KEY ISSUES FOR DIGITAL TRANSFORMATION IN THE G20

Report prepared for a joint G20 German Presidency/ OECD conference

BERLIN, GERMANY
12 JANUARY 2017

OECD
BETTER POLICIES FOR BETTER LIVES

This report is issued under the responsibility of the Secretary-General of the OECD. This report was prepared by the Secretariat at the request of the G20 German Presidency for the joint G20 Presidency – OECD conference on Key Issues for Digital Transformation in the G20, in Berlin, Germany, on 12 January 2017. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD Member countries or of the G20.

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

ACKNOWLEDGEMENTS

Key Issues for Digital Transformation in the G20 was prepared by the OECD Directorate for Science, Technology and Innovation, headed by Director Andrew Wyckoff and Deputy Director Dirk Pilat. The work was co-ordinated by Molly Lesher of the OECD Digital Economy Policy Division, headed by Anne Carblanc. The leadership and oversight of Gabriela Ramos, OECD Sherpa, and the OECD Sherpa Office, is gratefully acknowledged.

Authors and contributors from the OECD Secretariat include, in alphabetical order: Laurent Bernat, Frédéric Bourassa, Josie Brocca, Flavio Calvino, Chiara Criscuolo, Koen De Backer, Hélène Dernis, Timothy Destefano, David Gierten, Gael Hernandez, Elif Koksal-Oudot, Molly Lesher, Pierre Montagnier, Sam Paltridge, Dirk Pilat, Lorrayne Porciuncula, Giorgio Presidente, Christian Reimsbach-Kounatze, Elettra Ronchi, Cristina Serra-Vallejo, Vincenzo Spiezia, Jonathan Timmis, Colin Webb and Jeremy West. Lucia Cusmano from the OECD Centre for Entrepreneurship, SMEs, Local Development and Tourism, and Deborah Roseveare from the OECD Directorate for Education and Skills, provided valuable comments.

Ben Wallis, consultant to the OECD, was the main author of Chapter 2 on digital infrastructures; he also contributed to Chapter 5 on regulation in the ICT sector and Chapter 3 on financing digital infrastructures and new business models. Konstantinos Karachalios and Karen McCabe, as well as Oleg Logvinov, Wilbert Adams, Dennis Brophy and Sri Chandrasekaran, all from IEEE Standards Association, were the main authors of Chapter 4 on developing standards for a digital world.

Many thanks to Sarah Box for her valuable feedback and to Angela Gosmann for her help in editing and formatting the report.

TABLE OF CONTENTS

Figures

Tables

Boxes

EXECUTIVE SUMMARY

As the cost of data collection, storage and processing continues to decline dramatically and computing power increases, social and economic activities are increasingly migrating to the Internet. Technologies, smart applications and other innovations in the digital economy can improve services and help address policy challenges in a wide range of areas, including health, agriculture, public governance, tax, transport, education, and the environment, among others. Information and communication technologies (ICTs) contribute not just to innovation in products, but also to innovation in processes and organisational arrangements.

As well as a catalyst for growth, digital technologies may be disruptive, with far-reaching effects on productivity, employment and well-being. While new technologies create opportunities for businesses (especially SMEs), workers and citizens to engage in economic activity, these technologies are also likely to displace workers doing specific tasks and may further increase existing gaps in access and use, resulting in new digital divides and greater inequality.

This report provides an assessment of G20 economies' performance with respect to digitalisation (Part I) and examines some of the most pressing policy challenges in areas spanning from access to digital infrastructures to digital security to legal frameworks (Part II). Part III includes a set of 11 core policy recommendations that could underpin a comprehensive G20 digital agenda. Overall, the report aims to help identify the policy mix that will enable G20 economies to best maximise the benefits of an increasingly digitalised global economy, and one in which governments, trading partners, and individuals are all engaged together to ensure that the digital transformation is inclusive.

The following is a brief description of the content of the report. It must be read in conjunction with the key policy recommendations in Part III.

Assessing digitalisation in G20 economies

A set of indicators on digital infrastructure, access to and use of digital technologies, innovation in the digital economy, the skills needed to participate effectively in the digital economy, and metrics around trust, illustrate G20 economies' performance with respect to digitalisation. While G20 countries' performance varies significantly, in part linked to each economy's stage of development, it is clear that those economies that do not have strong digital infrastructures do not perform as well in many of the other areas, in part because digital infrastructures are a foundational element. G20 economies that are relatively isolated geographically tend to engage strongly online, as shown by web presence and e-commerce transactions. With respect to innovation, a relatively small number of G20 economies dominate. An important gap in cross-country comparable metrics on trust is also evident. G20 economies can usefully work together to further develop cross-country comparable metrics in areas such as e-commerce and business use of sophisticated digital technologies (e.g. cloud computing and big data analytics, among others). New areas, such as trust and the IoT, are the next frontier. All countries need to work together to fill the data gaps and in doing so enabling better benchmarking, evidence building, policy development, and the identification and prioritisation of reforms, taking into account each G20 economy's level of development.

Access to digital technologies and services

Despite the rapid spread and uptake of digital technologies, adoption and use vary among G20 economies by demographic categories, industries and firm size, raising concerns about the inclusiveness of the digital transformation. Barriers to the access and effective use of digital technologies typically include some combination of a lack of high-quality and affordable infrastructure; a lack of trust in digital technologies and activities; a shortage of the skills needed to succeed in the digital economy; a more reactive than proactive approach to the openness of the Internet; services trade barriers; high costs and poor access to financing for smaller firms; barriers to the reallocation of resources across firms and sectors; and a lack of interoperability of standards. These barriers can be ameliorated by developing and implementing comprehensive national digital strategies that would encompass actions to enhance competition in telecommunication markets and improve Internet access for disadvantaged groups, SMEs and regions; elevate the importance and clarify the objectives of policies and practices to address digital security and privacy risks; reduce firm-level barriers and enable complementary investments; ensure life-long learning mechanisms to improve workers' skills; ensure Internet openness and cross-border data flows; and foster firm dynamics within the economy.

Digital infrastructures

It is essential that G20 economies continually invest in the development of digital infrastructures to meet existing and future demand. They provide the foundation for many new services, applications and business models. They are also crucial in underpinning and enabling the digital innovations that are transforming production, including in the context of Industrie 4.0. Key barriers to the deployment of high-speed networks and services include the nature of the infrastructure itself (monopolies, duopolies), which can give rise to high barriers to entry. In addition, geography, administrative barriers, regulatory uncertainty, and high capital expenditure, access to spectrum, and in some countries, a lack of basic infrastructure (e.g. electricity) particularly in rural areas, can be stumbling blocks. An important area for policy action involves establishing national broadband plans with well-defined targets and reviewing them regularly. These plans should ideally address the key barriers to the deployment of high-speed networks and services and include measurable targets to address the policy challenges associated with ensuring competition and investment. It is also important that these plans include targets associated with the important technical enablers, such as access to Internet exchange points and spectrum, among others.

Financing digital infrastructures and new business models

Further investments in digital infrastructures, especially high-speed broadband networks, are essential to supporting vibrant, innovative and inclusive digital G20 economies. Financing hurdles related to digital infrastructure investment include high capital costs, susceptibility to changes in market conditions, low rates of return in rural and remote areas, and a lack of accurate data for making informed investment decisions. Encouraging investments in and sharing of data – itself an important 21st-century infrastructure – is also needed. Challenges related to financing digital infrastructures include issues linked to data curation and investment incentives, trust (privacy and digital security risk management), data evaluation, pricing, data ownership and intellectual property rights (IPRs). Access to finance is also a key challenge for innovative enterprises that are seeking to implement new business models based on digital technologies. There are a number of areas in which the G20 could play a role to help address some of these concerns, including by strengthening infrastructure deployment through public and private financing; improving framework policies to foster financing of digital infrastructures and new business models; exchanging experiences and good practices on national initiatives aimed at creating a more entrepreneurial culture; and encouraging investor participation in crowdfunding platforms.

Developing standards for a digital world

Open, voluntary standards, grounded in bottom-up and market-led approaches, are an important tool in the context of fast-developing technologies. Such standards and related guidelines are needed to maintain current levels of safety, ensure trust based on enhanced levels of digital security and privacy, improve energy and resource efficiency, and address emerging social and organisational challenges brought about by the digital transformation. The development of standards and standards-based interoperability are critical for the development of Industrie 4.0 and the IoT, including smart cities and smart mobility. The key to success lies in inclusive standards development, built on collaboration and co-operation among the many players that make up the standards ecosystem. Advanced governance frameworks – building upon both existing public- and private-sector-led processes and new multi-stakeholder initiatives for the benefit of all – are necessary to effectively address the complexity of today's interlinked issues in successful Industrie 4.0 development and deployment. G20 leaders could support the adoption of best practices and policies that enable all relevant actors, including SMEs, to more effectively work together to help foster an interoperable environment in support of the IoT and Industrie 4.0.

