills section of the 2016 OECD DEO Policy Questionnaire have at least one type of ICT education and training policy in place. The most common type of policy, implemented in more than 80 percent of the countries, involves support for vocational training and higher education in ICT. That includes, for example, undergraduate degree programmes, courses that may or may not lead toward a technical certification, and private initiatives or public-private partnerships to educate ICT specialists. Three-quarters of countries allocate funds to buy ICT goods and services for students, e.g. PCs and broadband connections in schools. Equally common are policies that set ICT literacy objectives in state/federal curricula. Over 55 percent of countries support ICT training for workers through programmes such as courses for the unemployed or for people who simply want to update their skills. Note that, while the programmes and policies described here are mostly implemented by governments, that is not intended to suggest that they bear all the responsibility for promoting ICT skills. Employers can and do invest in developing employees' ICT skills, as well. In addition, some governments provide support or incentives to firms for providing ICT training to employees.

**Figure 5. Policies to improve ICT skills**




Source: OECD Digital Economy Outlook Policy Database.

*Computing devices and Internet connections dominate public expenditures on ICT goods and services for schools*

88. Questionnaire results indicate that the most common two types of government ICT expenditure policies involve financial support for either ICT equipment or Internet connections for public schools. Each of those types of policies has been implemented in about half of the respondent countries. A quarter of the countries also mentioned having policies for buying or developing digital learning materials, such as e-textbooks.

89. Several countries have implemented policies designed to help poor and/or disabled students to gain or improve access to ICTs. For example, Chile's Digital Empowerment of Persons with Disabilities policy aims to improve access, participation, retention and learning for students with a disability or disease through the use of ICT. The programme delivers technologies and digital resources, including teaching training for the efficient use of those resources. Its purpose is to improve their pedagogical practices to give students a more inclusive and sustainable education. Costa Rica's "Tecno@prender" programme is aimed partially at educational institutions in zones that have shown lower economic development. It supports curriculum development and the promotion of meaningful learning process for students by providing ICT infrastructure and equipment as well as connectivity in educational institutions. Estonia has a needs-based support system for students who cannot afford digital devices or who have specialised digital device needs due to a disability. Israel provides assistance to 2400 schools for buying ICT equipment, acquiring Internet access, and supporting teachers in the use of ICTs, depending on the socio-economic level of their students.

90. A number of other innovative programmes were described in the questionnaire responses. Among these is Brazil's policy for bringing broadband to rural public schools: to obtain spectrum for

commercial operation of mobile 4G services, companies must provide free broadband Internet access (wired, wireless or via satellite) to rural schools. Colombia's Democratizing Innovation in the Americas programme connects vulnerable young people (ages 15 to 25) from low-income backgrounds with ICT-related economic opportunities in their regions. Luxembourg's MathemaTIC is an interactive learning app introduced by the Ministry for Education in all primary classes for 10-12 year old students. They can access MathemaTIC 24/7 on any connected device, at school, home or elsewhere. Parents and teachers can use the app to track students' learning progress. The app is also available in several languages. Mexico's Digital Inclusion Programme is notable for its breadth as well as the fact that it aims to prepare students for the 21st century by focusing more on creating information than consuming it. The programme provides connectivity and digital devices; training to promote teachers' ICT skills and their ability to apply them in pedagogic activities; digital educational resources that will be curated and evaluated to ensure their quality and impact; initiatives that promote creativity and research for solving today's social problems through ICT; and ongoing monitoring and evaluation that will allow the programme managers to find ways to improve it. About two million students and teachers are expected to benefit from this policy. Finally, through policies such as E-school bag, Slovenia has developed 30 interactive e-textbooks covering mathematics, sciences, languages, history, etc.

91. Some policies for developing students' ICT skills are being implemented at very substantial scales. China, for instance, has a long-term policy that aims to give all primary and secondary schools full network coverage, including fixed broadband and WiFi. So far, 87 percent of Chinese schools are fully covered. Poland aims to create a network connecting all of its approximately 30,000 schools via broadband Internet access by 2018. Turkey's FATIH project will invest about USD1.3 billion to equip all schools with broadband Internet connections and smartboards and to distribute tablets to 8 million students.

*ICT literacy objectives in school curricula are expanding beyond proficiency in productivity software and coding*

92. With respect to ICT literacy in state and national school curricula, objectives have branched out beyond teaching competency in coding and the use of productivity software such as word processing and spreadsheets. Several countries have recognised the need to provide students with the means to use ICTs safely and responsibly, as well. For example, Japan not only encourages its schools to familiarise pupils with computers and information and communications networks, and to teach basic operation skills, but to provide instruction on information ethics and how to use information devices appropriately. Similarly, Portugal's Seguranet Project promotes safe Internet and mobile devices usage in the educational community. In addition to basic computer and programming skills and the use of software, Latvia's school curriculum includes digital security.

93. Other countries' ICT curricula include other topics such as teaching students how to critically assess what they see online and encouraging them to take advantage of e-government resources. Singapore's Media and Digital Literacy programmes, for example, aim to nurture discerning citizens who have the ability to evaluate media content effectively and to use, create and share content safely and responsibly. The Digital Poland programme, meanwhile, aims to enhance students' ability to use the Internet and specifically includes the use of e-public services.

*Policies in support of vocational training and higher education in ICT are common, may involve partnerships with the private sector, and sometimes aim to assist specific groups such as the unemployed, women, and the elderly*

94. A large majority of respondents have policies in place to support vocational training and higher education in ICT. Frequently, but not always, these involve programmes that lead toward a university degree or a vocational certification. They are also often funded entirely by the public sector.

95. However, several countries have formed partnerships with corporations, professional associations and other groups to fund and design programmes that produce trained personnel with ICT skills that match available jobs. Estonia's Ministry of Education and Research, for example, cooperates with private sector partners and universities to support the IT Academy initiative. It promotes the further development of IT higher education through scholarships, summer schools, in-service training, and IT curricula development, among other things. The United Kingdom has begun to offer Digital Degree Apprenticeships, which are the product of a government-backed collaboration between employers and higher education institutions. These apprenticeships help employers to tailor graduate-level candidates to their business needs through on-the-job and academic training, while young people are given opportunities to study for an Honours degree while they work.

96. Many policies are aimed at helping specific groups of people rather than students in general. Most common among these are programmes designed specifically for training unemployed people to begin new careers in ICT-related fields. The Czech Republic's Ministry of Labour and Social Affairs, for example, has a nearly USD 100 million strategy to increase digital literacy and e-skills development among job seekers, including displaced workers. Turkey offers hundreds of vocational training courses to the unemployed to help prepare them for ICT-related occupations. The Netherlands has a programme called Make IT Work that is for highly educated but unemployed people who are looking for a new career in ICT. It retrains them for jobs such as software engineering, business analysis, ICT project management and ICT consulting. Israel's Labor and Welfare Ministry offers training and job placement in ICT specifically for disadvantaged populations. An innovative feature of that programme is that it includes grants to employers who give jobs to the trainees. All of these programmes should help to soften some of the job displacement effects that are part of the digitalisation process.

97. The unemployed are not the only group that policymakers are aiming to assist with ICT training, though. In Australia, where only one in four IT graduates are women, the National Innovation and Science Agenda supports the improvement of gender equity and diversity in STEM fields, including ICT, by increasing opportunities for women. Among the initiatives is a new grant programme designed to foster interest in STEM amongst women and girls. Luxembourg supports a programme with similar objectives called Rails Girls, an idea that began in Finland but is now a global, non-profit volunteer community. It promotes women-only coding classes such as app programming. Another group, the elderly, is the focus of an Austrian policy that supports a training course leading to a further qualification for ICT teachers and trainers who work with older citizens. In addition, a Colombian ICT Ministry initiative called Apps.co has so far trained more than 65,000 budding entrepreneurs to develop their ideas into sustainable digital businesses.

*A number of countries have implemented forward-looking programmes that strive to match current ICT training priorities with expected skills needs in various industrial sectors*

98. In Belgium, for example, the employment Agency of Wallonia carries out prospective studies on the expected impact of the digital transformation on occupations and skills in a wide variety of fields. The resulting catalogue of emerging and future jobs is then used to select training courses to be reinforced. Finland's Ministry of Transport and Communications carried out such a study in 2016 specifically to find out what types of skills are needed by companies with respect to data use and intelligent robotics and automation. Meanwhile, Latvia's Ministry of Economics has made medium and long-term forecasts every year since 2008 that enable the higher education system to better match the supply of IT specialists to the labour market's demand for them.

### 6.3 Innovation, Applications and Transformation

99. Two major trends are making digital technologies transformational for industrial production. One is the decline in their cost, enabling wider diffusion, including to SMEs. The other is the growing integration of three key digital technologies: big data analytics, cloud computing, and the Internet of Things. That combination of technologies is enabling new types of applications such as 3-D printing, autonomous machines and systems, and human-machine integration. These are the applications that are likely to drive the greatest industrial innovation, and thus productivity, effects in the future (OECD, 2016c). The questionnaire explored these trends, the extent to which countries are capitalising on them, and how, with questions on topics such as what is being done to further encourage diffusion (see previous section on usage and skills), promote interoperability, and boost data analytics capabilities.

100. This section is based on responses to the innovation, applications and transformation section of the Digital Economy Outlook Policy Questionnaire by 31 countries[20]. The questionnaire responses related to this section were particularly extensive and led to a multitude of key findings. First, with regard to policies for improving conditions for digital innovation, most of them involve support for innovation networks or better access to financing. It is surprising that more of these policies do not target young firms, as research shows that they play a central role in innovation, growth, and job creation[21]. Moreover, few countries reported policies that are designed to boost investment specifically in ICTs or knowledge-based capital. The policies of that nature that were reported varied and included training to help IT and digital content businesses access foreign investment, general financial support to SMEs that introduce e-business solutions, removing a cap on foreign ownership in the communication sector, and a patent box tax incentive. Furthermore, given the promise of data-driven innovation, the level of attention and resources being devoted to policies for creating data analytics capacity is surprisingly low. Relatively few countries have policies that are specifically about data analytics, and some of them are comparatively small steps. The amount of spending is nowhere near what is being spent on other types of digital economy policies. Another key finding is that new and proposed regulations for markets where digital technologies are raising new challenges for competition show that policymakers are focusing on peer platform markets. Some of the measures they are implementing increase government control over digital technologies, whereas others grant greater freedom to them.

101. With respect to applications, countries' policies for fostering digital content creation and diffusion do not follow a distinct pattern. They include measures such as digitising cultural resources and making them available online, allowing newspapers to share their information on an independent digital platform, and building an online knowledge library that provides unlimited access to scientific periodicals and e-books. Another key finding is that a small number of countries have addressed the need for interoperable standards for the Internet of Things, but most have not. On the other hand, policies for facilitating data (re-)use across organisations and sectors are popular and take many forms. The impetus behind these policies usually involves a desire to encourage innovation, to improve public services and efficiency within government agencies, or to promote open government. Meanwhile, e-health policy measures range from small steps to ambitious undertakings and tend to involve research funding, health data platforms, or telemedicine.

102. Countries have undertaken, or are contemplating undertaking, a wide variety of reforms and reviews of their regulatory frameworks in light of the digital transformation, many of which concern labour laws or sector-specific employment rules. These include statutory reforms to formally recognise or define new work status categories and employment arrangements, the deregulation of certain sectors to remove barriers to the development of new services, and public, multi-stakeholder dialogues on the future of work. Few countries have yet gone so far as to enact entirely revised labour laws in light of the new forms of work enabled by digital technologies, but several have added new provisions and regulations to recognise developments such as teleworking and informal work contracts.

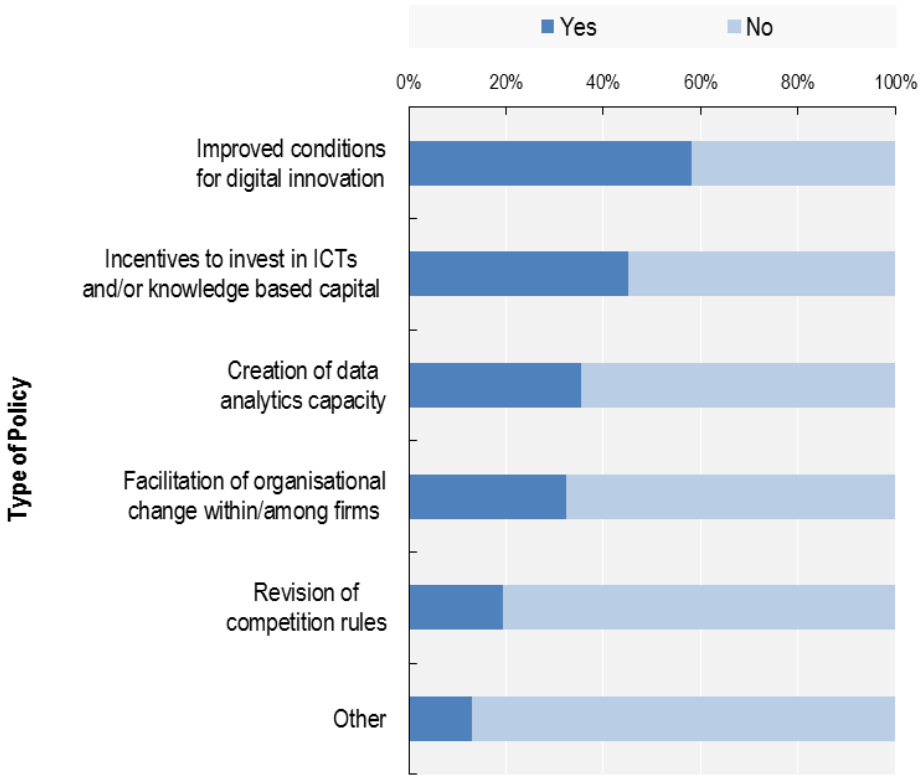
103. Finally, demonstrating that digitalisation is also transforming trade agreements, nearly half of the countries surveyed have included provisions related to trade in a digital world in their bilateral or regional trade agreements. These provisions tend to concern on-line privacy, cross-border data transfers, consumer protection for on-line transactions, restrictions on certain types of Internet content, and restrictions on the imposition of customs duties on trade in digital products.

***Digital innovation policy tends to focus on traditional measures, lacking attention to ICT investment***

104. The following discussion addresses policies and regulatory measures for stimulating or addressing digital innovation in business models and markets. It includes a discussion of regulations for product and service markets in which digital technologies are raising challenges for competition.

105. Twenty-six of the 31 countries that responded to the digital innovation section of the questionnaire have, or plan to have, at least one type of policy for stimulating digital innovation, technologies, and business models, and/or addressing related effects. The most common type of policy, implemented in eighteen of the countries, aims to improve conditions for digital innovation, such as by encouraging ICT diffusion, supporting innovation networks, or expanding access to finance. Fourteen countries reported having policies that enhance incentives to invest in ICTs and/or knowledge based capital (KBC)[22]. Eleven countries have policies that stimulate the creation of data analytics capacity, for example by investing in technologies and training. Ten countries facilitate organisational change within and among firms, such as by encouraging teleworking and teleconferencing. Finally, six countries have revised their competition rules for data-driven markets. Figure 6 provides a visual representation of this distribution of policies.

**Figure 6. Policies to support innovation**




Source: OECD Digital Economy Outlook Policy Database.

*Many digital innovation policies involve support for innovation networks and better access to financing*

106. Most of the policies for improving the conditions for digital innovation that were described by the respondents involve creating better access to financing or supporting innovation networks. With respect to financing, Brazil's Ministry of Science, Technology, Innovation and Communications has a noteworthy programme called Project Inova Empresa. It provides businesses and R&D institutes with lines of credit and other financial support to promote innovation, including digital innovation. Initiated in 2013, Inova Empresa has a budget of up to USD 11 billion and has helped approximately 400 businesses and 140 R&D institutes in the ICT sector alone.

107. Germany has taken a multi-pronged approach to financing digital innovation. The Federal Ministry for Economic Affairs and Energy, sometimes in cooperation with the European Investment Fund, has developed a suite of five funds[23] that provide different kinds of financing to innovative companies at various stages of development. For example, one fund provides equity to business angels for financing innovative companies in their early phases, while another is designed specifically to finance fast-growing but underfunded companies. Another fund teams up with investors from the private sector to provide venture capital (VC) to innovative start-ups and young technology companies, while another provides VC to innovative technology companies in the seed phase. Some of those funds have existed for more than ten years, while others started in 2016. Altogether, they have a budget of approximately USD 4 billion.

108. Regarding innovation networks, Denmark's Ministry of Higher Education and Science and the Danish Agency for Science, Technology and Innovation have helped to build 22 of them. These networks offer companies access to the latest research and innovation trends within their respective fields of expertise. The networks also help companies to find collaboration partners on small or large scale research and innovation projects by connecting private companies, researchers, the public sector, technological service providers and other partners, both in Denmark and abroad. Each network receives a main grant of approximately USD 2 million from the Agency for STI, but they also attract funding from other public and private sources. In all, 7522 companies have participated in these networks, and 5348 of them have fewer than 50 employees.

109. In 2017, Switzerland's Commission for Technology and Innovation (CTI) set up several theme-based national innovation networks that work on issues such as additive manufacturing, Industry 4.0, the digital economy, and interactive and imaging technologies. These networks will receive an annual payment from the CTI that ranges from approximately USD 200,000 to 400,000 per year.

110. One programme that does not fit into either the funding or innovation network categories is a partnership between the UK's Treasury and the Bank of England. Its purpose is to broaden access to payment systems for non-bank payment institutions. The objective is to allow FinTech payment firms to access payment systems directly. Currently, these firms must access payment systems via a bank (indirect access), which comes at a cost. Direct access is expected to boost competition starting in 2018, when the arrangement will go live[24].

111. Finally, the questionnaire results show that five of the eighteen countries that mentioned having at least one policy for improving digital innovation conditions specifically aimed their policy (or policies) at SMEs, while another five aimed at start-ups. One might have expected a sharper focus on start-ups, or at least on young firms generally. As mentioned earlier, OECD research has shown that more than half of SMEs are older businesses, but it is young SMEs (less than five years old) that play a central role in enhancing innovation, growth and job creation (OECD, 2014b).

112. Another topic that received little attention in the questionnaire responses was efforts to build a regulatory environment in which businesses can thrive and fail. By reducing the cost and administrative

burden of starting up a new company, governments can increase incentives to innovate. This includes implementing bankruptcy regulations that reduce the costs of failure and ease the legal procedures for re-starting a business, which would better recognise the fact that innovation is risky and occurs through "trial and error" (Adalet McGowan and Andrews, 2015). Figure 5 in Chapter 4 provides a comparative view of the level of administrative burdens that start-ups face in various countries.

113. Inadequate or outdated regulation may also limit the returns that firms can achieve from their investments in digital technologies, as it can hold them back from entering new markets or developing new products or business models. For example, recent OECD work finds that product market regulation, employment protection legislation, and ICT regulation have significant effects on the uptake of ICT hardware (DeStefano, De Backer and Moussiegt, 2017).

*Few countries reported policies that boost investment specifically in ICTs or knowledge-based capital*

114. Only four of the thirty-one countries that responded to the digital innovation section of the questionnaire mentioned a policy tailored specifically to increase investment in ICTs or KBC. Those policies were varied and included Colombia's training programme to help IT and digital content businesses access foreign investment, Lithuania's general financial support to SMEs that introduce e-business solutions for optimising business processes, Mexico's telecommunications sector reform that removed the cap on foreign ownership, and Switzerland's patent box tax incentive. These results seem to indicate some limitations concerning the questionnaire, though, as they do not necessarily conform to findings in other studies. For example, another source shows that at least ten OECD countries have patent boxes (Appelt, S., et al., 2016).

115. Eight countries listed at least one policy that may have the effect of augmenting ICT or KBC investment, but those policies are more general measures such as tax credits for all types of R&D or grants for investments in companies that are considered to be innovative.

*The attention and resources devoted to policies for creating data analytics capacity is surprisingly low*

116. As explained in Chapter 4, data-driven innovation holds great potential to create economic benefits and has already begun to deliver on its promise in many sectors. Overall, however, policymakers seem to be paying relatively little attention to their countries' data analytics capacities.

117. That is not to say that nothing is being done. Some respondents mentioned formidable programmes in their questionnaire responses. These include efforts such as setting up big data research centres and designing postgraduate degree programmes. One country, Colombia, has a national Big Data Strategy for its public sector, entailing a contract with the Massachusetts Institute of Technology that will result in a general architecture and pilot projects to showcase the use and benefits that Big Data Analytics can bring to the public sector.

118. But in all, only eight countries described policies that were specifically about data analytics, and many of those were comparatively small steps, such as holding big data contests and conducting assessment studies. There was nothing in this area that approached the billions of USD that are being spent on the other types of digital economy policies mentioned earlier.

*New and proposed regulations for markets where digital technologies are raising new challenges for competition show that policymakers are focusing on peer platform markets*

119. Reflecting the disruptive impact that peer platforms such as Uber and AirBnb are having, respondents mentioned the road transportation and accommodation sectors more than any others when asked to describe new or contemplated regulations for markets in which digital technologies are raising

competition challenges. (Among the 18 respondents that reported such regulations, eight listed transportation measures and five listed accommodation measures).

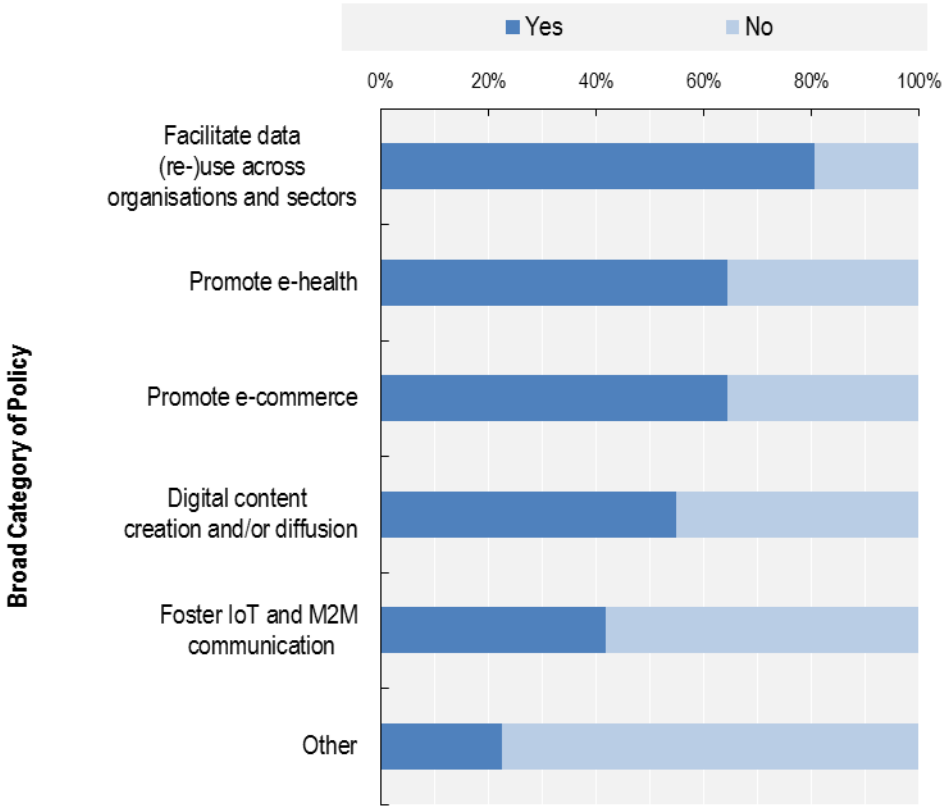
120. The responses that provided information about the specific nature of the regulations, however, were split almost evenly between those that described measures to increase government control over digital technologies (7) and those that described granting greater freedom to or otherwise assisting digital technologies (9). In a few cases the measures contained both types of elements.

121. At first glance, the split may appear to indicate a difference of opinion among the surveyed countries about whether competition from disruptive digital technologies is to be welcomed or feared. The nature of the restrictive measures that are mentioned in the questionnaire responses, though, mainly reveals concerns for consumers and tax collection rather than worries about protecting incumbent firms. France's recent Law for a Digital Republic, for example, imposed new rules for online platform operators, but they are largely aimed at protecting consumers' personal data[25]. Meanwhile, in the other category, new or proposed regulations reflect a desire to promote digital technologies. Finland, for example, is considering the idea of heavily deregulating market access in the transport sector, including taxi market (de)regulation. The objective is to enable digitalisation of the whole transport sector primarily by removing regulatory obstacles to digitalisation and innovation and by being technology-neutral.

***Digital applications and services are promoted by a variety of policy measures***

122. All 31 countries that responded to the digital applications section of the questionnaire have or plan to have in place at least one policy or regulatory measure to enhance digital applications and services. The most common type of policy, implemented in more than 80 percent of the countries, facilitates data (re-)use across organisations and sectors, e.g. by promoting open formats. Just under two-thirds of the respondents promote e-health in some manner, e.g. through better health data governance. An equal number of countries have adopted, or plan to adopt, measures to promote e-commerce. About 55 percent of countries support digital content creation and/or diffusion, including access to foreign digital content. Finally, 42 percent of the respondents foster IoT and M2M communication with measures such as interoperable standards.

**Figure 7. Policies to promote digital applications and services**




Source: OECD Digital Economy Outlook Policy Database.

*Countries' policies for fostering digital content creation and diffusion do not follow a distinct pattern*

123. Countries' questionnaire responses about digital content creation and diffusion reveal widely varying policies rather than consistent patterns. The most frequently mentioned policy measure, digitising cultural resources and making them available online, showed up in only five countries' responses. Some of the other notable policies include:

- Belgium's "Infotelligence", which allows francophone daily newspaper publishers to share the collection, processing, use and presentation of their information on an independent digital platform. Using big data and artificial intelligence, it will allow the publishers to better understand the behaviour and needs of their readers and to customize the supply of information. Consequently, the platform will offer readers better organised, more relevant content. An express aim of the project is to lead the sector away from international online giants such as Google, Apple, Facebook, and Instagram.

- Colombia's Apps.co initiative, mentioned earlier, helps to transform ideas for apps into sustainable businesses – including games, apps for the disabled, and apps for the government. So far it has funded 84 projects at a cost of approximately USD 3.5 million.

- Israel's "Campus" is an open, edX-based, national online education platform for high school students, underprivileged populations, and government employees. It is projected to benefit between 100,000 and 200,000 people in 2017, rising to 1.5 million in 2019.

- Portugal has a somewhat different education-related programme called B-on (Biblioteca do Conhecimento Online), which is an online knowledge library that provides unlimited and permanent access for research and higher education institutions to full texts of scientific periodicals and e-books through nationally negotiated contracts.

*A small number of countries have addressed the need for interoperable IoT standards, but most have not*

124. Only Germany, Japan and the Netherlands mentioned having efforts underway to develop interoperable standards for the Internet of Things. Amongst that group, Germany has far outspent its peers. Through the Industry 4.0 research agenda, the Federal Ministry of Education & Research has devoted more than half a billion USD since 2011 to fund R&D projects aimed at developing standards and applications of the IoT in production.

125. This is an area where more policymakers could make important strides: recent surveys of potential cloud users have highlighted a lack of standards – specifically open standards – as one of the biggest barriers to their use of advanced ICTs such as the IoT (OECD, 2016b, p. 33). As an example, an executive survey by the World Economic Forum (WEF, 2015) indicates that lack of interoperability ranks behind security concerns, but before uncertain return on investments (ROI), among the top three barriers to IoT adoption. Fear of potential vendor lock-in is often the culprit, as users know they can become extremely vulnerable to price increases if they cannot practicably migrate to another vendor.

*Policies for facilitating data (re-)use across organisations and sectors are popular and take many forms*

126. Policies for encouraging and facilitating data use and re-use across organisations are common amongst the respondents, with 25 of 31 countries indicating that such policies are in place. Motivations generally revolve around a desire to encourage innovation in both the private and public sectors, to improve public services, to improve efficiency within government agencies, and to promote open government.

127. About two-thirds of the data use and re-use policies focus on making government data available (or more available) in open formats. One popular measure is to create a national open data portal where the public can access wide varieties of open datasets. Alternatively, Chile holds an annual public hackathon, in which participants compete to develop the best applications using open public datasets. Since 2012, Portugal has had a National Digital Interoperability Regulation, which specifies a series of open formats and essentially states that the government must always provide information in open formats rather than proprietary ones. Slovenia's Act on Access to Public Sector Information similarly promotes open formats. The Japanese government has taken many steps to improve its use and re-use of data (see Box 2 for details on some of them).

128. Another measure adopted by several countries, including Estonia, Israel, Latvia, and Luxembourg, is based on the "once-only principle". That principle holds that public agencies are allowed to collect data only if it is not already in another public sector database. In other words, if a company or an individual has already submitted data to the public sector, then that company or individual should not have to submit it again, but rather the public sector itself should cross-use data. That clearly motivates government agencies to adopt common formats and share data across organisational boundaries, though it may also raise data protection concerns.