Regulation of the ICT sector

The convergence of fixed-line communications, wireless communications and broadcasting over the Internet has created a need for countries to review their regulatory frameworks and public policy objectives to ensure that all market participants have incentives to continue to innovate, compete and invest. Ensuring a 21st-century approach to the ICT sector involves removing regulation where it is no longer necessary or extending the scope of regulation to new service providers. It may also entail creating converged regulators and/or adjusting regulatory powers so they can oversee all elements of bundled services and ensure consistent consumer protection. Promoting competition in the converged communications environment is another important challenge. At the G20 level, a comparative analysis of the effects of convergence on competition and innovation across countries would help to further inform policy actions. The analysis could include elements such as the regulatory environment, mergers and acquisitions, investment and revenue, access paths (fixed, mobile and machine-to-machine (M2M)) and network neutrality rules among others. The development of a "converged analytical framework" to benchmark G20 countries could contribute to a more informed debate on the effects of specific policy actions.

Digital security

Digital security risk has traditionally been approached as a technical problem but the changing nature and scale of digital security risk is driving G20 economies to re-evaluate their strategies and policies in this area. In recent years, many governments and stakeholders have emphasised the importance of considering digital security risk from an economic and social perspective. G20 economies could develop strategies, supported at the highest level of government, to create the conditions for all stakeholders – including SMEs – to manage digital security risk to economic and social activities and to foster trust and confidence in the digital environment. G20 economies could also initiate international arrangements that promote effective privacy and data protection across jurisdictions, including through the development of national privacy strategies that would foster interoperability among frameworks. Such privacy strategies should incorporate a whole-of-society perspective that adjudicates across competing priorities while providing the flexibility needed to take advantage of digital technologies for the benefit of all. To address the need for better evidence on digital security and privacy risk, G20 economies could explore opportunities for strengthening co-operation and international arrangements that promote greater sharing of good practices and information.

Skills and the digital economy

To ensure that all people can engage in and benefit from the digital economy and adapt rapidly to new and unexpected occupations and skill needs, education and training systems in G20 economies should place a stronger emphasis on promoting ICT generic skills, ICT specialist skills, and ICT-complementary skills, including foundational skills, digital literacy, higher-order critical thinking skills as well as social and emotional skills. Greater efforts are also needed to raise the skills of those adults with weak literacy, numeracy and digital skills to enable them to fully participate in the digital economy and society. At the same time, digital technologies are creating new opportunities for skills development. Seizing these opportunities requires a process of institutional learning, where actors are given sufficient scope to experiment with new tools and systematic assessment of outcomes leads to the selection of the most effective practices. Barriers to access these new technologies must be addressed, as well as concerns about the quality of online education and the lack of recognition for learning outcomes. The development of more effective strategies in G20 economies that enable all people to adapt to and excel in the digital economy, including through the use of ICTs and other technologies to upgrade skills, is essential.

Digitalisation, SMEs, start-ups and dynamism

Important differences in ICT adoption and usage exist between large and small firms, with SMEs facing several barriers to adopting ICTs and digital technologies in their operational activities, in particular in having the resources to acquire the necessary complementary knowledge-based assets, such as organisational and human capital. It is essential to help promote adoption of these digital technologies among SMEs because they can help overcome some of the traditional barriers to investing in digital technologies, including the often high, upfront sunk costs of these investments, and allow them to switch more rapidly from one technology to another to avoid being locked in. Comprehensive national digital strategies that take into account SMEs, policies that facilitate access to finance, and SME engagement with competency centres and/or technology diffusion extension services, can be helpful in this regard. Moreover, business dynamism in many G20 economies has declined, especially following the crisis and particularly in ICT-producing and ICT-using sectors, raising concerns about innovation. Policies that can help boost business dynamism include facilitating access to finance, building on the *G20/OECD High-level Principles on SME Financing*. Pro-competitive product market regulations and employment protection legislation that is not overly stringent can also foster dynamism and the adoption of certain digital technologies. Policies that facilitate the mobility of workers as well as training and skills development are important to help smaller firms compete with larger, established incumbents.

Consumer rights in the digital era

Despite the steady increase business-to-consumer e-commerce, there remains considerable untapped potential. Well-tailored consumer protections and competitive markets are essential to build the trust needed to further develop these markets for the benefit of consumers and businesses alike. More effective implementation of consumer rights is essential for e-commerce to reach its full potential. Policy frameworks in the OECD and UN offer an excellent starting place, but likewise require a greater implementation commitment by governments. Cross-border and cross-sectoral enforcement co-operation is but one area for further work. In an increasingly data-centric environment, approaches like data portability offer promise but require further study to ensure that they work for both consumers and businesses. At the same time, G20 economies could usefully explore the issue of platforms and consumer trust with a view to assessing if concerted G20 action could help strengthen consumer trust. Consumer choices in this information-intensive environment are impaired by challenges relating to complexity and uncertainty, sometimes compounded by misleading or fraudulent business practices. The expanding reach of platforms – including peer platforms – poses special challenges to consumer trust, while at the same time opening up new opportunities.

Digitalisation and legal frameworks

Digitalisation is changing the world faster than many laws have evolved. G20 economies should develop mechanisms to periodically review their legal frameworks and, where appropriate, update them to ensure that they are well-suited to the increasingly digitalised world. Designing and implementing a whole-of-government approach to digitalisation is crucial in this regard because advances in one area can be mitigated by retaining the status quo in another. One important legal area that is being affected by digitalisation is competition, which may need to undergo some adjustments in the digitalised context, such as a shift towards looking at data as the most vital competitive asset in some markets, different approaches to market definition and market power, and a greater focus on international co-operation and co-ordination among competition authorities. The G20 may wish to develop tools for assessing the particular complexities of competition in the digital era. Online platforms create new markets and opportunities, but also raise a range of economic and social challenges. Governments should consider updating laws to address factors that unnecessarily make working through online platforms less attractive, the lack of clarity in certain regulations, tax issues that emerge with the proliferation of small revenues earned via platforms, and consumer and privacy protection of online market participants. More broadly, G20 economies could undertake analysis of the opportunities and challenges raised by online platforms and how different policies may help address them.

The ongoing digitalisation of our economies and societies will only expand and deepen; the G20 must be ready to make the most of it. This report has helped chart an innovative, ambitious, and pro-active digital agenda, for the G20 and beyond. It is essential that the G20 work together to build a brighter common future, using the multi-stakeholder model that has served so well. Only by taking a pro-active, 21st-century approach to the digital economy will the G20 maximise the enormous potential the digital economy holds for our economies and well-being.

INTRODUCTION

The digital shifts underway are reshaping economies and societies today and will continue to do so in the future. The ongoing digitalisation of the economy and society holds many promises to spur innovation, generate efficiencies, and improve services throughout the economy. Moreover, the successful transition to a digital economy is a necessary condition for boosting more inclusive and sustainable growth and enhancing overall well-being.

At the same time, digitalisation can be disruptive. It transforms how individuals interact with one another and with society more broadly and changes the structure and business models of the economy. In doing so, digitalisation raises important policy challenges including privacy, security, consumer policy, competition, innovation, jobs and skills, among others. Failure to adequately address these issues could lead to economic inefficiencies, reactionary policies, a worsening of inequalities and a further erosion of the social fabric, as well as slower growth.

The challenge for policy makers is to identify the policy mix that will enable their economies to best maximise the benefits of an increasingly digitalised global economy and adequately address the resulting challenges. To do so, it is essential to ensure access to, and participation in, the digital economy for everyone in all countries; maximise the contribution of technological and ICT innovations to productivity and inclusive growth, job creation and well-being; and build trust and resiliency for networks and users. Given the inherently global nature of the Internet, and the strengthened interconnections it has created, collaboration among and within G20 economies across a wide range of policy areas is critical.

This report aims to help G20 economies assess how they can best work together to foster a vibrant and innovative digital economy. To do so, the report highlights the degree to which digitalisation has impacted economies and societies across the G20 (Part I), identifies some of the key policy issues raised by digitalisation (Part II), and outlines policy recommendations for the G20 in these areas (Part III).

Part 1

ASSESSMENT OF DIGITALISATION IN G20 ECONOMIES

Assessment of digitalisation in G20 economies

It is useful to start with a brief overview of empirical work undertaken to establish the relationships between digitalisation and productivity growth, and between digitalisation, employment, well-being and development.

Productivity and digitalisation

A large body of evidence has emerged on the relationship between digital technologies and productivity growth. Early studies on the impact of digital technologies on growth failed to establish a robust relationship with productivity (Loveman 1994; Strassmann 1990). That is the reason why in 1987, Robert Solow wrote: "You can see the computer age everywhere but in the productivity statistics." Stimulated by the "Productivity Paradox", a rich body of new literature emerged during the early years of the 1990s. Thanks to more advanced econometric techniques and better data, the second generation of studies almost unanimously found positive returns to investment in digital technologies (Brynjolfsson, 1993, 1996; Bresnahan, 1999; Brynjolfsson and Hitt, 1995, 1996, 1997; Oliner and Sichel, 2000; Jorgenson, 2001; Jorgenson and Stiroh, 2000).

Some of these studies emphasised new channels through which digital technologies foster economic growth. For instance, important complementarities have been discovered between investments in digital technologies and other assets, such as human capital, organisational changes and process innovations, i.e. knowledge-based assets (OECD, 2004; Pilat, 2005). Moreover, ICT-related changes in firms are typically part of a process of search and experimentation, where some firms succeed and grow and others fail and disappear. Countries with a business environment that enables this process of creative destruction may be better able to seize the benefits from ICTs than countries where such changes are more difficult and slow to occur. Brynjolfsson and Hitt (1995) and Van Reenen et al. (2010) also find that due to positive "spillover effects" that benefit other sectors, digital technologies tend to exhibit excess returns, both within and across sectors.

The relationship between digital technologies and growth, however, has been found to vary substantially across countries, with stronger effects observed in countries such as the United States and the United Kingdom compared to continental Europe. The existence of such heterogeneity suggests an important role for institutions in determining the effective contribution of digital technologies to productivity. Subsequent studies have found that regulation in labour and product markets tends to reduce incentives to invest both in digital technologies and other complementary assets, such as organisational capital.

While the most prominent studies on the issue are at the firm level, industry-level studies tend to confirm their findings, namely that digital technologies increase labour productivity and foster economic growth. The effect is stronger in manufacturing sectors than in services, although that is possibly due to the important measurement issues linked to services sector productivity. Investment in digital technologies is also found to have important effects in the digital technology-producing sector, due to technological upgrading, scientific discoveries and the production of advanced semiconductors.

Also at the country level, investment in digital technologies is found to be associated with better economic performance. For instance, a significant positive effect is found by Schreyer (2000), Colecchia and Schreyer (2002), Van Ark et al. (2002), Daveri (2002) and Jorgenson (2003). However, the slowdown in productivity growth over the last decades has induced some authors (e.g. Gordon, 2004) to argue that digital technologies will not be able to generate sustained economic growth, at least to the same extent that other great innovations, such as electricity, did in the past. A less pessimistic view can be found in OECD (2015a), where

structural factors associated with the decline in business start-up rates observed in many OECD economies, are thought to be responsible for the decline in aggregate productivity growth.

More recent analysis shows that new and emerging digital technologies affect productivity through mechanisms that are many and varied (OECD, 2016a). For instance:

- By being faster, stronger, more precise and consistent than workers, robots have vastly raised productivity on assembly lines in the automotive industry. They will do so again in an expanding range of sectors and processes.
- The combination of new sensors and actuators, big data analytics, cloud computing and the IoT is enabling autonomous productivity-enhancing machines and intelligent systems.
- Automated maintenance scheduling, enabled by new sensors, artificial intelligence and machine-to-machine (M2M) communications, will reduce disruptions to production caused by breakdowns.
- 3D printing can remove the need for assembly in some stages of production by printing already-assembled mechanisms.
- Progress in materials science and computation will permit a simulation-driven approach to developing new materials. This will reduce time and cost as companies perform less repetitive analysis.

At the same time, the technologies considered in this report have more to contribute to productivity than they currently do (Box 1). Often, their use is predominantly in larger firms, although even in larger firms many potential applications are underused. This can reflect such factors as skills constraints, the novelty of the technologies, incomplete understanding of a technology's potential uses, and institutional inertia. Unexploited opportunities exist throughout industry. For instance, robotics could improve logistics and reduce the price of food and other goods by several percent (CCC/CRA, 2009). Manufacturers see unmet opportunities for automation in skilled and less skilled fields, from manufacturing parts, to machine loading, packaging, palletisation and assembly (Rigby, 2015).

BOX 1. HOW LARGE ARE THE PRODUCTIVITY EFFECTS?

Evidence on productivity impacts from new production technologies come mainly from firm- and technology-specific studies. A sample of these studies is provided below. These studies suggest sizeable potential productivity impacts. However, the studies follow a variety of methodological approaches, and often report results from a few, early-adopting technology users, making aggregate estimates difficult to derive.

- In the United States, output and productivity in firms that adopt data-driven decision making are 5% to 6% higher than expected given those firms' other investments in ICTs (Brynjolfsson, Hitt and Kim, 2011).
- Improving data quality and access by 10% – i.e. presenting data more concisely and consistently across platforms and allowing them to be more easily manipulated – would increase labour productivity by 14% on average, but with significant cross-industry variations (Barua, Mani and Mukherjee, 2013).
- Autonomous mine haulage trucks could in some cases increase output by 15% to 20%, lower fuel consumption by 10% to 15% and reduce maintenance costs by 8% (Citigroup-Oxford Martin School, 2015).
- Autonomous drill rigs can increase productivity by 30% to 60% (Citigroup-Oxford Martin School, 2015).
- By raising productivity new technologies can also improve financial performance among adopters. A recent case study shows that by developing a significant IoT and data analytics capability, a leading United States automaker has saved around USD 2 billion over the past five years (2011-14 and most of 2015). A 1% increase in maintenance efficiency in the aviation industry, brought about by the industrial Internet, could save commercial airlines globally around USD 2 billion per year (Evans and Anninziata, 2012).

In the past, there has also been unrealistic enthusiasm regarding timescales for the delivery of some industrial technologies. Sometimes, this reflected miscalculation of the technical challenges. In terms of adoption, advanced ICTs remain below potential. Cloud computing, for instance, was first commercialised in the 1990s, but is still not widely adopted in G20 economies. And the mere availability of a technology is not a sufficient condition for its uptake and successful use. Realising the benefits of a technology often requires that it be bundled with investments in complementary assets such as new skills and organisational forms and that new, better adapted, business models are invented that channel income to innovators (OECD, 2013a).

The aggregate impacts of ICTs on productivity are often obscured by the large differences in impact across firms. Recent analysis points to a growing dispersion in productivity performance between leading firms and their non-frontier counterparts within countries and sectors (OECD, 2015a; Andrews, Criscuolo and Gal, 2016). For instances, the 2000s saw labour productivity at the global technological frontier increase at an average annual rate of 3.5% in the manufacturing sector, compared to just 0.5% for non-frontier firms. The gap was even more pronounced in the services sector.

There are several, possibly complementary, explanations for this dispersion in productivity growth. Possible contributing factors include: the growing capture of rents by frontier firms, e.g. in the ICT sector; the ability of these firms to attract the limited pool of highly skilled workers with new sets of horizontal skills required to cope with the rapid pace of innovation, and the lingering presence of poorly performing firms, that have remained in the market rather than close down, trapping valuable resources in unproductive activities. All of these may have contributed to the slowdown in the pace of diffusion from the productivity frontier to the rest of the economy. Structural settings limiting competition, discouraging firm entry and exit, and leading to skills mismatch may have contributed to each of these phenomena. Turning digitalisation into productivity growth will therefore require a comprehensive approach that considers these elements in turn.

Another strand of literature questions whether the productivity slowdown could be due to mismeasurement. For instance, Ahmad and Schreyer (2016) analyse whether existing concepts for the measurement of gross domestic product (GDP) could be inappropriate given that many new goods and services have a preponderant digital component. While they suggest that overall the current accounting framework seems still appropriate, they discuss a number of measurement issues.

Digitalisation and employment

Recent OECD findings suggest that so far, while leading to restructuring and reallocation, ICTs have not led to greater unemployment over time. If adopted successfully, i.e. if combined with organisational changes and good managerial practices (Brynjolfsson and Hitt, 2000; OECD, 2004), ICTs can contribute to increased productivity, which progressively translates into lower prices and/or new products, higher final demand and higher employment, thus compensating for the initial job displacement. There is indeed evidence that ICTs have – thus far – not produced an increase in technological unemployment (OECD, 2015b).

Skill-biased technological change (SBTC), a manifestation of productivity-enhancing technological change, has been a main factor linked to growth over recent decades. Most new technologies have required higher levels of skill to use than those they displace. This is a long-standing trend. Analysis suggests that the faster the rate of technological change, the wider the increase in wage dispersion, the greater the increase in the supply of skilled labour, and the slower the increase in wage dispersion (OECD, 2011a).

The SBTC hypothesis is successful in explaining the rise in the employment share of workers in high-skill jobs over the past three decades. For example, in the United States, the employment share of workers in high-skill occupations increased by 11 percentage points from 26% in 1983 to 37% in 2012 (Tüzemen and Willis, 2013). However, a simple version of the SBTC hypothesis suggests that the share of low-skilled jobs should have fallen. Instead, the employment share of low-skilled occupations rose from 15% in 1983 to 18% in 2012 in the

United States. This pattern of an increasing share of low-skilled jobs has been mirrored in other countries. Such trends do not necessarily disprove the SBTC hypothesis; it is possible that some jobs require a higher level of skills than in the past (car mechanics now often need to have ICT skills, for example).

Nevertheless, attention has turned to another possible link between technological change, productivity and inequality – the job polarisation hypothesis. Developments in artificial intelligence, unprecedented computer power, the IoT and big data, among other technological advancements may change the nature of the link between technology and jobs. Some studies suggest that digitalisation may make it possible that, in the near future, a large proportion of tasks or even entire occupations currently carried out by workers could be performed by machines (Frey and Osborne, 2013) enhancing the fear that computers and many are bound to lose (Brynjolfsson and McAfee, 2011). Recent analysis suggests that on average across countries, 9% of jobs are at high risk of being automated, while for another 25% more jobs, 50% of the tasks will change significantly because of automation (Arntz, Gregory and Zierahn, 2016). A key question remains whether digitalisation increases the pace or nature of hollowing-out, with implications on jobs.

Those jobs relying on a high proportion of automatable tasks are at high risk of being substituted for by new technologies. Computers and algorithms mainly substitute for easily codifiable, conceptual jobs on the highly skilled end of the skill distribution, or manual jobs at the bottom end of the skill distribution. But the implications for job changes will only take place if these technologies are taken up by firms, or firms that do not use these technologies exit the market. If this occurs, however, the gains to overall productivity would also be limited.