129. One measure unlike any others mentioned in the survey has been implemented in the UK, where a working group consisting of industry experts from the banking, data, consumer, and business communities developed an open banking standard in 2016. The standard offers guidance on how banking data should be created, shared, and used by its owners and those who access it, so as to help people

transact, save, borrow, lend and invest their money. The underlying idea was that enabling the sharing of data that banks have historically held will improve people's banking experience. When securely shared or published openly using open application programming interfaces, the data can be used to build useful applications and resources to help people find what they need. For example, customers can look for a mortgage more easily, banks can find customers whose needs match up well with a new product, and businesses can share data with their accountants. That, in turn, will improve competition, efficiency and stimulate innovation in the banking sector.[26]

**Box 2. Japan Is Taking Steps to Facilitate Governmental Use and Re-Use of Data**

Having recognised that information technology is not only a key to achieving strong economic growth, but also an important tool for transforming Japanese society and creating a safe, secure, and comfortable life for citizens, the Japanese government established the Declaration to Be the World's Most Advanced IT Nation in June 2013 to serve as its IT strategy. Since then, all parts of the Japanese government have been cooperating to promote measures based on the IT Declaration, including breaking down barriers between ministries so as to achieve cross-cutting coordination.

The initiatives undertaken over the last three years have now started to bear fruit and some of the major ones involve data use and re-use. One initiative was to **create user-oriented administrative services by reforming administrative information systems**. The government promoted radical business process re-engineering (BPR) through IT use, breaking down barriers between administrative areas with the aim of creating ways to facilitate linkages between the information systems of central and local governments and business operators. Through these efforts, the government wanted to ensure that public services are run efficiently and are convenient for users. The consolidation of administrative information systems and their migration to the cloud is reducing operating costs. The savings are being invested in efforts to enhance the value added by e-Government.

An example is the government's effort to set up new information systems for the Social Security and Tax Number System. By consolidating the central government's administrative information systems and transferring them to the cloud, Japan has saved money that it is now using to cover part of the cost of further system development and upgrades (including security measures). In fact, 908 central administrative information systems are forecast to be eliminated by FY2018 – a reduction of approximately 63 percent compared to FY2012 (when there were 1450 systems). In addition, 316 systems are due to be migrated to the cloud-based common government platform by FY2021. As a result, operating costs are expected to decline by nearly USD 900 million annually across all systems, subject to cost reductions, by FY2021. That is a savings of approximately 28 percent versus FY2013.

Another measure adopted in connection with the goal of reforming administrative information systems was setting up an infrastructure for multilayer interoperability, consisting of projects for creating a common vocabulary and Japanese characters. The former facilitates data exchange and use through the establishment of common notation, meanings, and data structures for names, addresses, and other vocabulary. The latter enables formal and simplified ideographic variants of personal and company names to be recorded and used appropriately in administrative information systems. The government expects that this infrastructure will enable administrative information systems to be linked across organisational and operational boundaries, facilitating smoother provision of public services.

A second type of initiative was to promote **safe, secure data circulation**. The idea was to improve the quality of life for Japanese citizens by means such as identifying and resolving challenges affecting a super-aging society with a low birthrate and creating new services based on data use. Japan has implemented many measures to achieve that goal, including encouraging open data initiatives by central and local governments and administrative agencies. The measures include initiatives such as establishing a government data catalog website with around 16,000 datasets and formulating the Government of Japan Standard Terms of Use (Version 2.0), approved by the Inter-Ministry Council of Chief Information Officers on December 24, 2015. To support the open data initiatives of local governments, the central government has formulated and distributed the Local Government Open Data Promotion Guidelines. In addition, it is raising awareness and offering personnel-based support through Open Data Evangelists. These are experts with deep knowledge about open data, appointed and dispatched to local governments by the Cabinet Secretariat's National Strategy Office of IT. Their role is to popularise and promote awareness of open data among local governments and support open data initiatives.

*Source*: Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (2016).

*E-health policy measures range from small steps to ambitious undertakings and tend to involve research funding, health data platforms, or telemedicine*

130. An example of funded research is the German Federal Ministry of Education and Research's R&D programme for medical technology, which aims to stimulate patient-centred innovation, support high-potential SMEs, and promote digitalisation in health care generally. Ministries in several other countries, such as Norway and the UK, have issued papers about how the health and care system could use technology, including e-health, to improve outcomes for patients and citizens.

131. Seven respondents mentioned having policy measures to create platforms, standardize health records, and link healthcare procedures and services to the people who received them, the health professionals who provided them, and the facilities where they were performed. Some of these systems, such as Brazil's Unified Health System National Card (which operates through an electronic registry), have existed for years. Others, like Costa Rica's Single Digital Health Record system, a platform to be used by primary health care centres of the Costa Rican Social Security Fund, are currently under development.

132. Finally, China, Colombia, and Germany noted that they have telemedicine policies in place. The main purpose of these programmes is to extend healthcare to more places in a cost-effective manner. One telemedicine centre in China, for instance, is connected to more than 700 two-way satellite sites and more than 60 remote vehicle satellite mobile terminals that cover more than 1300 locations across the country, facilitating remote diagnosis and treatment. Germany currently has more than 200 regional telemedicine projects underway[27].

133. Overall, countries' policy measures on e-health range from rather modest to immense. On the more modest end of the spectrum are projects such as building web-based medical appointment and cancellation systems. Towards the other end are efforts such as Germany's R&D funding programme for medical technology, mentioned earlier, which has a ten-year budget of well over USD 500 million. China's effort to develop big data for health and medical applications, meanwhile, involves building 100 regional clinical medicine data centres to give urban and rural residents standardised electronic health records and fully functional health cards. In 2016, the national population and health science data sharing platform released data sets that included biomedical, basic medical, clinical, public health, Chinese medicine, pharmacy, population and reproductive health information. The total data volume was 49.1 terabytes, equivalent to about 20 billion single-spaced typewritten pages of data.

***Digital transformations of jobs and trade have triggered reviews of legal or regulatory frameworks and the inclusion of digital aspects in trade agreements***

134. The following discussion covers policies and regulatory measures that address the digital transformation of jobs and/or trade, including reviews of regulatory frameworks, active labour market policies, and bilateral and regional trade agreements that include provisions related to trade in a digital world. It also covers new labour laws, regulation and social partners' agreements related to new forms of work enabled by digital technologies. For additional information, see OECD (2014c, 2015c, and 2016d).

135. Twenty-five of the thirty-one countries that responded to the digital transformation section of the questionnaire have at least one type of policy that addresses the digital transformation of production, jobs or trade. Among those countries, thirteen indicated that they are reviewing or have already reformed relevant regulatory frameworks, such as general labour laws or sector specific rules.

*Countries have undertaken, or are contemplating undertaking, a wide variety of reforms and reviews of their regulatory frameworks in light of the digital transformation, many of which concern labour laws or sector-specific employment rules*

136. Measures related to the digital transformation of jobs fall into two broad categories: those that have already been implemented and those that are about considering the possibility of regulatory reforms. In the former group are efforts that include

- statutorily defining telework (Slovenia) and regulating the relationship between companies and teleworkers (Colombia)
- conducting ex-ante and ex-post reviews of the administrative burdens imposed by regulations, with digitalisation being an increasingly important factor (Switzerland)
- deregulation of the transport (Finland) and fintech (Switzerland) sectors to remove barriers to the development of new services
- comprehensive reform of labour law in light of the rapid development and progress of technologies (Lithuania; more detail on the new law appears in the next sub-section)

137. The measures that involve ongoing considerations of regulatory reform in light of digital transformation include:

- Possible changes to on-call time regulations for workers in the ICT sector (Estonia)
- Deliberations on labour market regulations that are being challenged by the sharing economy (Norway)
- The design of a digital test concept for evaluating the suitability of all current regulations for meeting the challenges brought by digitalisation (Switzerland)
- A public, multi-stakeholder dialogue process on the future of work (Germany)

138. Germany's dialogue process is a major effort. Entitled Work 4.0, it is part of a comprehensive review of labour market and social policies. In 2015, the Federal Ministry of Labour and Social Affairs initiated the process by publishing a green paper for discussion[28]. The paper outlines the main trends, important areas for action and key social issues concerning the world of work in the future. It also contains a set of fundamental questions that initiated a broad dialogue about how society will work in the future. The questions were addressed with the help of experts from the fields of research and operational practice, social partners, and associations. A white paper detailing policy proposals will be published sometime in 2017.

139. Norway's deliberations on labour market reforms are also extensive. A committee on the sharing economy is assessing the opportunities and challenges that arise from the sharing economy. The potential for the more efficient use of resources is emphasised in the work. The committee is also focused on identifying regulations that are being challenged by the sharing economy, including labour market regulations. Their mandate includes:

- evaluating whether regulations should be adjusted to achieve a greater degree of symmetry between the sharing economy and traditional activities, and evaluating whether there exist regulations from which certain players should be exempted

- assessing the potential effects of the sharing economy on labour, including employees and contractors; in this regard, the committee will also consider the consequences of more people being able to be self-employed and the need for changes in the rules that apply to this group, and

- examining regulations in individual markets where sharing economy actors are especially prominent, and considering whether it is necessary to change the regulations as a result of new technology or new business models.

*Few countries have yet gone so far as to enact entirely revised labour laws in light of the new forms of work enabled by digital technologies, but several have added new provisions and regulations to recognise developments such as teleworking and informal work contracts*

140. Eleven of the thirty-one countries that responded to the digital transformation section of the questionnaire listed new labour laws, regulations or social partners' agreements related to new forms of work enabled by digital technologies that they have developed or are currently developing. Among the specific new measures implemented or under discussion in those 11 countries, new types of workers' status (7) and contracts (5) were mentioned most frequently (several countries listed more than one type of measure).

141. For example, Austria's Ministry of Labour, Social Affairs and Consumer Protection is currently observing and discussing workers' status trends so that they can be in a position to take informed, appropriate measures to address the transformation of work and ensure employee protection. The Ministry has its eye on phenomena such as crowd working, recruitment via internet platforms and comparable new forms of work. It is particularly concerned about the risk that these phenomena could cause precarity and replace regular forms of work. Depending on the relevance of these concerns in the future, the Ministry may have to develop instruments to maintain proper working and remuneration conditions.

142. In the Czech Republic, an amendment to the Labour Code is currently working its way through the legislative process. The amendment will change, among other things, provisions in the Code that concern work performed outside the employer's site, such as telework. The new approach is that whenever electronic communications networks are used for the off-site work, a) the employer must provide the hardware and software necessary for the performance of the employee's work, except when the employee performs the work using his/her own equipment, and to ensure, particularly in terms of software, data protection in case of their transfer; and b) the employee must act so as to protect the data and information related to the performance of the work.

143. Similarly, Lithuania has just completed a full revision of its Labour Code, which now includes principles regarding the protection of employees' personal data and the privacy of their personal lives. The Code now provides that the exercise of the right of ownership to the information and communication technologies used in the workplace must not infringe the inviolability of employees' communications. Lithuania's new Labour Code also introduced several new types of employment contracts: for apprenticeships, project work, workplace sharing and multiple-employer contracts.

144. Colombia is one of several countries that have set certain mandatory terms for contracts involving telework. Among the key issues that telecommuting contracts must specify are:

- the technology and required environment, and how to perform the work in terms of time and if possible space

- the days and times that the teleworker will carry out his or her activities for the purpose of defining liability in case of an accident and preventing ignorance of the legal maximum working week

- the responsibilities regarding custody of work items and the method of delivery by the teleworker when finalising the telework

- the security measures that the teleworker must know and comply with.

*The international legal framework for trade in a digital world*

145. International trading relationships are governed by bilateral, regional and multilateral trade and investment agreements, which play an essential complementary role to domestic structural reforms. Multilateral action is of particular importance in promoting the mutual interests of countries in terms of trade liberalisation, locking-in domestic reform and building confidence between firms and the societies in which they operate.

146. Trade-related aspects of the digital transformation are covered under multilateral agreements and plurilateral agreements forged at the World Trade Organisation (WTO). WTO agreements are technologically neutral, so disciplines pertaining to trade in goods under GATT, or trade in services under GATS, apply equally in the online and offline worlds. Hence a wide range of WTO agreements are considered relevant to trade in a digital world, including the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the Agreement on Technical Barriers to Trade (TBT), the Information Technology Agreement (ITA) and its recently concluded expansion, and the Trade Facilitation Agreement. Yet with rapid changes in technology, there is a discussion among WTO Members about whether there is a need to update or clarify existing rules and commitments.

147. Already in 1998, in recognition of the growth of e-commerce and the opportunities it presented for trade, WTO members agreed to establish a work programme to examine trade-related issues concerning e-commerce (WTO, 1998). They also agreed not to impose customs duties on electronic transmissions. While the agreement not to impose customs duties on electronic transmissions has been extended at every WTO Ministerial since the initial agreement, the work programme has varied over the years.

148. As the digital transformation has progressively deepened, countries have also begun to include issues specifically related to trade in a digital world in bilateral and regional trade agreements. In addition to specifying that general provisions of the agreement also apply in the online world, some bilateral and regional trade agreements include specific chapters on digital services, e-commerce and telecommunications. While agreements vary, these chapters sometimes include:

- Measures that prohibit the imposition of customs duties;

- Measures aimed at non-discriminatory treatment of digital products;

- Measures that promote paperless trading;

- Measures that prevent the imposition of localisation requirements for computing facilities;

- Measures protecting the movement of cross-border data flows;

- Measures regarding privacy on-line;

- Measures on data protection;
- Measures ensuring enforceable consumer protection for on-line transactions;
- Restrictions on certain types of Internet content (e.g. routing traffic to domestically-owned firms, blocking particular sites);
- Measures to restrict the imposition of mandatory requirements to transfer or provide access to a software's source code;
- Measures concerning unsolicited commercial electronic messages (i.e., to advocate for the effective regulation of unsolicited spam and telemarketing); and
- Measures promoting strong and balanced copyright protection and enforcement.

149. In this respect, current and future negotiations of bilateral and regional trade agreements, which increasingly touch upon some of the emerging and complicated trade issues, as well as discussions within the WTO context, will most likely pave the way to further developing the trade-related aspects of the digital transformation.

*Nearly half of the countries surveyed have included trade-related aspects of the digital transformation in their bilateral or regional trade agreements*

150. Fourteen of the 31 countries that responded to the digital transformation section of the questionnaire indicated that issues related to trade in a digital world have been included in their bilateral or regional trade agreements. Within such agreements, five of the topics in the bullet list above appeared with roughly equal frequency: privacy on-line, cross-border data flows, consumer protection for on-line transactions, restrictions on certain types of Internet content, and prohibitions on the imposition of customs duties.

151. Chile provided an extensive response and has provisions of nearly all the types just mentioned within its trade agreements. See Box 3 for more information on those provisions, most of which were mentioned by other respondents, as well.

**Box 3. Trade-related aspects of the digital transformation in trade agreements: the case of Chile**

Being aware that the digital transformation, catalysed by the Internet, is creating powerful opportunities for increasing participation in international trade, especially in sectors that have traditionally been considered non-tradable, Chile has incorporated trade-related aspects of the digital transformation in its trade negotiations. With respect to free trade agreements (FTAs), this has involved negotiating telecommunications and electronic commerce chapters that facilitate trade conducted electronically by ensuring that it takes place efficiently and with appropriate consumer protections:

- *Measures regarding privacy on-line*. Many of the FTAs negotiated by Chile include provisions that recognise the economic and social benefits of protecting users' personal information and the contribution that this makes to enhancing consumer confidence, especially in electronic commerce. Chile has adopted provisions in its FTAs that mandate the adoption of laws or regulations for the protection of personal information. Another set of provisions allows taking measures that are deemed necessary to ensure the security and confidentiality of messages and to protect end-users' personal data. See, for instance, Trans-Pacific Partnership Article 14.7: Online Consumer Protection, and the Pacific Alliance's Article 13.8: Protección de la Información Personal.
- *Measures regarding cross-border data flows*. In accordance with the technical architecture of modern

electronic communications networks, and having regard for the end-to-end principle, Chile's practice in this area has been to allow, as a general rule, the cross-border transfer of information by electronic means, when this activity is necessary for conducting business. However, nothing prevents a party from taking measures that are necessary to ensure the security and confidentiality of messages and to protect end-users' personal data, provided that those measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

- *Measures concerning consumer protection for on-line transactions*. As a way to increase consumer confidence, Chile has recognised the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities, including provisions mandating, adopting or maintaining consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities. Certain FTAs also include provisions that aim to enhance cooperation between national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare.

- *Restrictions on certain types of Internet content*. Chile does not include this kind of restriction, as it would be against consumers' choice to access and use services and applications available on the Internet.

- *Measures that restrict the imposition of customs duties on electronic transmissions*. Chile has a standing practice of not imposing customs duties on electronic transmissions, including electronically transmitted content. Chile seeks to ensure non-discriminatory treatment of digital products (computer programs, text, videos, images, sound recordings or other products that are digitally encoded and that can be transmitted electronically) that are transmitted electronically, which includes guaranteeing that these products will not face discriminatory measures based on the nationality or territory where they are produced.

*Source*: OECD Digital Economy Outlook Policy Database.

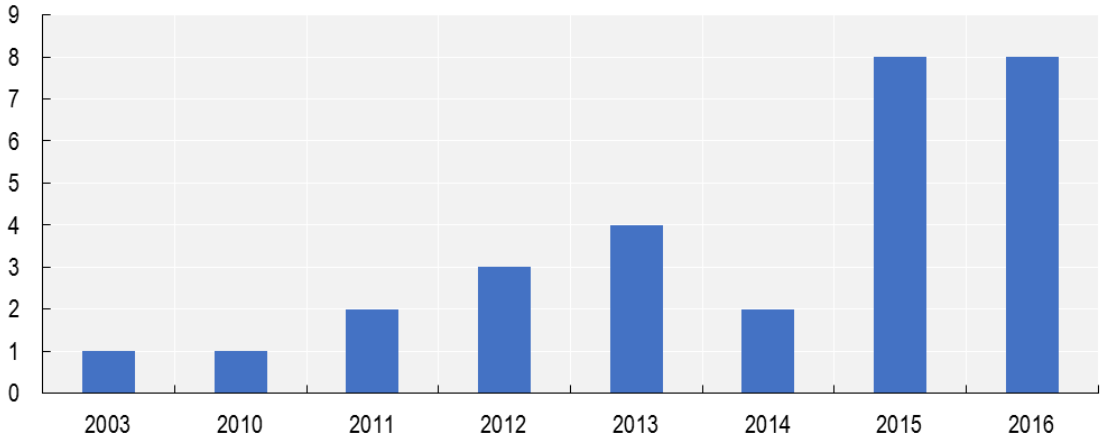
## 6.4 Digital Risk and Trust

152. As highlighted in Chapter 5, individuals (including consumers) and businesses have several means at their disposition to enhance the level of trust in the digital economy, ranging from transparent online reviews for consumers to risk management practices in organisations. However, evidence presented in Chapter 5 also shows that there are still several challenges to be addressed. This section discusses the role of public policies in addressing these challenges, with a focus on digital security, privacy and consumer protection. It discusses current policy trends including the development of national strategies related to digital security and privacy respectively. The digital security policy measures discussed include measures to build capacity, international co-operation, as well as measures to promote digital security risk management, information sharing and exchange, and the digital security industry. The discussion of privacy related policies includes, for example, policy measures to promote awareness raising and education, technical measures for privacy protection, and international co-operation.

### *Nearly all countries surveyed reported having introduced National Digital Security Strategies*

153. National digital security strategies are essential to establish the trust needed for economic and social activities to fully benefit from digital innovation. In 2016, 29 of the 33 countries that responded[29] to the digital security risk section of the 2016 DEO Policy questionnaire indicated they had introduced national digital security strategies (Figure 8) and the other four were in the process of developing one. National strategies are developed by a variety of government agencies and organisations ranging from the Cybersecurity Agency in France and Singapore to the ministry of defence in Denmark and the ministry of the interior in Iceland. Although most countries had involved non-governmental stakeholders in the development of their national strategy, only 56 percent reported having carried out a broad public consultation on the strategy. Nearly half of the surveyed countries are planning to revise their strategy in 2017-2018.

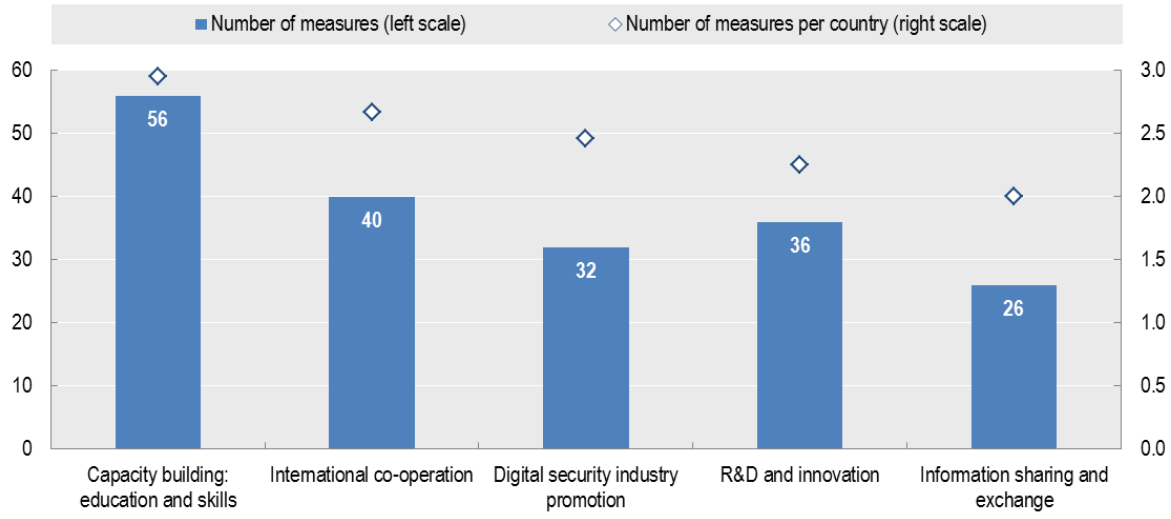
**Figure 8. Number of Countries Introducing National Digital Security Strategies**




Source: OECD Digital Economy Outlook Policy Database.

154. Figure 9 shows several types of measures to strengthen digital security that were frequently mentioned by countries that responded to the digital security risk section of the questionnaire. Most prominent are measures that aim to build capacity through education and skills, including steps to promote digital security risk awareness in SMEs, and international co-operation.

**Figure 9. Policy measures to strengthen digital security**




Note: This figure is based on a total of 190 policy measures to strengthen digital security reported by up to 19 countries.

Source: OECD Digital Economy Outlook Policy Database.

*Capacity building focusses on education and skills development*

155. Demand for cybersecurity specialists has increased significantly in recent years but supply has remained low. Increasing the current pool of skilled digital security and risk management professionals is a policy objective for 31 of the 33 countries that responded to the digital security risk section of the

questionnaire. According to 2016 data by the Burning Glass, in the United States online job postings for digital security professionals took approximately 14 percent longer to fill than the average for all IT jobs. Digital security talent shortages are reported by all countries.

156. Amongst the main barriers to attracting more individuals to digital security professions, countries mentioned low awareness of career opportunities, which is compounded by the limited statistics on job offerings and absence of a standard higher education curriculum. Today, digital security is part of specialized postgraduate programmes, certifications or professional trainings. Whereas what is needed is a system in which digital security skills are honed from primary to secondary education, university as well as in work-based training.

157. Countries are introducing a wide range of policy measures and initiatives aimed at addressing the digital security skills gap. In the United States, the National Initiative for Cybersecurity Education is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Luxembourg created in 2017 the Cyber Security Competence Centre, based on a public-private partnership with the objective of delivering cybersecurity services and training. In the United Kingdom the National Cyber Security Centre established in 2016 aims to work with industry, government and academia to support the next generation of researchers, students and innovation. In France, the National Digital Security Agency, ANSSI, has recently launched a number of training and professional certification initiatives (e.g., CyberEdu, SecNumedu) in collaboration with universities and the private sector. Korea's MSIP/KISA provides scholarships for digital security college students including budget support for universities.

*Steps are being taken to promote SMEs digital security risk awareness and foster good practice*

158. When asked about the three most pressing digital security challenges affecting economic and social activities, most countries responding to the OECD survey mentioned cyberattacks against small firms or cyberattacks that disrupted or prevented economic and social activities and cybercrime/cyberespionage that involved the theft of digital intellectual property and assets.

159. Small and medium enterprises (SMEs), and early-stage start-ups in particular, are critical to economic growth; they drive competition and innovation, and contribute to job creation. They also face distinct challenges in managing digital security and privacy risk. A digital security incident that can result in a loss of consumer trust, damage to reputation, or a drop in revenue, may be more damaging for SMEs than for larger companies because they are more likely to find it difficult to weather a temporary loss of customers or revenue. As well, they may not have the resources or expertise to effectively assess and manage risk. On the positive side, SMEs that are aware of the risk and can demonstrate they have robust digital security and privacy practices may have a competitive advantage when seeking partnership opportunities with larger organisations.

160. Promoting digital security risk awareness by SMEs was a specific objective of 82 percent of countries. However, only 46 percent of countries who responded have developed specific incentives (rewards and/or sanctions) for business to promote digital security risk management.

161. Korea and Japan are providing tax incentives for companies that invest in digital security products.

162. The UK also requires that "only companies that have a valid Cyber Essentials certification can supply central government with any services that require the processing of personal data". The *Cyber Essentials* scheme identifies some fundamental technical security controls that an organisation needs to have in place to help defend against Internet-borne threats.

163. Lithuania can apply "economic sanctions" against companies that do not meet legal obligations regarding digital security.

164. Nineteen out of 33 countries reported that there was interest in digital risk insurance (cyberinsurance) as a market-based approach to manage business risk. Insurance coverage for digital security risk is viewed by these countries as a means for companies and individuals to transfer a portion of their financial exposure to insurance markets. Insurance companies can also potentially contribute to the management of digital security risk by promoting awareness, encouraging measurement, and by providing incentives for good practice. Those same countries generally have considered measures to encourage businesses to adopt digital security risk insurance. The digital security risk insurance market is still developing, however, and countries that did respond reported that they were just looking at how policy in this area could be applied. Canada, for example, reported that it is in the early stages of assessing this issue as part of its cyber review.

165. These opinions are reflected in the responses of countries when they were asked to rank, in order of relevance, eight main obstacles to the adoption of risk insurance in their countries.

**Table 2. Obstacles to the adoption of risk insurance**

| Obstacle | Mean Rank |
|---|---|
| **Lack of actuarial models** | 3 |
| **Insurance premiums are too expensive** | 3 |
| **Management does not see the value of this type of insurance** | 3 |
| **Coverage is inadequate** | 4 |
| **Current insurance policies are considered sufficient** | 4 |
| **Digital security risk does not warrant insurance** | 4 |
| **There is no market for digital security insurance products** | 5 |
| **There is no supply of digital security insurance products** | 6 |

Source: OECD Digital Economy Outlook Policy Database.

166. The top two obstacles for most countries were:

1. Lack of actuarial models - More comprehensive data on the frequency and impact of digital security incidents (and the related claims payments) is needed for the development of actuarial models and to provide more confidence in the underwriting of insurance coverage for digital security risk.

2. Cost of insurance premiums - The premiums for digital security insurance per million in coverage has been estimated to be three times more expensive (for the same amount of coverage) than general liability coverage and six times more expensive than property coverage.

167. Finally, countries were asked about any other policy measures considered important to promoting digital security risk management as a business priority. Canada listed the following policy measures:

- Effective de-identification/anonymisation/pseudonymisation practices

- Addressing accountability for all stakeholders involved in the information lifecycle

- Protecting communication channels
- Identifying risks associated with metadata
- Updating and maintaining privacy enhancing measures (such as encryption)
- Audit controls
- Risk assessments (privacy impact assessments and threat risk assessments)
- Up-to date and revised information sharing agreements

*International co-operation enables progress on information sharing and at the technical level*

168. Facilitating international co-operation on cross-border digital security issues is a priority for all countries that responded to the survey. Countries mentioned a large number of initiatives aimed at improving international collaboration particularly to promote greater information sharing and exchange on digital security incidents.

169. The European Directive on Security of networks and information systems (NIS Directive) adopted in 2016 represents a very significant step in this direction. The Directive requires EU Member States to increase their preparedness by establishing a Computer Security Incident Response Team (CSIRT) and a competent national authority in charge of digital security, and to improve strategic co-operation and exchange of information with each other. Additionally it requires EU Member States to adopt appropriate measures to promote of a culture of digital security risk management. Member States are also asked to "ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations", which includes an obligation to notify incidents having a significant impact on the continuity of the essential services they provide.[30]

170. The NIS Directive's aim is to create a collaboration framework, within which the Member States and the European Commission can share early warnings on risks and incidents. Co-operation is facilitated by the creation of a single point of contact in each country, the establishment of a "Cooperation Group" with representatives of the Member States, the European Commission and the European Network and Information Security Agency (ENISA), and by the creation of a CSIRTs Network. EU members have until May 2018 to adopt appropriate laws and regulations to comply with the directive and some countries such as France[31] and Germany[32] have already adopted legislative and regulatory measures in this area.