The extent and permanence of hollowing-out remains controversial. Estimates such as Frey and Osborne (2013) have been criticised on the basis that rather than occupations it is specific tasks that are at risk of automation, while occupations are more likely to evolve to accommodate the penetration of technology rather than face complete substitution (Bessen, 2015). Workers with the skills to adapt to changes in the workplace are less at risk of being left behind. Also, with the productivity gains and the adoption of technology, new and complementary jobs are likely to be created (Autor, 2015; Moretti, 2010; Goos, Konings and Vandeweyer, 2015). Overall, however, these studies find evidence that the share of middle wage jobs, characterised by routine tasks, has declined and the wage share of the middle-skilled has also contracted, which has contributed to increased inequality. Evidence of temporary job polarisation is also supported by OECD findings (OECD, 2015c) which suggest that in periods where labour demand decreases due to ICTs, the decrease is stronger for medium-skilled workers than for their high- and low-skilled counterparts.

Workers will need different skills, not just more skills. Regardless of the precise number of jobs at risk of automation, continued hollowing-out will continue to disrupt the labour market. Up-skilling will be part of the solution, but workers will also need a different sort of skill-set. Data from the OECD Survey of Adult Skills show that on average across the 22 countries that implemented the survey, 55% of workers lack basic problem-solving skills in technology-rich environments, suggesting weak prospects for capitalising on the opportunities offered by the digital economy (OECD, 2013b).

Digitalisation is also changing the way work is organised. The “platform economy” (referring broadly to the ”gig”, “sharing”, and “on-demand” economies), though still small in scale, is growing quickly across many sectors since it lowers the transaction costs of businesses accessing a larger pool of potential workers and suppliers, with workers increasingly engaged as independent contract workers. This has benefits for some workers, providing them with greater flexibility, and allowing people to earn additional income and access work, sometimes for the first time. At the same time, these jobs rely mostly on non-standard work arrangements (e.g. self-employment) that may limit access to regular jobs; it may also offer less promising employment trajectories and lower access to social protection or training opportunities; and it could also limit worker’s access to union representation and wage-setting mechanisms.

Digitalisation and well-being

Having established a positive relationship between digital technologies, productivity and growth, the literature has more recently moved to study how digital technologies can affect well-being. For example, Atkinson and McKay (2007) argue that digital technologies are improving healthcare, access to education, the monitoring of the environmental quality, and that they are giving consumers the possibility of interacting more fluidly with business and governments. The digital economy also has huge potential to enhance social well-being.

Inequality, by definition, means that people do not have the same access to scarce resources, and that some do not have any access. New technologies in some cases can eliminate that scarcity. For example, new technologies can leverage human brain capacities and cognitive skills in similar ways to earlier breakthrough technologies, such as steam power and electricity, which magnified human physical strength. This holds the promise of similar or even greater increases in living standards, considering that digitised information can be reproduced at low cost and used simultaneously thus being far less subject to scarcity.

Digital technologies can also promote social inclusion by creating better access to quality education and offering new opportunities for skills development (OECD, 2014a). Digital learning environments can enhance education in multiple ways, for example by expanding access to content to people from low-income backgrounds or disadvantaged areas, supporting new pedagogies with learners as active participants, fostering collaboration between educators and between students, and enabling faster and more detailed feedback on the learning process. Similarly, several authors argue that digital technologies have enormous potential to innovate and improve the quality of teaching, and more in general the learning experience (Yusuf, 2005; Jhurree, 2005; Hepp et al., 2004).

New digital technologies are particularly important to better connect disadvantaged groups (OECD, 2016b). For example, mobile connectivity is helping reach remote populations as well as those with lower incomes, due to its low costs. Pantea and Martens (2014) find that low-income users spend even more time on the Internet than the average, browsing websites that deal with education, career opportunities, health and nutrition themes and online sales platforms. Potential benefits for low-income groups also relate to improved access to free or very low-cost knowledge and information; services that allow consumers to negotiate better prices for products (as well as identify better quality products); as well new consumption opportunities offered by Internet-based platforms.

Technological innovations in the financial and health sectors can also promote social inclusion. Digital lending innovations and innovative financing like peer-to-peer lending and crowdfunding platforms have the potential to fill a bank lending gap and improve access to finance for both households and small enterprises, allowing for the participation of small investors. Financial innovations will, however, require an appropriate regulatory and legal framework ensuring transparency and accountability. Tailored financial education programmes can help enable individuals and small businesses to make use of these new opportunities and help them make informed choices. In the health sector, a study by Deloitte (2015) also finds that digital technologies enable patients, carers and healthcare professionals to access data and information more easily and improve the quality of outcomes of both health and social care.

Digitalisation and development

Following the rapid spread of digital networks across the world, a large body of evidence is now emerging that shows that digitalisation does not only contribute to productivity and efficiency, but also to broader socio-economic development. It can give rise to a more inclusive society and better governance arrangements; enhance access to key services such as health, education and banking; improve the quality and coverage of public services and political participation; expand the way that individuals collaborate and create content; and enable them to benefit from a greater diversity and choice in products and from lower prices.

The role of digital networks as an accelerator of development has been recognised globally, and due to its critical importance to the three pillars of development – economic development, social inclusion and environmental protection – the task of making the Internet universal and affordable was approved as a target (Target 9.c) of the Sustainable Development Goals (SDGs), echoing the objective already elaborated by the United Nation's Broadband Commission for Sustainable Development. Policies that explore the full potential of ICTs can accelerate progress towards the attainment of the SDGs. Table 1 summarises the ICT components already set as targets in the SDGs and includes other possible ICTs components that can contribute to the remaining goals.

Table 1. Sustainable Development Goals (SDGs) and ICTs

1 NO POVERTY	Target 1.4. *By 2030, ensure that all men and women, in particular the poor and the vulnerable, have equal rights to economic resources, as well as access to basic services […], appropriate* ***new technology*** *and financial services, including microfinance."*	9 INDUSTRY, INNOVATION AND INFRASTRUCTURE	Target 9.c. *Significantly increase access to* ***information and communications technology*** *and strive to provide* ***universal and affordable access to the Internet*** *in least developed countries by 2020.*
2 ZERO HUNGER	Target 2.a. *Increase investment […] in rural infrastructure, agricultural research and extension services,* ***technology development*** *and plant and livestock gene banks […]."/* Target 2.c. *Adopt measures to ensure the proper functioning of food commodity markets […] and facilitate timely* ***access to market information****, including on food reserves, in order to help limit extreme food price volatility.*	10 REDUCED INEQUALITIES	ICTs, and especially through mobile-based services, can contribute to reducing inequality by drastically **expanding access to information**, hence contributing to individual empowerment and social inclusion of individuals that used to fall outside of the reach of traditional services.
3 GOOD HEALTH AND WELL-BEING	The use of ICTs in the health sector can result in higher quality, safer and more responsive to patient's needs. **E-Health** can be particularly important in rural and remote areas by enabling innovative models of care delivery, such as by telemedicine and mobile health.	11 SUSTAINABLE CITIES AND COMMUNITIES	ICTs can be leveraged to organise cities and communities more efficiently. **Smart cities** use ICTs and big data to improve public service delivery and to advance wide policy outcomes such as energy saving, safety, urban mobility and sustainable development.
4 QUALITY EDUCATION	Target 4.b. *By 2020, substantially expand globally the number of scholarships available to developing countries […] for enrolment in higher education, including vocational training and* ***information and communications technology****, technical, engineering and scientific programmes, in developed countries and other developing countries.*	12 RESPONSIBLE CONSUMPTION AND PRODUCTION	ICTs, and especially broadband, has connected consumers and producers directly and given rise to **"on demand" markets** of products that can be customised and localised, which can save time, reduce transportation costs and contribute to a more efficient and sustainable consumption.
5 GENDER EQUALITY	Target 5.b. *Enhance the use of enabling technology, in particular* ***information and communications technology****, to promote the empowerment of women.*	13 CLIMATE ACTION	
14 LIFE BELOW WATER		15 LIFE ON LAND	The use of **Internet of Things** can contribute to making environment-monitoring tasks cheaper, faster and more convenient.
6 CLEAN WATER AND SANITATION		7 AFFORDABLE AND CLEAN ENERGY	ICTs can contribute to improving water and energy access by using **mobile solutions, smart grids and meters** to advance efficiency, manage demand and develop new ways to expand access.
16 PEACE, JUSTICE AND STRONG INSTITUTIONS	The use of ICTs in the public sector can improve the offer and uptake of **digital government** services; strengthen the performance of public institutions and improve transparency and citizen's participation.		
8 DECENT WORK AND ECONOMIC GROWTH	Target 8.2. *Achieve higher levels of economic productivity through diversification,* ***technological upgrading and innovation****. /* Target 8.3. *Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship,* ***creativity and innovation****, and encourage the formalisation and growth of micro-, small- and medium-sized enterprises, including through access to financial services.*	17 PARTNERSHIPS FOR THE GOALS	Target 17.8. *Fully operationalise the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular* ***information and communications technology****.*

Note: Not all SDGs had an ICT component officially included in a corresponding target by the UN. In those cases, identified by (*), examples were identified by the OECD to depict how ICT could contribute to that particular goal.

Sources: United Nations General Assembly (2015), "Transforming our world: the 2030 Agenda for Sustainable Development", *https://sustainabledevelopment.un.org/post2015/transformingourworld*; OECD.