171. In accordance with its International Strategy for Cyberspace, the policy priorities of the United States are to promote innovative open markets; enhance security, reliability, and resilience of global networks; and extend law enforcement collaboration. There are many venues and forums in which the US promotes information sharing. A key area of focus is information sharing between CSIRTs with national responsibility. Accordingly, the US government works closely with foreign authorities, as well as through international and regional organizations focused on cybersecurity information sharing. Similarly, Australia partners with international law enforcement, intelligence agencies and other computer emergency response teams. The country is planning to appoint a Cybersecurity Ambassador who will identify opportunities for practical international cooperation and ensure Australia has a coordinated, consistent and influential voice on international cybersecurity issues.

172. Canada's Computer Emergency Response Team (CERT) works with the international CERT community in an effort to address and co-ordinate responses to serious cyber security incidents. In

Colombia, "The National Digital Security Police of Colombia, through the Police Cyber Center, is part of international agreements and alliances in order to report incidents." Latvia has a memorandum of understanding in place for co-operation in cybersecurity with Lithuania and Estonia. Separate MOUs cover agreements with Azerbaijan and Kazakhstan and Georgia. Spain highlighted the role of the international Forum of Incident Response and Security Teams (FIRST[33], 2016) in coordinating incident reporting. France is actively promoting its approach to the protection of critical infrastructure to other countries. It will also be part of formal collaborations in Europe as a result of the implementation of the NIS Directive including the "European network of CSIRTs". France is also participating in CERT -level cooperation groups (TF CSIRTs, FIRST, NatCSIRT, AfricaCERT) bringing together CSIRTs around the world. Finally, 24 OECD members, 13 non-members, 8 international organisations and 11 companies have joined the Global Forum for Cyber Expertise (GFCE) launched in 2015 in the context of the Global Conference on Cyber Space. The objective of the GFCE is to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level.

***Privacy protection continues to rise on governments' agendas as privacy challenges further intensify***

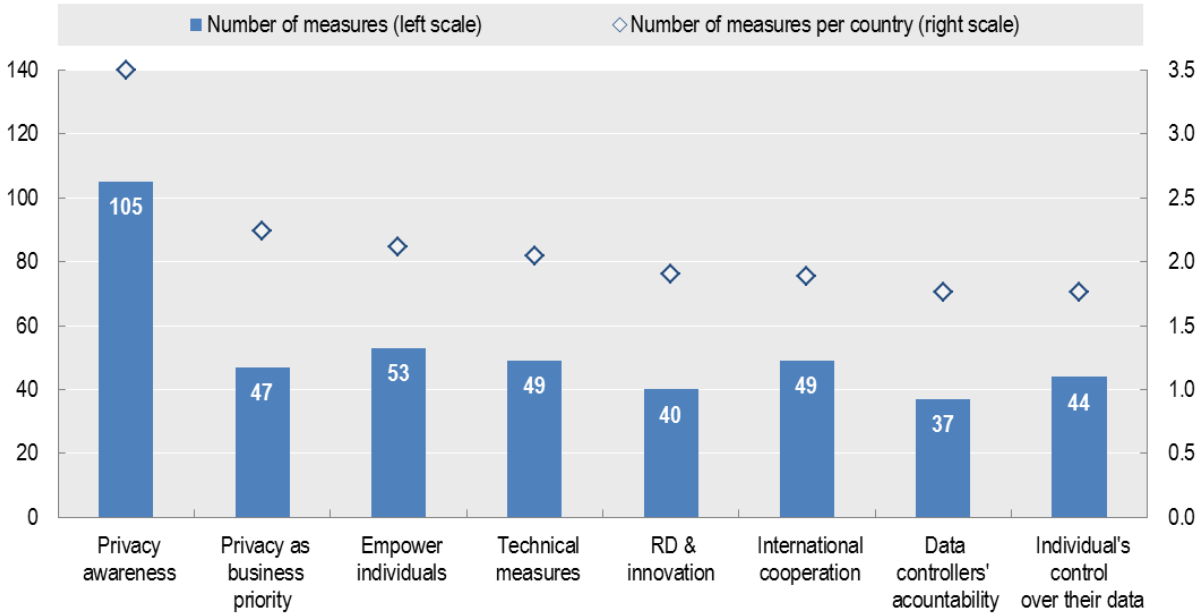
173. The diffusion of the new digital technologies such as Internet of Things (IoT), big data and algorithmic decision-making through artificial intelligence (AI; see Chapter 7) are raising deep questions as to the potential impacts on individual privacy and data protection. For the large majority of governments responding to the 2016 OECD Digital Economy Outlook Policy Questionnaire (25 out of 34 countries[34]) these technologies pose significant challenges in the application of existing regulation. Some governments have highlighted that these new technologies raise new societal and ethical challenges that need to be better understood and may need to be addressed through the development of new data governance framework and policies. For example, the French Commission Nationale de l'Informatique et des Libertés (CNIL) has established a working group on innovation and digital technology that is undertaking a reflection on these issues (see section below). Effective anonymization or de-identification of personal data in the context of open (government) data also rank high among the identified technological challenges, which many governments aim to address through innovation-enhancing policy measures.

174. Many governments (15 out of 34 countries) also highlight the international dimension of privacy as a policy issue of growing importance given the increasing reliance on cross-border data flows. In this context lack of, or poor, legal interoperability is seen as one of the biggest challenges, in particular by non-European countries. This is true not only at the international level (between national privacy regimes), but also at the national level (between regional privacy laws) in some countries.[35] For European Union (EU) member countries, the most important development in this area has been the adoption of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) which takes effect on 25 May 2017 and replaces the current Data Protection Directive 95/46/EC.[36] While the GDPR will resolve remaining barriers to legal interoperability between EU member countries, a number of new questions on the effective implementation of certain provisions in the new Regulation remain, such as the implementation of a new right to data portability[37] (see section below). For some EU member countries, the renewal of their data protection framework may thus raise new policy challenges, but also new policy opportunities, in particular in respect to the development of possible national privacy strategies and policies. The effects of the GDPR goes beyond EU member countries as it will affect for instance international businesses active in the EU (OECD, 2016x). Legal interoperability therefore remains crucial as highlighted in Part Six of the OECD (2013) *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines) on international co-operation and interoperability, which states among other that: "Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines."

175. In most countries, the use of big data by governments emerges as a major legal challenge for privacy protection. Of 32 countries responding to question on privacy challenges, 18 have highlighted that the reuse of personal data across government agencies constituted a policy challenge for privacy protection. Among them around half indicated that the collection of personal data for (national) security interest was one of the biggest policy challenges, in particular in cases where personal data was collected from the private sector. In Canada, for instance, the use of new investigative techniques by government institutions leveraging digital technologies to produce "digital evidence" on individuals is creating privacy risks. In particular, information sharing between government agencies has increased dramatically following the introduction of the Anti-Terrorism Act (Bill C-51). Under the Act's changes, seventeen government agencies like the Canada Border Services Agency or the Canada Revenue Agency can now share information with, for example, Health Canada or the Communications Security Establishment. This means significantly more personal information could be exchanged, increasing the risk of privacy violation. Another pertinent example, is the Directive (EU) 2016/680 which still needs to be transposed into national law in all EU member countries, and aims at the "processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data".[38] In 2016, Brazil has adopted Decree n. 8.789, which regulates the sharing of databases containing personal information held by governmental bodies. The Decree allows government processing of personal data and more specifically the gathering of personal data for national security reasons including access of personal data through legal interception, which has raised concerns especially when over the top (OTT) services are involved.

176. The 2016 OECD DEO Policy Questionnaire reveals that governments have adopted a wide range of policy measures to address the privacy challenges highlighted above (and in Chapter 5). Among these policy measures, promoting privacy awareness ranks by far the highest (see Figure 10). Of the 424 policy measures on privacy that responding countries reported having, one quarter (105) were adopted to raise privacy awareness and education (in government, business and individuals). Another quarter empower individuals either through easy and clear redress possibilities or through mechanisms to enhance individuals' control over their personal data (in both cases, 97 measures in total). Other policy measures that ranked high on governments' agenda included measures to foster privacy as a business priority and to support privacy related innovation and the adoption of technical measures (136), followed by the promotion of international cooperation and the coordination and harmonisation of privacy legislation across government agencies (49). The following sections discuss the most frequently adopted policy measures in more detail.

**Figure 10. Policy measures to promote privacy**




Note: This figure is based on a total of 424 policy measures to strengthen digital security reported by up to 30 countries.

Source: OECD Digital Economy Outlook Policy Database.

*Awareness, skills, and empowerment are the most frequent policy levers used by governments to promote privacy protection*

177. To better protect privacy, it is necessary to be both aware and well informed about all potential privacy risks. Policy makers and privacy enforcers recognise raising the level of awareness, skills and empowerment as a key lever to better address privacy risks (OECD, 2015). In fact, enhancing privacy awareness and education is the policy measure most frequently adopted, in particular by privacy enforcement agencies. Most agencies do so by providing guides and good practices, including offline or online publications; the latter usually through dedicated web sites. Some agencies provide templates to help organisations develop privacy notices such as in the case of Mexico (see https://generador-avisos-privacidad.ifai.org.mx) and privacy management plans such as in the case of the Office of the Australian Information Commissioner (OAIC). The OAIC developed a specific privacy management plan template for public sector agencies.[39]

178. Many government agencies are reaching out to the public through events such as conferences, consultations and workshops. While some of these events aim to provide the public with basic knowledge and a better understanding of privacy (see e.g. regular roadshows and talks organised by Singapore's PDPC to educate the public on the importance of protecting own personal data), others are dedicated to more specific and advanced privacy issues. Examples for the latter include a public workshop organised by the United States (US) Federal Trade Commission (FTC) to examine the predicted changes in various diverse groups and discuss what impact those changes will have on the marketplace, or a series of public debates on the ethical questions raised by algorithmic decision making initiated in January 2017 by the CNIL in accordance with its new mission of looking at the ethical and societal issues raised by digital technologies. Several agencies are also using media, including in some case serious games, to raise awareness about privacy issues. The Israeli Law Information and Technology Authority (ILITA), for

instance, initiated a comprehensive plan for media appearances in television, radio, newspapers and on the Internet with regards to the importance of the right of privacy, data protection and the related risks. The CNIL, as another example, has organised a web campaign based around a serious game « Fred et le Chat démoniaque » to illustrate privacy risks associated to the dissemination of digital content.

179. Education and training programmes also rank high among the measures adopted by governments to promote privacy. While most of these measures target students and teachers (mainly in primary and secondary education institutions), others focus on adults working in the public sector. Education programmes aimed at the private sector were less frequent. In 2015, for example, Canada's Office for the Privacy Commissioner (OPC) created and distributed a classroom activity to schools across Canada to help teachers familiarise students with privacy policies and issues related to the collection of personal information online. In Norway, the Center for ICT in Education together with the Data Protection Authority (DPA) put in place an initiative, DuBestemmer (YouDecide), to disseminate teaching resources about privacy and digital responsibility for children and young adults aged 9-18 years. Focusing on government officials, the Ministry of Internal Affairs and Communications (the Administrative Management Bureau) of Japan, developed a course about the implications of privacy within the government.

180. In terms of mechanisms for enhancing empowerment, most governments have mechanisms to simplify privacy complaints procedures, such as introducing digital services[40], and in some cases emphasising the introduction and/or simplification of compensation claim procedures.[41]. A recent development is the implementation of mechanisms to enhance individuals' access to their own personal data, such as the regulation of EU member countries by Article 20 on the "*right of data portability*" of the GDPR. Other countries have also implemented or are considering implementing similar rights. For example, the Blue Button initiative of the U.S. Dept. of Health and Human Services allows patients to download their health records quickly and securely. ILITA, as another, published draft guidelines for public consultation according to which, service providers must transfer consumers' electronic transcripts of phone conversations or chats upon their request. All these mechanisms are in line with the Individual Participation Principle of the OECD Privacy Guidelines: In the world of big data, data portability seems the only reasonable means to provide data "in a form that is readily intelligible to [the individual]". This is because data portability enables the individual to apply data analytics and related services to his or her own personal data to gain the knowledge needed to e.g. "challenge data relating to him". However, questions on how best to implement data portability remain unanswered.

*Fostering privacy as a business priority and supporting related innovation and their adoption rank high among government policies*

181. While regulatory developments are ongoing, there is increasing understanding that regulation will be only one element in strengthening privacy protection. A recent development, for example, is the promotion of privacy as a business opportunity. Governments have adopted different types of approaches to achieve this objective. A large majority of governments are relying on awareness raising campaigns as discussed already above. The Finnish Ministry of Transport and Communications, for instance, organises the Digital Business Forum on Data Protection two to three times a year with the goal not only to help companies prepare for GDPR implementation, but also to see data protection as a business opportunity. Similarly, in Italy where ILITA has highlighted in its Vademecum for Business[42] ten best practices that can improve not only a firm's corporate social responsibility image but also business performance, essentially by increasing consumers' trust.

182. Many governments are also implementing certification schemes to increase business' incentives to implement effective privacy enhancing processes. In Korea, for instance, the Korea Communications Commission (KCC) incentivises businesses to obtain the Privacy Certification (PIMS) by reducing fines or

postponing sanctions when a certified business faces a privacy violation investigation due to a personal data breach. Similarly, in the United Kingdom where the ICO is currently planning a privacy seals programme that could act as a 'stamp of approval' demonstrating good privacy practice and high data protection compliance standards. In some other cases, governments are promoting privacy as a business priority by putting emphasis on the link between digital security and privacy protection. For instance, this is the case in Mexico, where the Federal Institute for Access to Public Information and Data Protection (INAI) provides a table of functional equivalence between digital security standards and in collaboration with the Spanish National Cybersecurity Institute (INCIBE) has developed a strategic plan to help organisations improve their digital security when processing personal data.

183. Research and development (R&D) is being increasingly promoted by Governments to address privacy issues arising from emerging technologies such as the IoT. Governments are also promoting R&D in privacy enhancing technologies, including anonymization and cryptography technologies and techniques, as well as their adoption across organisations. While it is true that most countries have policy measures that are aiming directly or indirectly at the promotion of (academic) research (the 'R' of R&D), policy measures promoting the development of business relevant technologies and applications (the 'D' of R&D) as well as new business models remain rather rare. Very few countries have established funding schemes to directly support privacy related R&D and innovation. But there are positive exceptions: France's Investments Programme for the Future (Programme d'investissements d'avenir, PIA) supports the development of privacy enhancing technologies. In October 2015, a call for projects was launched within the Programme to mobilize up to EUR 10 million for innovative companies in three areas: (i) the anonymization of personal data, (ii) the protection of privacy in the context of the IoT, and (iii) innovative privacy architectures, such as distributed architectures. The objective of this call for projects is to encourage good practices in privacy enhancing technologies and to support companies in developing commercial solutions. Another example is SPRING Singapore, an agency under the Ministry of Trade and Industry, that developed a funding scheme (the Capability Development Grant, CDG) to promote the adoption privacy enhancing processes in SMEs. Up to 70% of the project cost of a SME for enhancing its privacy measures are covered by the CDG.

*While most governments engage in international collaboration, many are still lag in coordinating their own domestic privacy policies*

184. International co-operation remains and will continue to be an important policy area for privacy protection as the volume of cross border data flows increases. Governments ranked the potential incompatibilities of legal regimes as a key rationale in favour of international co-operation, before the lack of resources to address international privacy issues and existing restrictions on international data sharing, including the current practices of law enforcement and intelligence agencies to collect or exchange personal data internationally. Of the 34 countries responding to the 2016 OECD DEO Policy Questionnaire section on privacy, 26 countries could name at least one initiative through which they cooperate internationally. Participation in the Global Privacy Enforcement Network (GPEN) was most frequently cited as a key arrangement for privacy cooperation, beside the Article 29 Working Party (in the case of EU member countries) and the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Enforcement Arrangement (in the case of APEC countries). In addition, for EU member countries and the US an important development has been the establishment of the EU-U.S. Privacy Shield Framework, which represents a significant achievement for data protection as it provides legal certainty for data flows between the US and Europe.[43]

185. Privacy policy making and regulation involves multiple government agencies, including but not limited to privacy enforcement agencies and ministries in charge of justice or legal affairs and the digital economy. But it also involves government agencies in charge of specific sectors such as health care, finance, and transportation to just name a few. This means that privacy policy making and regulation

requires ongoing mechanisms or processes to ensure coordination and coherence of policy and regulatory developments and implementation. However, while most governments engage in international collaboration, in particular through their privacy enforcement agencies, domestic coordination of national privacy policy and regulatory development remains poor in a number of countries. According to the responses to the 2016 OECD DEO Policy Questionnaire section on privacy, a third of all responding countries do not have an ongoing mechanism or process in place to ensure coordination and coherence of their privacy policies and regulations at national level, and even where countries report having such mechanisms in place, the extent to which these are effective remains uncertain.

186. In many countries privacy policy coordination is achieved at different levels during policy development. This can involve cross-governmental working groups, national consultation procedures and public-private partnerships. In other countries, a dedicated coordination body exists – in some cases attached to highest level of government (e.g. prime minister's office) – to ensure coordination and coherence of policies and regulations across government agencies. This is for example the case in Israel where a central unit in Israel's Prime Minister's office is evaluating the efficiency of Israeli regulations including privacy regulations. In some countries, the introduction of a coordination mechanism was established in the context of the development and/or implementation of their national digital economy strategy (see Chapter 1). In the process of the launch of *Digital Roadmap Austria* in 2015, for example, a coordination team was formed, and all federal ministries were involved as well as a number of local authorities and the social partners. In other cases, the negotiation of the GDPR has been a driver to establish or enhance domestic coordination mechanisms in a number of EU member countries. In Belgium, for instance, processes have been put in place to coordinate between the different public authorities, as well as to engage with the private sector during the negotiation of the GDPR. To what extent these coordination processes and mechanisms are still used and effective to ensure the continuous coordination and coherence of privacy policy and regulation is to be seen.

*The development of national privacy strategies promises to enhance a whole-of-government approach to privacy*

187. Legislation continues to be the primary response to addressing personal data protection. Rather than being directed at all stakeholders, these laws typically impose obligations on organisations subject to the law and require them to grant individuals specific rights. As highlighted in the previous sections, there are a wide range of complementary measures such as education and awareness-raising, which however are often left to privacy enforcement authorities or civil society bodies. While protection by the law is essential, privacy in an increasingly data-driven economy would thus benefit from a multifaceted strategy, reflecting a whole-of-society vision, and supported at the highest levels of government, as called for in the OECD Privacy Guidelines (Part Five) and more generally in Chapter 1 of this report (see section 1.4).

188. The OECD Privacy Guidelines recommend that governments "develop national privacy strategies that reflect a co-ordinated approach across governmental bodies". Along the model of "digital security strategies", such multifaceted privacy strategies would help create the conditions for privacy protection to become a differentiator in the marketplace while providing the flexibility needed to capitalise on emerging technologies. They could also encourage R&D and innovation with respect to privacy by design approaches and help focus efforts by privacy enforcement authorities and other actors. Coordinated privacy strategies at the national level would help foster cooperation among all stakeholders and lessen uncertainty in data flows.

189. While many countries have adopted national digital security strategies, very few countries have adopted equivalent privacy policy strategies despite the need to introduce, or improve existing, coordination mechanisms as highlighted above. According to the responses to the 2016 OECD DEO Policy Questionnaire section on privacy, more than half of the countries (18 out of 34 countries) clearly indicated

that they did *not* have a national privacy strategy. For most countries, including those that report having a national privacy strategy, the concept is either misunderstood or remains unclear.

***As the e-commerce marketplace evolves so do policy responses to protect consumers and ensure trust***

190. Policymakers have implemented a number of initiatives to protect and empower digital consumers and address some of the impediments to trust described in Chapter 5. The recent revisions to the *OECD Recommendation on Consumer Protection in E-commerce* provide a robust foundation to guide policy initiatives for a global online marketplace. More specifically, the Recommendation addresses challenges relating to information disclosure, misleading and unfair commercial practices, confirmation and payment, fraud and identity theft, product safety issues and dispute resolution and redress. Its provisions have been adapted to cover digital content, privacy and security, consumer reviews and ratings, new payment mechanisms, and use of mobile devices to conclude transactions. In addition, the Recommendation updated a number of provisions, including the ones related to the essential role of consumer protection authorities. It highlights the need to enhance their authorities to protect consumers online, and exchange information and cooperate in cross-border matters (OECD, 2016d).

191. The particular issues to be covered here include policy initiatives to protect consumers in peer platform markets, to address consumer protection related impediments to cross-border e-commerce and to detect and deter the sale of unsafe products online.

*Policymakers are beginning to grapple with the challenge of applying consumer protection frameworks to peer platform markets*

192. Peer platform markets have steered debates in many OECD countries over how to regulate their economic activity. In this area, regulators must balance competing considerations: appropriate regulatory measures can protect consumers but unnecessary or excessive regulation can impact the disruptive innovation associated with these platforms, thus reducing benefits for consumers. When access to a peer platform is a service in itself, the OECD E-commerce Recommendation highlights that consumer laws should apply. Less obvious is whether and how responsibilities can be imposed on platforms for the actions of the peer users (OECD, 2016e). In June 2016, the EC issued its "European agenda for the collaborative economy", which is part of the Single Market Strategy. It provides non-building guidance on how existing EU law should apply to the collaborative economy including peer-to-peer markets, and clarifies key issues facing market operators and public authorities, such as consumer protection, market access requirements, liability if problem arises, labour law and tax (EC, 2016d).

193. A number of countries have recently looked into issues related to the development of peer platform markets, along with appropriate policy responses, by conducting studies or organising events. In 2015, the US FTC held a public workshop entitled *The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators*" to examine competition, consumer protection, and economic issues arising from peer platform markets activity. A staff report drawing on the Workshop's discussions and more than 2,000 public comments examines regulatory approaches to protect consumers and the public. One observation by participants was that regulatory issues in these platforms may diverge from those posed by traditional suppliers. Moreover, peer platforms are innovating at a rapid pace, which will likely require adjusting regulation as these platforms develop, thus requiring flexibility in regulatory approaches and avoidance of pre-emptive regulation (FTC, 2016).

194. In 2015, the Competition Bureau of Canada undertook a comprehensive study of the taxi industry in light of the rapid expansion and proliferation of ride sharing services such as Uber. The aim of the study was to explore how existing regulations for taxi and limousine services could be adapted to govern ride-sharing services. The Bureau concluded regulators should both ensure that new regulations on ride-sharing

services were no broader than necessary to achieve policy goals, while also relaxing existing regulations on traditional taxis, with the aim of creating a level playing field. That way, consumers can benefit from lower prices, reduced waiting times, and higher quality service. Ultimately, competition can ensure that consumers have the broadest range of products and services at the best possible prices (Competition Bureau of Canada, 2015).

195. Self-regulation initiatives such as codes of conduct, accountability measures and enforcement mechanisms, interface with other policy initiatives and existing consumer laws. Sharing Economy UK in partnership with Oxford University and SAID business school recently developed the TrustSeal, the first trust mark for the sharing economy. It sets out minimum standards for businesses to ensure certain standards of business conduct. Trust mechanisms such as reviews and endorsements have sometimes be associated with a form of self-regulation although it is difficult to assess the effectiveness of such mechanisms as a vehicle for consumer protection.

*Steps are being taken to address the consumer protection-related impediments to cross-border e-commerce, but more is needed to realise the untapped potential*

196. The issue of cross-border barriers to e-commerce growth has been discussed in Chapter 5. These barriers are affecting consumer trust in e-commerce as consumers may find difficult to understand which rules apply to their transactions and what rights and responsibilities apply in case of problems. The 2016 OECD E-commerce Recommendation encourages countries to improve the ability of their consumer protection enforcement authorities to co-operate and co-ordinate with each other with a view to provide for effective consumer protection in the context of global e-commerce. One example at national level is the U.S. SAFE WEB Act, passed in 2006 and reauthorized in 2012, which gives the FTC enhanced abilities to combat cross-border fraud, including through enhanced information sharing and investigative assistance powers that allow the FTC to cooperate with foreign counterparts. At international level, the International Consumer Protection and Enforcement Network's Econsumer.gov website, last updated in October 2015, serves that purpose by helping law enforcement authorities gather and share cross-border consumer complaints that can be used to investigate and take action against international scams.

197. Within the context of its Digital Single Market Strategy, the EC is looking into different measures to reduce barriers to cross-border e-commerce, notably by removing key differences between domestic and global e-commerce marketplaces. In May 2016, the EC put forward a proposal for the reform of the Consumer Protection Cooperation, with the aim of equipping EU enforcement authorities with the powers they need to better cooperate, and a proposal for a regulation on geo-blocking, a form of discrimination based on the place of residence. To improve and facilitate dispute resolution in cross-border online disputes, the EU adopted in 2013 its Directive on Consumer Alternative Dispute Resolution (ADR) and its Regulation on Online Dispute Resolution (ODR), which was followed in 2016 by an ODR platform. This platform, available in 23 languages, assists consumers in finding access to bodies that offer online dispute resolution.

198. Some countries have engaged into bilateral agreements that facilitate cross-border cooperation on e-commerce issues. For instance, the Korea Consumer Agency has signed MOUs with the National Consumer Affairs Center of Japan (NCAC), the Better Business Bureau (BBB), and the Office of the Consumer Protection Board (OCPB) of Thailand which sets out procedures for cross-border dispute resolution.

*The complexities of global e-commerce supply chains highlight the need for greater co-operation to detect and deter the sale of unsafe products to consumers*

199. The 2016 OECD E-commerce Recommendation recognises that consumer product safety issues have become more challenging as global e-commerce supply chains become more complex. It calls for online businesses to not offer, advertise or market unsafe goods or services. It also encourages businesses to co-operate with the competent authorities when a good or a service on offer is identified as presenting a risk to the health or safety of consumers (OECD, 2016d).

200. In recent years, a number of market surveillance activities and enforcement actions have been undertaken by consumer product safety authorities in order to detect and deter unsafe products made available through e-commerce. This includes having in place organisations dedicated to e-commerce market surveillance, such as the "Control of e-commerce of Food, Feed, Cosmetics, Commodities and Tobacco" in Germany or the Centre de Surveillance du Commerce Electronic in France, and developing specific guidelines and strategies on market surveillance (OECD, 2016f). The 2016 National Market Surveillance Programme in Turkey includes market surveillance activities and procedures for detecting unsafe products (Turkish Government, 2016).

201. Co-operation between market surveillance and custom authorities as well as international co-operation between authorities is essential considering the important cross-border element of product safety issues. In the EU, the RAPEX-China system enables information sharing on unsafe products between the EC and Chinese authorities. The Cooperative Engagement Framework between Canada, the United States and Mexico provides a framework for sustained and increased cooperation on consumer product safety in North America. Online sweeps, such as the OECD online product safety sweep conducted in 2015 in 25 jurisdictions, are also seen as an effective way of enhancing international cooperation (OECD, 2016f).

## NOTES

[1] https://www.viestintavirasto.fi/en/spectrum/radiospectrumuse/spectrumauction.html

[2] Examples of such light regulation include requiring companies that are providing services to notify the regulator and imposing minimum content standards (i.e. protection of minors, illegal content and advertising rules)

[3] These are the Framework Directive (2002/21/EC), the Authorisation Directive (2002/20/EC), the Access Directive (2002/19/EC), the Universal Service Directive (2002/22/EC) and the Directive on privacy and electronic communications (2002/58/EC).

[4] Not amended, therefore still not encompassing platforms without editorial responsibility.

[5.] For a full list of notified on demand services in the UK:- http://stakeholders.ofcom.org.uk/binaries/broadcast/on-demand/List_of_Regulated_Video_On_Demand_Services.pdf.

[6.] For the directory of regulated VoD in Hungary see: http://mediatanacs.hu/dokumentum/163976/lekerheto_audiovizualis_mediaszolgaltatasok.pdf.

[7] http://interfone.com

[8] http://dfat.gov.au/trade/agreements/safta/pages/singapore-australia-fta.aspx#news

[9] Austria, Belgium, Brazil, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, Norway, People's Republic of China, Poland, Portugal, Russian Federation, Singapore, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom.

[10] Note that this portion of the questionnaire covers innovation policies only for the ICT sector. A much wider review of innovation policies is available in OECD (2016g).

[11] To find out more about Austria's ICT of the Future program, see here: https://www.ffg.at/en/ictofthefuture/

[12] Further information on Estonia's Venture Capital Fund can be found at http://www.kredex.ee/en/venture-capital-4/ .

[13] See http://www.hutzero.co.uk/ for further details.

[14] For more information, please see http://www.gouvernement.lu/5380127/27-fit4start?context=3422869 (in French only).

15 See http://ufm.dk/en/research-and-innovation/cooperation-between-research-and-innovation/commercialisation-and-entrepreneurship/the-innovation-incubator-scheme/the-innovation-incubator-scheme#cookieoptin for more information.

16 More of Israel's schemes directed towards promoting innovative start-ups can be found at http://innovation-israel-en.mag.calltext.co.il/?article=4 .

17 Australia, Austria, Belgium, Brazil, Canada, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, Norway, People's Republic of China, Poland, Portugal, Russian Federation, Singapore, Slovenia, Spain, Sweden, Switzerland, Turkey.

18 Australia, Austria, Belgium, Brazil, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, Norway, People's Republic of China, Poland, Portugal, Russian Federation, Singapore, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom.