However, despite the rapid spread of the Internet and the increasing agreement on the opportunities it brings, nearly 60% of the world's population, or four billion people, remain offline. These gaps in the availability and penetration of the Internet persist and a large portion of the population is still unable to directly reap digital dividends. Enhancing access to infrastructure, as discussed throughout this report, is therefore a major task for developing economies. The task of closing the access and usage gaps is a multifaceted one. It involves major 'supply-side' challenges, notably of encouraging investment and competition, extending broadband infrastructure outside of urban areas into rural and remote areas, and upgrading networks to match rising demand. Additionally, demand-side issues such as low levels of income, education and local content production add new challenges to improving affordability and relevance of services to users.

As the challenges are often substantial and the stakes so high, designing and implementing sound broadband policies is crucial. Policy makers and regulators have at their disposal a large variety of tools that can be used to stimulate and encourage investment, competition and network deployment, and contribute to making services more affordable, relevant, usable and safer for individuals and businesses.

Not all the challenges for extending access to the Internet use can be addressed by policy makers and regulators alone and other broader structural challenges present in developing economies, such as lack of basic electricity and road infrastructure in remote areas need to be considered. That being said, improved communication can also help to address and potentially substitute for deficiencies in essential services, such as enabling business models for off-grid energy availability (e.g. pre-paid solar energy) or overcoming distances or transport barriers to the delivery of public services and exchange of commerce. Critically, successfully implemented broadband policies, articulated towards improving social inclusion, productivity, and governance can act as catalysts for expanding the digital dividends of broadband access and use throughout the whole economy and society. Experience shows that well-designed regulatory tools and ambitious digital strategies and broadband policies that harness the potential of individuals, business and governments can make a substantial difference on fostering broadband deployment, investment, competition and use.

Select indicators of digitalisation in G20 economies

This section provides indicators to illustrate G20 economies' performance with respect to digitalisation. Indicators are presented at the individual country level and are shaded to highlight four regions:

Regional classification:

Europe **North and South America** **Asia, Middle East and Oceania** **Africa**

The indicators are grouped into five broad categories: digital infrastructure, access to and use of digital technologies, innovation in the digital economy, the skills needed to participate effectively in the digital economy, and metrics around trust.

Digital infrastructure

Efficient and reliable communication networks and services are the foundation on which the digital economy is based. It is critical that governments promote investment and competition in the provision of high-speed networks and services, ensuring that key enablers are in place (e.g. sufficient spectrum and increasing uptake of IPv6 Internet addresses), as well as encourage investments data itself to realise the full potential of the digital economy.

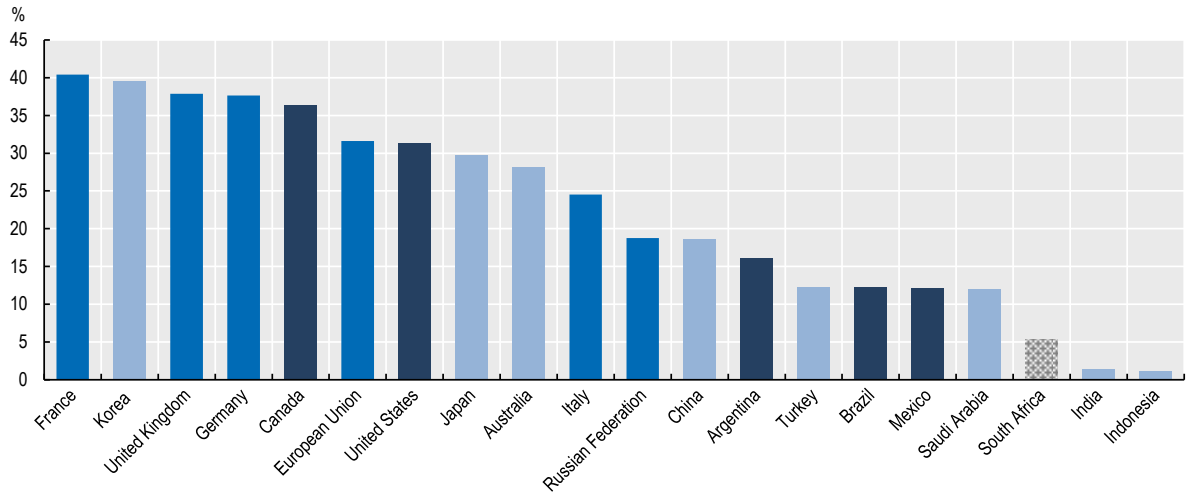
Broadband is an essential digital infrastructure. The demands for faster broadband are increasing due to the use of the Internet in providing a range of communication services, rapidly increasing volumes of Internet video traffic, increasing numbers of smartphone and other mobile devices, the connection of billions of smart

objects through the IoT, and access to applications and data stored remotely. Broadband infrastructure needs to keep pace with these growing demands for broadband Internet access. This applies to both terrestrial (e.g. fibre) and wireless or mobile broadband which are closely interrelated as terrestrial networks provide essential "back haul" that link the edges to the main (backbone) network.

Among the G20, France has the highest average fixed (wired) broadband penetration (almost 40.5 subscriptions per 100 inhabitants), closely followed by Korea, the United Kingdom and Germany, although large differences exist across countries, pointing to significant potential for emerging economies to catch up (Figure 1).

Figure 1. Fixed broadband subscriptions per 100 inhabitants

December 2015



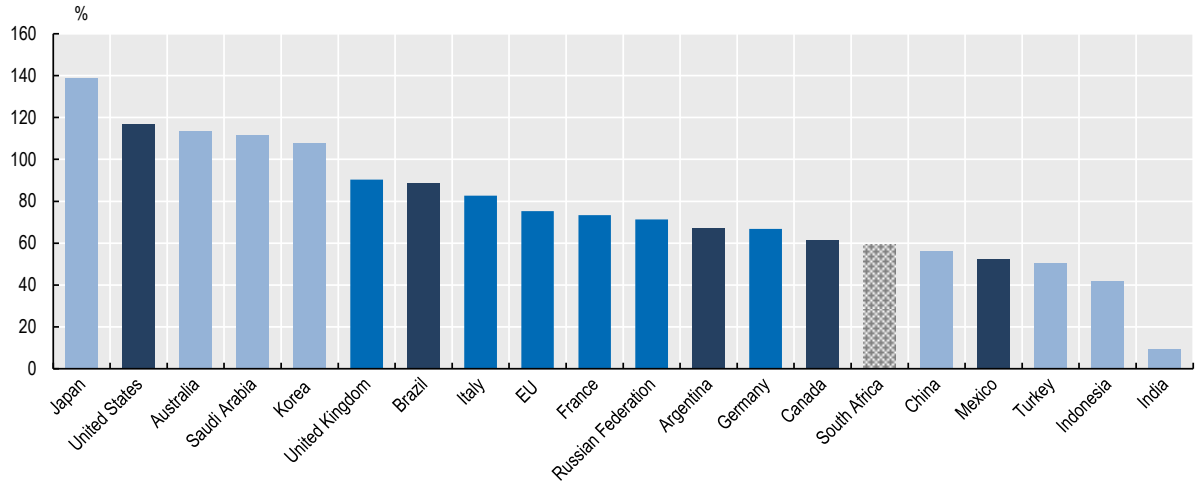
Note: EU data are for July 2015.

Sources: OECD for OECD G20 economies; European Commission (DG CONNECT) for European Union; ITU for other G20 economies.

Given the increasing importance of connectivity on-the-go and with the progressive deepening of the IoT, mobile broadband is another key digital infrastructure. At 139 subscriptions per 100 inhabitants, Japan leads the G20 in mobile broadband penetration, although the variation across countries is more mixed between developed and emerging economies, which points to potential leapfrogging in some cases (Figure 2). Expanding mobile broadband will become even more important with the evolving IoT in which more and more mobile devices will require an Internet connection over mobile networks.

Figure 2. Mobile broadband subscriptions per 100 inhabitants

December 2015



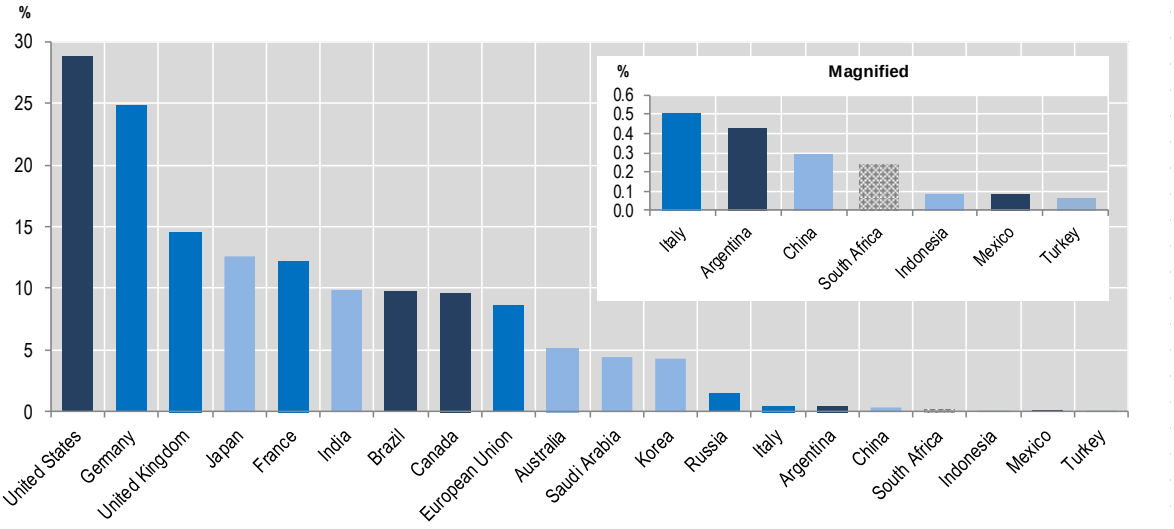
Note: EU data are for July 2015.