19 Estimates are based on the voluntary, ad hoc module in the EU Community Innovation Survey 2010 on the skills available in enterprises and on methods to stimulate new ideas and creativity. The indicator corresponds to the percentage of firms in the relevant innovation category responding affirmatively to the question: "During the three years 2008 to 2010, did your enterprise employ individuals in-house with the following skills, or obtain these skills from external sources?" Innovative enterprises had innovation activities during 2008-10, relating to the introduction of new products, processes, and organisational or marketing methods. This includes enterprises with ongoing and abandoned activities for product and process innovation. The question on innovation-relevant skills also applies to non-innovative enterprises. Estimates are based on firms with "core" NACE Rev. 2 economic activities (B, C, D, E, G46, H, J58, J61, J62, J63, K and M71).

20 Austria, Belgium, Brazil, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Israel, Japan, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, Norway, People's Republic of China, Poland, Portugal, Russian Federation, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom.

21 One area where there are plenty of policies targeting young firms, though, is ICT sector development, as mentioned in section 6.1. Among 34 respondents, 24 countries had policies aimed at both start-ups and SMEs, while 16 had policies specifically aimed at start-ups alone.

22 Again, other OECD work, however, shows that 29 of the 35 OECD countries have an R&D tax credit (OECD and European Commission, 2017, p. 4)

23 For more information on these funds, see www.eif.org/what_we_do/resources/erp/index.htm?lang=-en, http://www.eif.org/what_we_do/equity/eaf/Germany.htm, www.eif.org/what_we_do/equity/news/2016/eif-bmwi-new-instrument-venture-capital-germany.htm, http://coparion.de/en, and http://high-tech-gruenderfonds.de/en/#title.

24 For more information, see www.bankofengland.co.uk/publications/Pages/speeches/2016/914.aspx and https://services.parliament.uk/bills/2016-17/digitaleconomy.html.

25 This may not be an altogether representative data set, however, because disruptors such as Uber and Tesla, Inc. have faced many regulations – though not always new ones – that were designed to protect incumbents (OECD, 2015a).

[26] For more information on this initiative, see https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%201%20-%20Introducing%20the%20Open%20Banking%20Standard%202016.pdf.

[27] An overview may be found here: https://telemedizinportal.gematik.de/.

[28] An English language version of the paper is available at: www.bmas.de/EN/Services/Publications/arbeiten-4-0-greenpaper-work-4-0.html.

[29] Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, Denmark, Finland, France, Iceland, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

[30] Article 14 and 15 of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[31] https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

[32] http://ehoganlovells.com/cv/53b6c1e3cb33dedddd11ffd68c0022e08d10c4e4

[33] https://www.first.org/about

[34] Australia, Austria, Belgium, Brazil, Canada, Chile, Colombia, Costa Rica, Denmark, Estonia, Finland, France, Hungary, Iceland, Israel, Italy, Japan, Korea, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Russian Federation, Singapore, Slovak Republic, Slovenia, Spain, Switzerland, Turkey, United Kingdom, United States

[35] Canadian businesses, for example, are required to comply with privacy laws at both the Federal and provincial/territorial level.

[36] The official title is: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Hyperlink: http://eur-lex.europa.eu/eli/reg/2016/679/oj.

[37] Article 20 of the EU's (2016) General Data Protection Regulation on the right of data portability states: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance (…)".

[38] The official title is: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Hyperlink: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

[39] The privacy management plan template developed by the Office of the Australian Information Commissioner (OAIC) is dedicated to public sector agencies.

[40] See e.g. https://privacy.org.nz/your-rights/complaint-form/ in the case of New Zealand

[41] In 2015, Korea allowed individuals to provide claims for damages: up to 3 times of the amount of the punitive damage and up to 3 million KRW in the case of statutory damages.

[42] See http://194.242.234.211/documents/10160/2416443/Privacy%3A+working+with+business-vademecum.pdf

[43] It is estimated that the Privacy Shield underpins over USD 290 billion in digitally-deliverable services trade across the Atlantic each year.

## ANNEX 1: SELECTED COMMUNICATION MERGERS CIRCA USD 500 MILLION OR ABOVE BETWEEN 2014-2016

| Country | Transaction |
|---|---|
| Australia | Between 2014 and 2016, TPG Telecom and Vocus Communications both acquired multiple networks to become the second and fourth largest ISPs by subscriptions. |
| Belgium | In 2016, Telenet, Liberty Global Belgian's subsidiary, merged with the MNO Base. |
| Canada | In 2016, Shaw Communications, a cable operator, acquired the MNO Wind. In 2015, an incumbent MNO, Rogers, acquired a new MNO entrant, Mobilicity. In 2014, Bell Canada's acquired the related entity Bell Aliant. |
| Denmark | In 2016, Syd Energi and Nyfors merged – both provide fibre infrastructures. |
| Germany | In 2014, the two MNO's Teléfonica and E-Plus merged. Mergers between cable companies included Tele Columbus and Primacom in 2015, United Internet and Versatel in 2014 as well as the MNO Vodafone with Kabel Deutschland also in 2014. |
| Greece | In 2014, Vodafone, Greece, acquisition of HOL, a major, alternative fixed network operator. |
| Ireland | The two MNOs, H3GI and Telefonica (O2), merged in 2014. |
| Italy | The two MNO's '3 Italia' and Wind Telecomunicazioni (VimpelCom) merged in 2016. |
| Netherlands | In 2014 there was a merger between two cable network operaors – Liberty Global's UPC – Ziggo. In 2016, Vodafone and Ziggo subsequently merged. |
| Portugal | In 2014, ZON TV Cabo Portugal, was acquired by NOS Comunicações. In the same year MEO - Serviços de Comunicações e Multimédia, was acquired by PT Comunicações. PT Comunicações, then changed its name to MEO - Serviços de Comunicações e Multimédia. Cabovisão and ONITELECOM were acquired by Grupo APAX in 2015: In June 2015, Altice completed acquisition of 100 percent of the share capital of PT Portugal, SGPS, owners of MEO - Serviços de Comunicações e Multimédia; consequently, the European Commission required Altice to divest from ONI and Cabovisão. In January 2016, Altice announced the completion of the sale of ONI and Cabovisão to the Apax France investment fund. |
| Spain | The MNO Vodafone and ONO, a cable operator, merged in 2014, as did the MNO Orange with the fixed network Jazztel in 2015. Additionally, in 2015 Telefónica acquired DTS, (the main satellite pay-TV operator in Spain). |
| United Kingdom | BT, a fixed network provider, acquired Everything Everywhere (EE) an MNO. |
| United States | In 2016, Charter/Time Warner Cable/Bright House was a merger of three cable providers and in the same year Altice and Cablevision a merger of United States and international cable provider. In 2015, Altice had merged with Suddenlink, a cable provider. In the same year, the FCC approved the sale of wireline assets in California, Florida and Texas to Frontier. In 2015, the FCC also approved the acquisition of DirectTV, a satellite provider, by AT&T. In 2014, two fixed providers, Level 3 and twtelecom merged. In the same year, Frontier purchased AT&T's fixed line subsidiary in Connecticut. |

## ANNEX 2: CONVERGED REGULATORS

| Country | Converged NRA | Telecommunications | Broadcasting carriage regulation | Broadcasting spectrum allocation | Broadcasting content regulation |
|---|---|---|---|---|---|
| **Australia** | Yes | Australian Communications and Media Authority(ACMA) | ACMA | ACMA | ACMA |
| **Austria** | No | Telekom-Kontrol-Kommission (TKK), supported by RTR-GmbH | KommAustria (supported by RTR-GmbH) | KommAustria (supported by RTR-GmbH) | KommAustria (supported by RTR-GmbH) |
| **Belgium** | No | Belgian Institute for Postal Services and Telecommunications (BIPT) | *Vlaams Commissariaat voor de Media (VCM); Conseil supérieur de l'audiovisuel (CSA)*; Government of the German Community | BIPT; VCM; CSA; Government of the German Community | VCM; CSA; Government of the German Community |
| **Canada** | Yes | Canadian Radio-television and Telecomunications Commission (CRTC) | CRTC | Innovation, Science, and Sconomic Development Canada | CRTC |
| **Chile** | No | Subsecretaría de Telecomunicationes (Subtel) | Subtel | Subtel | Consejo Nacional de Televisón (CNTV) |
| **Colombia** | No | Comisión de Regulación de Comunicaciones (CRC) | Autoridad National Television Comission (ANTV) | ANTV; Agencia Nacional del Espectro (ANE) | ANTV |
| **Czech Republic** | No | Czech Telecommunications Office (CTU) | CTU | CTU; Council for Radio and Tele-vision Broadcasting | The Council for Radio and Television Broadcasting |
| **Denmark** | No | Danish Business Authority (DBA) | Danish Energy Agency (DAE) | Danish Energy Agency (DEA) | Ministry of Culture and the Radio and Television Board |
| **Estonia** | Yes | Estonia Technical Regulatory Authority (ETRA) | ETRA | ETRA | ETRA; Estonian Broadcasting Council (RHN |
| **Finland** | Yes | Finnish Communications Regulatory Authority (FICORA) | FICORA; Ministry of Transport and Communications. | FICORA | FICORA; Ministry of Transport and Communications. |
| **France** | No | ARCEP | Conseil supérieur de l'audiovisuel (CSA) | CSA | CSA and Direction Générale des Médias et des Industries culturelles (DGMIC) |
| **Germany** | No | BNA (Bundesnetzagentur) | BundesNetzAgentur, Association of Regulatory Authorities for Broadcasting (ALM), Commission on Concentration in | BNA (Bundesnetzagentur) | Authorities for Broadcasting (ALM) |

| | | | | | |
|---|---|---|---|---|---|
| | | | the Media (KEK) | | |
| **Greece** | No | Hellenic Telecommunications and Post Commission (EETT) | Ministry of Press and Mass Media; NCRTV | (EETT) | NCRTV |
| **Hungary** | Yes | National Media and Infocommunications Authority (NMHH) | NMHH | NMHH | NMHH |
| **Iceland** | No | Post and Telecom Administration (PTA) | PTA; Media Commission (Fjölmiðlanefnd) | Post and Telecom Administration (PTA) | Media Commission (Fjölmiðlanefnd) |
| **Ireland** | No | Commission for Communications Regulation (ComReg) | Commission for Communications Regulation (ComReg), Broadcasting Authority of Ireland (BAI) | Commission for Communications Regulation (ComReg) | Broadcasting Authority of Ireland (BAI) |
| **Israel** | No | Ministry of Communications (MOC) | Ministry of Communications (MOC) | Ministry of Communications (MOC) | Ministry of Communications (MOC) and the Second Authority for Television and Radio |
| **Italy** | Yes | Autoritá per le Garanzie nelle Comunicazionei (AGCOM) | AGCOM | Ministry of Economic Development (MISE) | AGCOM |
| **Japan** | No | Ministry of Internal Affairs and Communications (MIC) | MIC | MIC | MIC |
| **Korea** | Yes | Korea Communications Commission (KCC) | KCC | MIC | KCC |
| **Latvia** | No | Public Utilities Commission (PUC) | National Electronic Mass Media Council (NEPLP) | Electronic Communication Office(ESD) | NEPLP |
| **Luxembourg** | No | Institut luxembourgeois de régulation (ILR) | Autorité luxembourgeoise indépendante de l'audiovisuel (ALIA) | ILR | ALIA |
| **Mexico** | Yes | Instituto Federal de Telecomunicaciones (IFT) | IFT | IFT | IFT |
| **Netherlands** | No | Autoriteit Consument & Markt (ACM) | Dutch Media Authority (CvdM) | ACM | CvdM |
| **New Zealand** | No | Commerce Commission of New Zealand (ComCom) | Ministry of Economic Development | Ministry of Economic Development | NZ On Air; Broadcasting Standards Authority (BSA) |
| **Norway** | No | Norwegian Communications Authority (Nkom) | Ministry of Culture and Church Affairs; Norwegian Media Authority; Norwegian Communications Authority (Nkom) | Norwegian Communications Authority (Nkom) | Norwegian Media Authority |
| **Poland** | No | Prezes Urzędu Komunikacji Elektronicznej (UKE) | National Broadcasting Council (KRRiT) | UKE; KRRiT | KRRiT |
| **Portugal** | No | Autoridade Nacional de Comunicações (ANACOM) | Entidade Reguladora para a Comunicação Social (ERC) | ANACOM | ERC; Instituto da Comunicação Social (ICS) |
| **Slovak Republic** | No | Telecommunications Regulatory Authority of the Slovak Republic (TUSR) | Council for Broadcasting and Retransmission (RVR) | TUSR; Council for Broadcasting and Retransmission (RVR) | RVR |
| **Slovenia** | Yes | Agency for Communications Networks and Services of the Republic of Slovenia (AKOS) | AKOS | AKOS | AKOS |
| **Spain** | Yes | Comisión Nacional de Mercados y de | CNMC | Ministry of Industry, Energy and | CNMC and regional audiovisual |

| | | | | | |
|---|---|---|---|---|---|
| | | la Competencia (CNMC) | | Tourism (MINETUR) | authorities |
| **Sweden** | No | Swedish Post and Telecom Authority (PTS) | Swedish Broadcasting Authority | PTS | Swedish Broadcasting Authority |
| **Switzerland** | Yes | Federal Communications Commission (ComCom); Office fédéral de la communication (OFCOM); | Federal Council; Federal Department of Environment, Transport, Energy and Communications (DETEC); OFCOM | OFCOM | DETEC ; OFCOM; L'Autorité indépendante d'examen des plaintes en matière de radio-télévision (AIEP) |
| **Turkey** | No | Information And Communication Technologies Authority (ICTA) | Radio and Television Supreme Council (RTUK) | Tele-communications Authority; RTUK | RTUK |
| **United Kingdom** | Yes | Office of Communications (OFCOM) | Ofcom; Department for Culture, Media and Sport | Ofcom | Ofcom |
| **United States** | Yes | Federal Communications Commission (FCC) | FCC; Local government for cable television franchises | FCC | FCC; Federal Trade Commission (FTC); Department of Justice (DoJ) |

## ANNEX 3: ROAM LIKE AT HOME OFFERS

| Home Country | Roaming in: | Operators | Note |
|---|---|---|---|
| **Austria** | EEA countries, Switzerland | A1 | For Switzerland, up to 300MB/month |
| **Belgium** | EU countries and Norway | Proximus | Up to 240MB/month |
| | EU countries, China, Egypt, Switzerland, Turkey, USA | Orange | Up to 1GB/year |
| | EEA countries | BASE | Up to 600MB/month |
| **Canada** | United States | WIND Mobile | Up to 1GB/month |
| | United States | Videotron | Up to 5GB/month for up to 90 days/yr |
| **Colombia** | Canada and United States | Uff!Mobile | Up to 2GB/month |
| **Czech Republic** | EU countries | T-Mobile | Up to 300MB/month |
| | EU countries, Norway, Switzerland | O2 | Up to 300MB/month |
| | EEA countries, Switzerland | Vodafone | Up to 100MB/day |
| **Denmark** | EEA countries, Switzerland | TDC | Up to 30days/year, 2GB/month |
| | EEA countries, Switzerland | Telenor | Up to 30days/year, 10GB/month |
| | EEA countries, Switzerland | Telia | Up to 30days/year, 10GB/month |
| | EEA countries, Hong Kong, Switzerland, Singapore, USA | Hi 3G | Up to 30days/year, 10GB/month (excluding Sweden) |
| **Estonia** | EEA countries, Switzerland | Telia | Up to 300MB/month |
| **Finland** | EU countries | Sonera | Up to 600MB/month (excluding Sweden, Norway, Denmark, Estonia, Latvia and Lithuania) |
| | EU countries | Elisa | Up to 500MB/month |
| **France** | EEA countries, Switzerland, Canada, USA | Orange | |
| | EEA countries, USA | SFR | |
| | EEA countries, Australia, Canada, Israel, USA | Iliad Free | Up to 35days/year |
| | EEA countries and Switzerland | Bouygues | Up to 35days/year |
| **Germany** | EEA countries, Australia, Canada, New Zealand, Switzerland, USA | T-Mobile | |
| | EEA countries | O2 | Up to 1GB/month |
| | EU countries | Vodafone | |
| **Greece** | EEA countries | Cosmote | |
| | EU countries | Vodafone | |
| | EU countries | Wind | Up to 500MB/month |
| **Hungary** | EU countries | Telenor | |
| | EU countries | Vodafone | |
| **Ireland** | 32 European destinations | Vodafone | |
| | EEA countries | Meteor | |
| **Israel** | 23 Countries | Golan Telecom | 49NIS(13USD) one time handling fee required |
| **Italy** | EEA countries, Switzerland, USA | TIM | Up to 28days/year |
| | EEA countries, Albania, Switzerland, Turkey, USA | Vodafone | Up to 100MB/day |
| **Japan** | United States | Softbank | Users need an iPhone 6 or newer/ iPad Air2 or newer |
| **Latvia** | Estonia, Lithuania | Tele2 | |
| | EEA countries | Bite | |
| **Lithuania** | Denmark, Estonia, Finland, Latvia, Norway, Sweden | Omnitel | |
| | EEA countries | Bite | |
| **Luxembourg** | EU countries | Join | |
| | EEA countries, Switzerland | POST | Up to 1GB/month |
| | EEA countries, Switzerland | Tango | Up to 20GB/year |
| | EEA countries | Orange | Up to 2GB/month |
| **Mexico** | Canada and United States | AT&T Mexico | Limited to internet access using Facebook/messenger, Twitter and |

| | | | |
|---|---|---|---|
| | | | Whatsapp. |
| **Netherland** | EU countries | KPN | Up to 60days/year |
| | EEA countries, Australia, Japan, New Zealand, Turkey, Switzerland | Vodafone | |
| | EEA countries, Switzerland | T-Mobile | |
| **Norway** | EEA countries | Telenor | |
| | EEA countries | Telia | 45days/90days |
| **Poland** | EU countries | Orange | Up to 100MB/month |
| | EU countries | Play | Up to 500MB/month |
| | EEA countries | Plus | |
| | Albania, Austria, Croatia, Montenegro, Czech Republic, Greece, the Netherlands, Macedonia, Germany, Romania, Slovakia, Hungary | T-Mobile | Up to 1GB/month |
| **Portugal** | EEA countries, USA | MEO | Up to 200MB in 15days/year |
| | EU countries | Vodafone | |
| | EU countries | NOS | Up to 100MB/month, 15days/year |
| **Slovak Republic** | EU countries | Telekom | Up to 500MB/month |
| | EU countries | O2 | |
| **Slovenia** | EEA countries, Former Yugoslav Republic of Macedonia, Serbia | | |
| **Spain** | EU countries, United States | Vodafone | |
| | EEA countries | Orange | Up to 100MB/month |
| **Sweden** | Nordic and Baltic countries | Telia | |
| | EEA countries | Telenor | Up to 1Mbps outside Scandinavia. |
| | Denmark | Hi 3G | |
| **Switzerland** | European Union and Western Europe/ Rest of the world (with some exceptions) | Swisscom | Up to 24GB/year in EU/WE countries, up to 1GB/year in the rest. |
| | EEA countries, Canada, United States | Sunrise | Up to 2GB/month |
| | EU countries/ Rest of the world (more than 170 countries) | Salt | Up to 1GB/month in EU countries, and another 1GB/month in the rest. |
| **United Kingdom** | EEA countries | EE | Up to 500MB/month |
| | EEA countries | O2 | |
| | EEA countries, Albania, Bosnia, Switzerland, Turkey | Vodafone | Up to 4GB/month |
| | EEA countries, Australia, Hong Kong, Indonesia, Israel, Macau, New Zealand, Sri Lanka, Switzerland, USA | 3G-UK | |
| **United States** | Mexico | AT&T | |
| | Argentina, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay, Venezuela | Sprint | Up to 1GB |
| | Over 140 countries | T-Mobile (US) | For Mexico and Canada, unlimited data usage without speed cap. For the rest of the world, speed capped at 128Kbps. |

## REFERENCES

ACM (2015), *IP interconnection in the Netherlands: a regulatory assessment*, Authority for Consumers and Markets, The Hague, www.acm.nl/nl/publicaties/publicatie/14769/Onderzoek-IP-interconnectie-in-Nederland/, accessed on 9 May 2017.

Adalet McGowan, M. and D. Andrews (2015), "Skill Mismatch and Public Policy in OECD Countries", OECD Economics Department Working Papers, No. 1210, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5js1pzw9lnwk-en.

Appelt, S., et al. (2016), "R&D Tax Incentives: Evidence on design, incidence and impacts", *OECD Science, Technology and Industry Policy Papers*, No. 32, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5jlr8fldqk7j-en.

BEREC (2015), "Draft Report on OTT Services", *BoR*, Vol. 15, No. 142, Body of European Regulators for Electronic Communications, Riga, Latvia, http://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/5431-draft-berec-report-on-ott-services, accessed on 9 May 2017.

CNMC (2015), "Caracterización del Uso de Algunos Servicios Over the Top en España (Comunicaciones Electrónicas y Servicios Audiovisuales)", *Documento de Trabajo*, No. 4, Comisión Nacional de los Mercados y la Competencia, Barcelona, https://www.cnmc.es/Portals/0/Ficheros/Telecomunicaciones/Informes/20150130_DOC_OTT_21_11_CC_REVISADO.pdf

CRTC (2016), "Examination of differential pricing practices related to Internet data plans", *Telecom Notice of Consultation*, CRTC 2016-192, Canadian Radio-television and Telecommunications Commission, Ottawa, www.crtc.gc.ca/eng/archive/2016/2016-192.htm, accessed on 9 May 2017.

Competition Bureau of Canada (2015), "Modernizing Regulation in the Canadian Taxi Industry", 26 November 2015, www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04007.html, accessed on 9 May 2017.

Danish Agency for Culture (2015), *Media Development in Denmark 2015*, Copenhagen, http://english.slks.dk/publications/media-development-in-denmark-2015/, accessed on 9 May 2017.

DeStefano, Timothy, Koen de Backer and Laurent Moussiegt (2017) "Determinants of Digital Technology Use by Companies," *OECD Science, Technology and Industry Policy Papers*

EC (2015), *A Digital Single Market Strategy for Europe*, COM(2015)192 (final), European Commission, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192, accessed on 9 May 2017.

EC (2016a), *Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU [Audiovisual Media Services Directive (AVMSD)]*, COM(2016)287 (final), European

Commission, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN, accessed on 9 May 2017.

EC (2016b), "Roaming implementing regulation", Act, 15 December, European Commission, Brussels, https://ec.europa.eu/digital-single-market/en/news/roaming-implementing-regulation, accessed on 9 May 2017.

EC (2016c), "Roaming", 15 December, European Commission, Brussels, https://ec.europa.eu/digital-single-market/en/roaming, accessed on 9 May 2017.

EC (2016d), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Comprehensive Approach to Stimulating Cross-Border E-Commerce for Europe's Citizen and Businesses*, Brussels, May 2016, COM(2016 320 final, www.cdep.ro/afaceri_europene/CE/2016/COM_2016_320_EN_ACTE_f.pdf

EC (2017), "European legislation on reuse of public sector information", European Commission, Brussels, https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information, accessed on 4 April 2017.

European Parliament and European Council (2014), "Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on Measures to Reduce the Cost of Deploying High-Speed Electronic Communications Networks", *Official Journal of the European Union*, 23.5.2014, Brussels, http://eur-lex.europa.eu/eli/dir/2014/61/oj, accessed on 9 May 2017.

European Parliament and European Council (2015), "Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 on Laying Down Measures Concerning Open Internet Access and Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services and Regulation (EU) No 521/2012 on Roaming on Public Mobile Communication Networks Within the Union", *Official Journal of the European Union*, 26.11.2015, Brussels.

FCC (2016), "FCC Invites Public Comment on Updating Definition of Multichannel Video Programming Distributor", Federal Communications Commission, 9 November, Washington DC, www.fcc.gov/fcc-invites-public-comment-updating-definition-multichannel-video-programming-distributor, accessed on 9 May 2017.

Federal Trade Commission (FTC) (2016), *The "Sharing"Economy, Issues Facing Platforms, Participants & Regulators,* An FTC Staff Report, November 2016, www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf.

Gaggle, P. and G. Wright (2014), "A Short-Run View of What Computers Do: Evidence from a UK Tax Incentive", Discussion Paper Series No. 752, July, University of Essex, Colchester, UK.

Grazzi, M. and J. Jung (2016), "ICT, Innovation and Productivity: Evidence from Latin American Firms", in: Grazzi, Matteo and C. Pietrobelli, Firms' Innovation and Productivity in Latin America and the Caribbean: The Engine of Economic Development, Palgrave, New York.

Haller, S. and I. Siedschlag (2011), "Determinants of ICT Adoption: Evidence from Firm-Level Data", Applied Economics, Vol. 43, No. 26, pp. 3775-3788.

Hathaway, I. (2016), "What start-up accelerators really do", 1 March 2016, Harvard Business Review, https://hbr.org/2016/03/what-startup-accelerators-really-do, accessed on 15 March 2016.

Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) (2016), Government of Japan, http://japan.kantei.go.jp/policy/it/index_e.html, accessed on 9 May 2017.

MBIE (2015), Business Growth Agenda, Ministry of Business, Innovation and Employment, Wellington, New Zealand, www.mbie.govt.nz/info-services/business/business-growth-agenda, accessed on 9 May 2017.

MBIE and MCH (2015), *Exploring Digital Convergence*, Ministry of Business, Innovation and Employment and Ministry for Culture and Heritage, Wellington, New Zealand, http://convergencediscussion.nz/, accessed on 9 May 2017.

OECD (2012a), "ICT Skills and Employment: New Competences and Jobs for a Greener and Smarter Economy", *OECD Digital Economy Papers*, No. 198, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k994f3prlr5-en.

OECD (2012b), "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 (2014a), "International Traffic Termination", *OECD Digital Economy Papers*, No. 238, OECD Publishing, DOI: http://dx.doi.org/10.1787/5jz2m5mnlvkc-en.

OECD (2014b), "Young SMEs, Growth and Job Creation," Policy Brief, www.oecd.org/sti/young-SME-growth-and-job-creation.pdf.

OECD (2014c), "Non-regular employment, job security and assessing job quality", Chapter 4 of the OECD Employment Outlook 2014, OECD Publishing, Paris. DOI: http://dx.doi.org/10.187/empl_outlook-2014-en.

OECD (2015a), "Disruptive Innovation," DAF/COMP(2015)3, www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP(2015)3&docLanguage=En, accessed on 9 May 2017.

OECD (2015b), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264232440-en

OECD (2015c), "Non-standard work, job polarisation and inequality", Chapter 4 of *In It Together: Why Less Inequality Benefits All*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264235120-en.

OECD (2016a), "Developments in International Mobile Roaming", *OECD Digital Economy Papers*, No. 249, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jm0lsq78vmx-en.

OECD (2016b), Stimulating Digital Innovation for Growth and Inclusiveness: The Role of Policies for the Successful Diffusion of ICT, *OECD Digital Economy Papers*, No. 256, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwqvhg3l31-en.

OECD (2016c), Enabling the Next Production Revolution (NPR), Chapter 2: Digital Technologies and Future Production, DSTI/CDEP(2016)13/REV1.

OECD (2016d), "Be flexible! Background brief on how workplace flexibility can help European employees to balance work and family", www.oecd.org/els/family/Be-Flexible-Backgrounder-Workplace-Flexibility.pdf.

Ofcom (2016), *Making communications work for everyone: initial conclusions from the Strategic Review of Digital Communications*, Office of Communications, London, https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/digital-comms-review/conclusions-strategic-review-digital-Communications, accessed on 9 May 2017.

OECD (2016d), Recommendation of the Council on Protecting Consumers in E-commerce, http://webnet.oecd.org/oecdacts/, accessed on 9 May 2017.

OECD (2016e), "Protecting Consumers In Peer Platform Markets: Exploring The Issues", *OECD Digital Economy Papers*, No. 253, DOI: http://dx.doi.org/10.1787/5jlwvz39m1zw-en.

OECD (2016f), "Online Product Safety: Trends and Challenges", *OECD Digital Economy Papers*, No. 261, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5jlnb5q93jlt-en.

OECD (2016g), *OECD Science, Technology and Innovation Outlook 2016*, OECD Publishing, Paris. http://dx.doi.org/10.1787/sti_in_outlook-2016-en.

OECD and European Commission (2017), *OECD Review of National R&D Tax Incentives and Estimates of R&D Tax Subsidy Rates, 2016*, TAX4INNO Project 674888 (13 February). www.oecd.org/sti/RDTaxIncentives-DesignSubsidyRates.pdf.

Tambe, P. (2014), "Big data investment, skills, and firm value", *Management Science*, volume 60, issue 6.

Turkish Government (2016), *National Market Surveillance Programme for 2016*, available at: http://ec.europa.eu/DocsRoom/documents/15742?locale=fr, accessed on 9 May 2017.

WEF (2015), "Industrial Internet of Things: Unleashing the Potential of connected Products and Services", WEF Industry Agenda, January 2015, www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

WTO (1998), "Work programme on electronic commerce", WT/L/274, World Trade Organization, Geneva, https://docsonline.wto.org/dol2fe/Pages/FormerScriptedSearch/directdoc.aspx?DDFDocuments/t/WT/L/274.DOC, accessed 16 March 2017.