Sources: OECD for OECD G20 economies; European Commission (DG CONNECT) for EU; ITU for other G20 economies.

A key enabler of the Internet is the Internet Protocol (IP) system that routes information across the Internet. The transition from the current Internet addressing system (IPv4) to the latest version of the IP (IPv6) is essential as IPv4 addresses have almost run out, and the future growth of the Internet depends on the availability of a new pool of addresses. Part of this growth will come from the IoT and the Industrial Internet, as both paradigms demanding more addressing space. The United States leads the G20 with uptake of IPv6 at about 29% with Germany (25%) close behind (Figure 3).

Figure 3. Availability of end-to-end IPv6 connectivity among Google users in the G20

2016

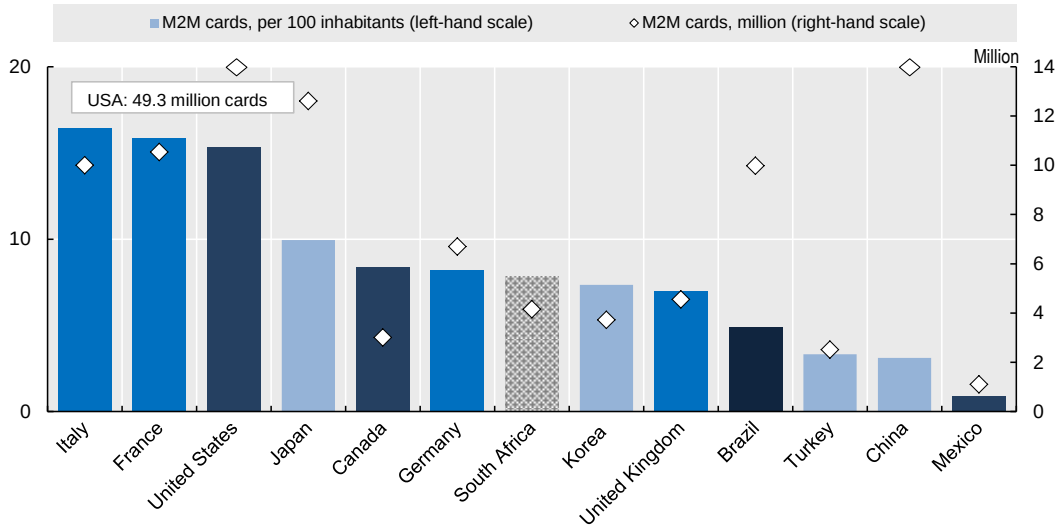


Source: Google (2016).

One way of measuring the IoT is the number of SIM cards and phone numbers allocated to M2M communication devices on mobile networks, which account for a growing segment of mobile data subscriptions. Current data show brisk market growth in SIM cards and phone numbers in many countries. In 2015, there were 162 million SIM cards for M2M communication in the 13 countries for which data is available, with the United States leading the reporting G20 economies with just over 49 million M2M SIM cards in circulation, followed closely by the People's Republic of China (hereafter "China") (43 million) (Figure 4).

Figure 4. Penetration of machine-to-machine (M2M) SIM cards

December 2015



Note: For Korea, provided data does not include some devices (personal navigation devices etc.) as they are based on different technologies rather than SIM cards.

Sources: OECD for OECD G20 economies; ITU for other G20 economies.

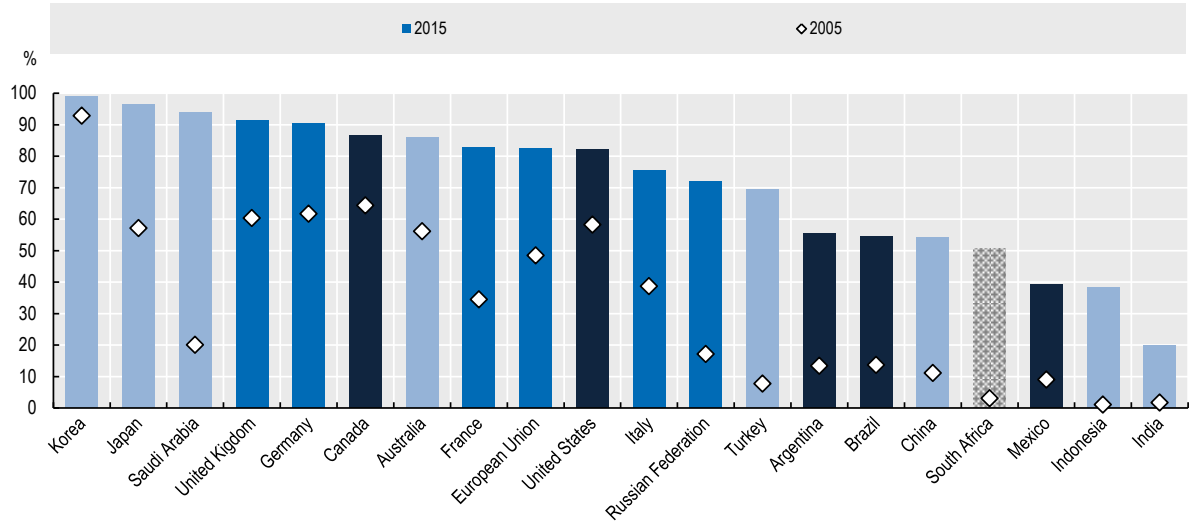
Access to and use of digital technologies and services

Individuals and businesses, including SMEs, need reliable and widespread access to digital networks and services to benefit from digital opportunities and boost growth and well-being. This is also important for ensuring that the global digital divide does not grow wider, and would help people in low- and middle-income countries, those in rural areas and other disadvantaged groups, to benefit from the education, employment and health opportunities that are enabled by the Internet. This section illustrates some measures of ICT adoption, with others included in Chapter 1 on access and use of digital technologies.

Access to the Internet has improved significantly in the past decade, with all G20 economies seeing significant gains, albeit some from a low base. Access is almost universal in Korea, Japan and Saudi Arabia, and is very high in much of the G20, with those countries lagging behind also having lower levels of broadband penetration (Figure 5).

Figure 5. Households with Internet access at home

As a percentage of total households

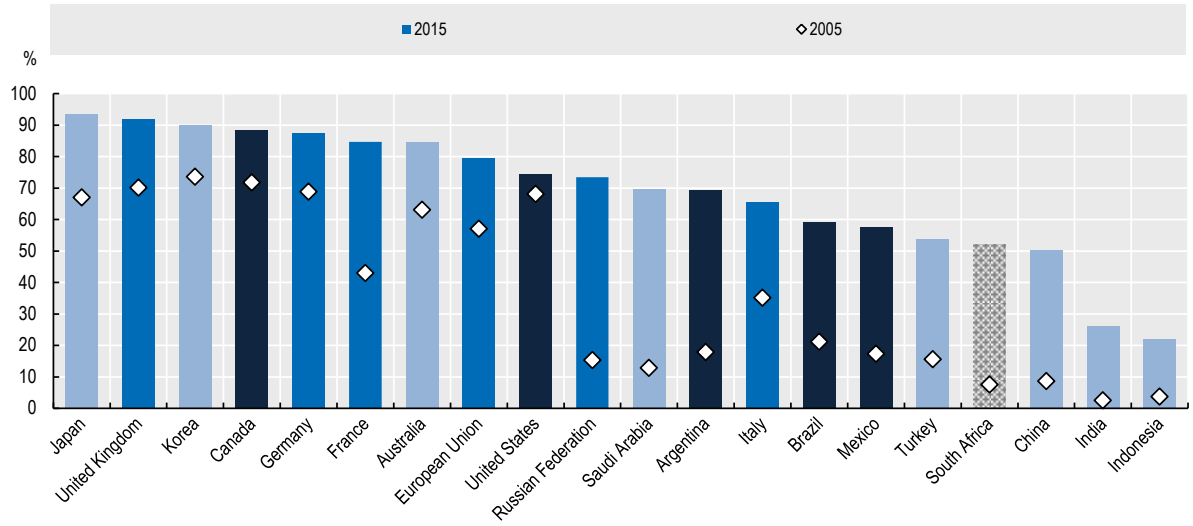


Sources: ITU World Telecommunication/ICT Indicators Database; Eurostat Information Society Statistics Database, November 2016.

Internet usage varies considerably across G20 economies, ranging from 22% of all individuals (Indonesia) to 93% (Japan). In addition to Japan, many other G20 economies show very high rates of Internet use, including the United Kingdom, Korea, and Canada, although some G20 economies show a significant gap in Internet users, due in large part to lower levels of broadband penetration and other digital infrastructures (Figure 6). Other differences in uptake are due primarily to age and education, often intertwined with income levels. In many countries, uptake by young people is almost universal, but there are large differences for older generations.

Figure 6. Individuals using the Internet

As a percentage of total individuals



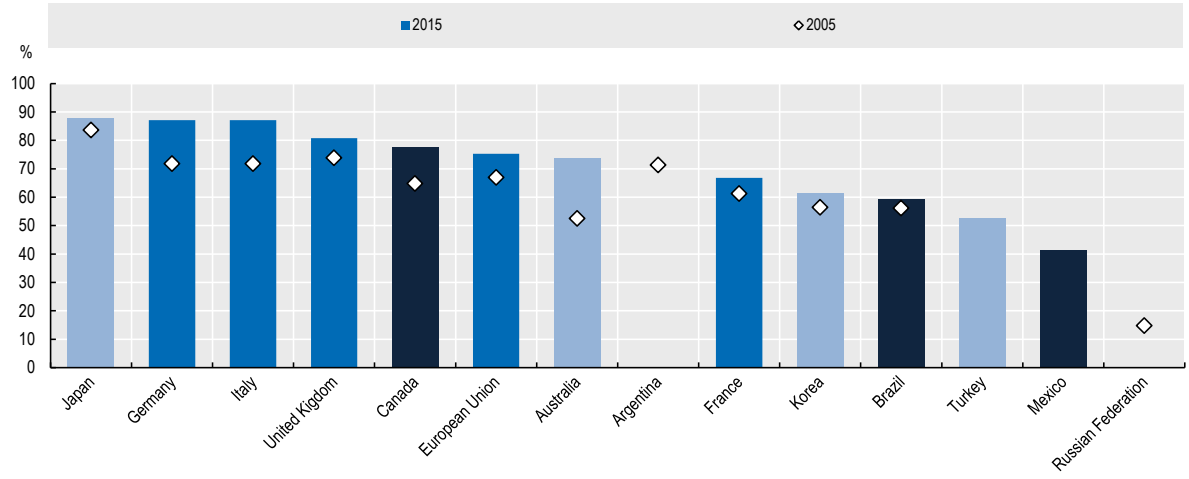
Note: Please note that the number of total individuals may vary across countries depending on age intervals.

Sources: ITU World Telecommunication/ICT Indicators Database; Eurostat Information Society Statistics Database, November 2016.

The Internet opens up new opportunities on domestic and global markets for consumers and businesses. To take advantage of these opportunities, a web presence is essential. More than half of all firms had a web presence in most G20 economies, and web presence among firms has increased across the board in the last decade (Figure 7).

Figure 7. Businesses with a web presence

As a percentage of total businesses



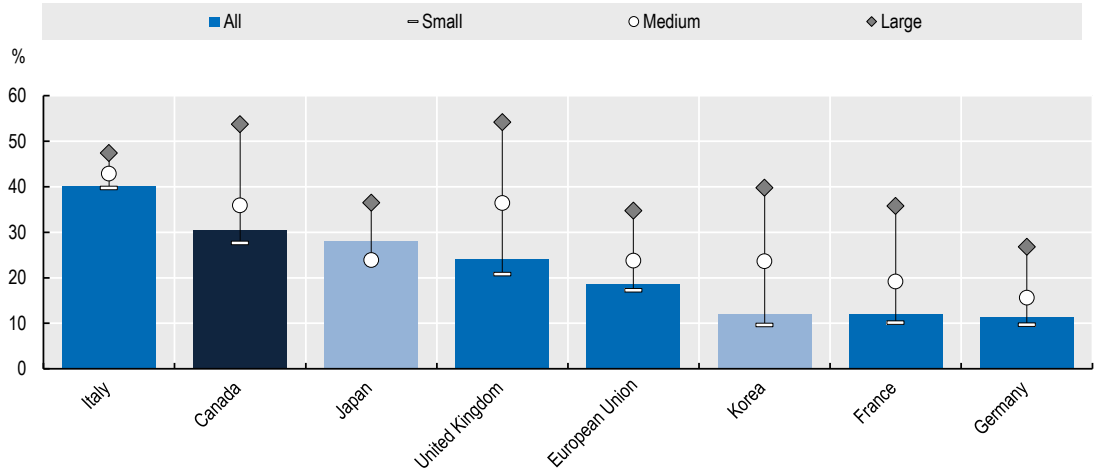
Note: For Argentina and the Russian Federation, no recent data is available.

Sources: Eurostat; OECD; UNCTAD, November 2016.

Cloud computing – a service model for renting computing services – has been a particularly transformative digital technology. Since cloud computing transforms computing into a service, firms can turn their capital expenditures into operating expenses. Firms more frequently invest in cloud computing services with a high degree of sophistication, such as financial and accounting software, customer relationship management software and raw computing power, rather than in less sophisticated services, such as email, office software or file storage. The diffusion of cloud computing among firms has accelerated in recent years, with Italy leading the G20 reporting economies with 40% of all firms indicating use of cloud computing services (Figure 8). However, there remains a substantial gap between large firms and SMEs in the use of more advanced ICT applications such as cloud computing, where SMEs lag larger firms across all countries.

Figure 8. Enterprises using cloud computing services, by size, 2015

As a percentage of enterprises in each employment size class



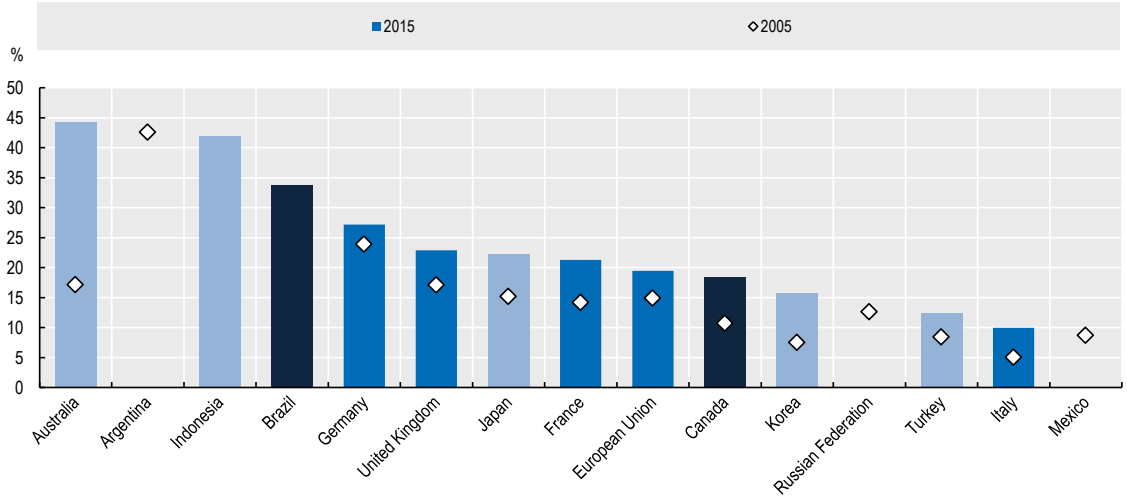
Sources: OECD, *ICT Database*; Eurostat, *Information Society Statistics Database*, April 2016.

Firms are increasingly using the Internet to engage in e-commerce. In Australia, for example, about 45% of enterprises reported making sales via e-commerce in 2015, compared to about one in ten firms in Italy (Figure 9). All reporting G20 economies increased their sales via e-commerce during this period, with Australian firms leading the group and Indonesian and Brazilian firms close behind. Data for a smaller sample of countries

show that large firms have much greater uptake than small firms, highlighting the importance of promoting the diffusion of digital technologies to SMEs.

Figure 9. Businesses engaged in sales via e-commerce

As a percentage of total businesses



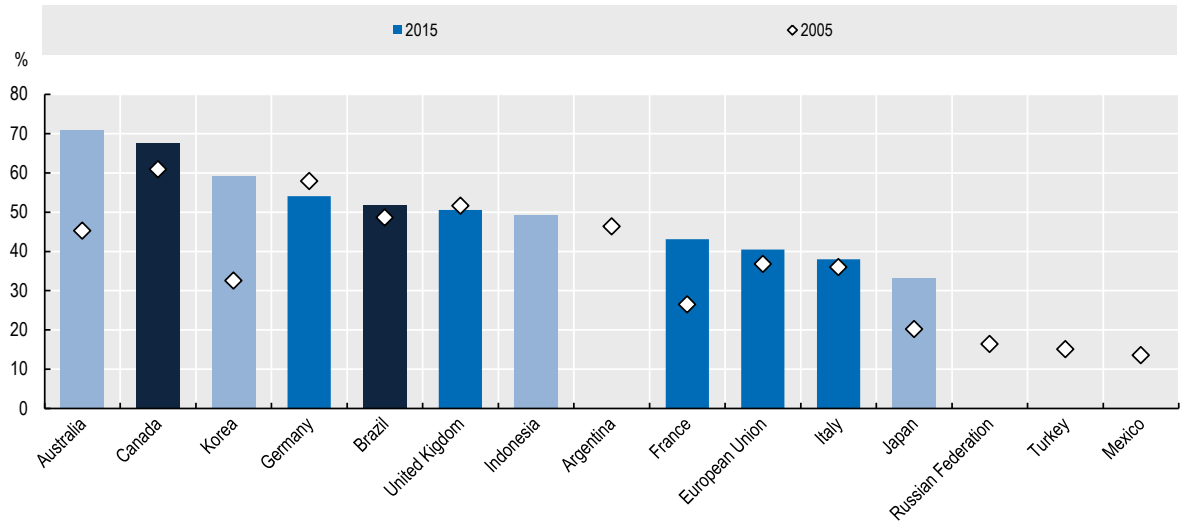
Note: For Argentina, the Russian Federation and Mexico, no recent data is available.

Sources: Eurostat; OECD; UNCTAD, November 2016.

At the same time, firms are increasingly placing orders over the Internet. About 70% of all Australian firms placed orders over the Internet in 2015, an increase of 26 percentage points in a decade (Figure 10). Only in Germany and the United Kingdom did firms slightly decrease their use of the Internet to place orders over the 2005-15 period.

Figure 10. Businesses placing orders over the Internet

As a percentage of total businesses



Note: For Argentina, the Russian Federation, Turkey and Mexico, no recent data is available.

Sources: Eurostat; OECD; UNCTAD, November 2016.

Innovation in the digital economy

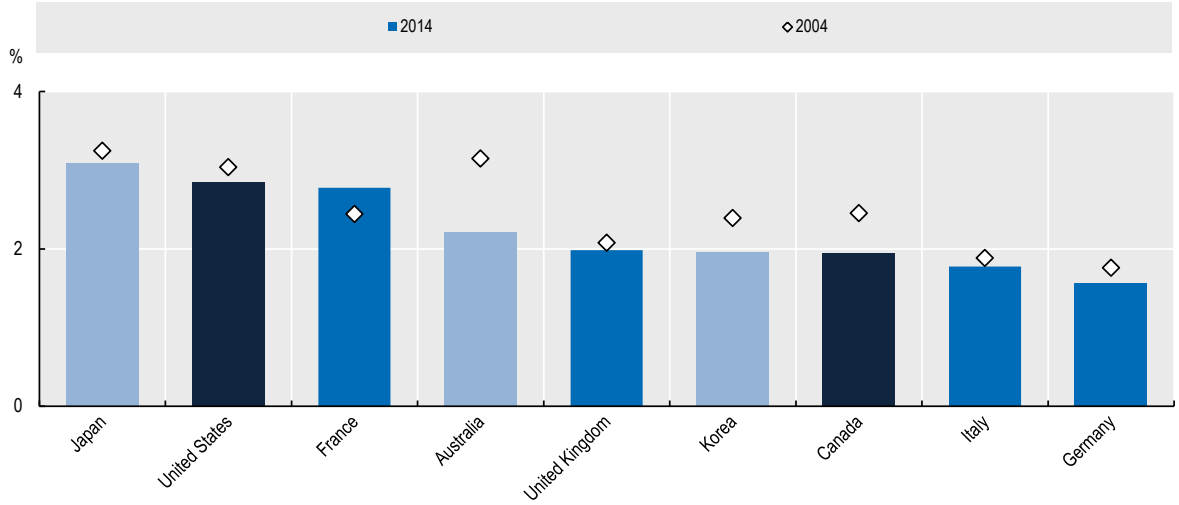
Technologies, smart applications and other innovations in the digital economy can improve services and help address policy challenges in a wide range of areas, including health, agriculture, public governance, tax, transport, education, and the environment, among others. ICTs contribute not just to innovation in products,

but also to innovation in processes and organisational arrangements. Digital innovations also facilitate co-operation within and among countries.

Investment in ICT goods and services is an important driver of growth in the long-term, with two-thirds of ICT investment devoted to computer software and databases. Since 2004, ICT investment has declined in almost all of the G20 economies for which data are available (Figure 11). This slowdown is in part due to a rapid decrease in prices, particularly for IT equipment, as well the fact that many firms are now buying IT services instead through the cloud, which means that at least a proportion of business ICT expenditures are not being capitalised and included in ICT investment.

Figure 11. ICT investment

As a percentage of GDP

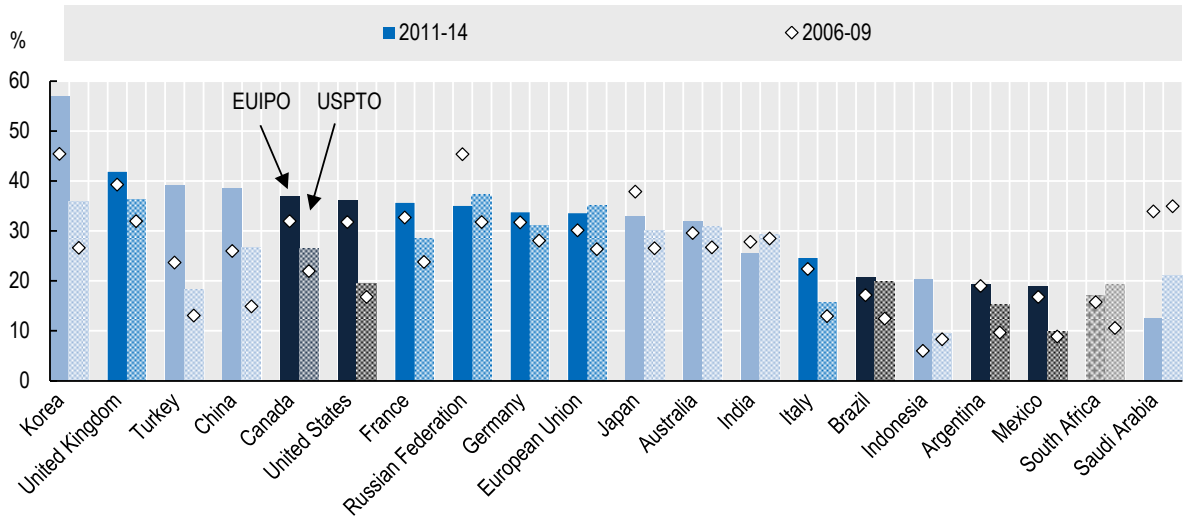


Source: OECD, *Annual National Accounts*, May 2016.

Trademarks provide a measure of the relevance of branding in particular product areas, conditional on the need to protect these brands against counterfeiting. The distribution of ICT-related trademarks offers a distinctive perspective on the competitive position of economies *vis-à-vis* digitalisation, especially in terms of innovation in ICT services. The data show that Korea leads the G20 in registrations of ICT-related trademarks, with 57% of all of its trademark applications to the European Union Intellectual Property Office (EUIPO) and 36% of its trademark applications to the United States Patent and Trademark Office (USPTO) in ICT-related areas, and these shares have increased significantly in recent years in Korea, Turkey and China (Figure 12).

Figure 12. ICT-related trademarks

As a percentage of applicants' total trademark registrations at EUIPO and USPTO

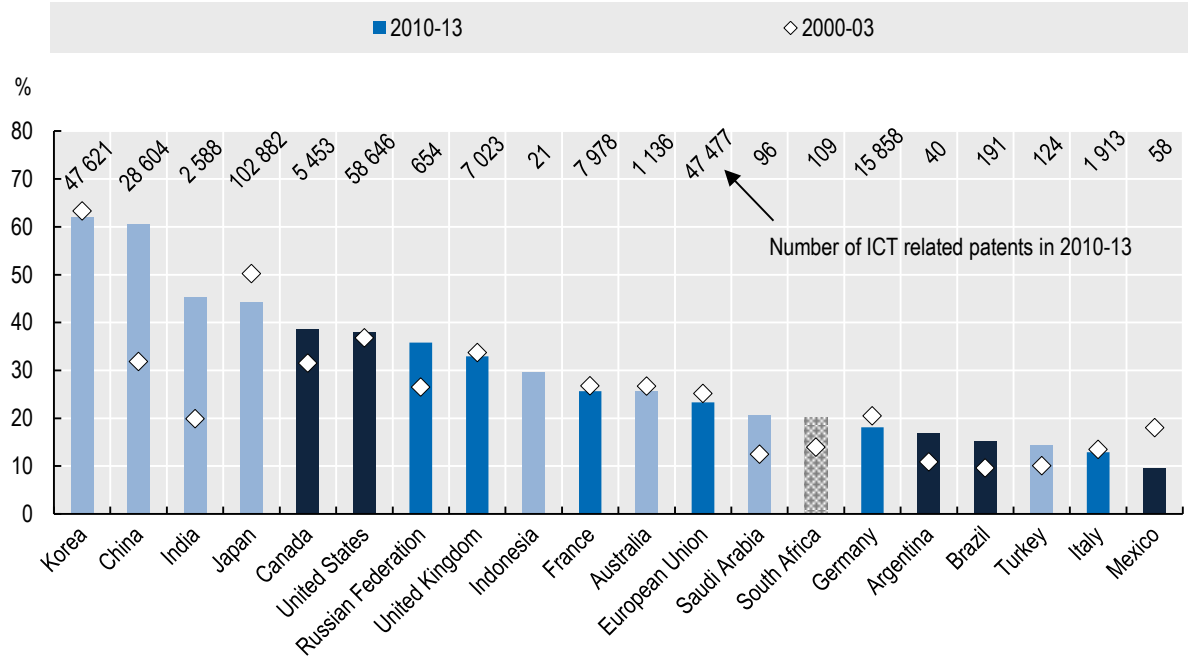


Source: OECD calculations based on US Patent and Trademark Office and EUIPO Trademark Database, November 2016.

Further innovations in ICTs are essential to addressing the grand challenges we face such as providing healthcare to aging populations, reducing inequalities and preserving the environment. Patenting in ICTs grew by almost 60% between 2000-03 and 2010-13 among G20 economies (Figure 13). Since 2000, ICT-related patents as a share of total patents grew markedly in China and India, by almost 30 and 25 percentage points, respectively.

Figure 13. ICT-related patents

As a percentage of total patents



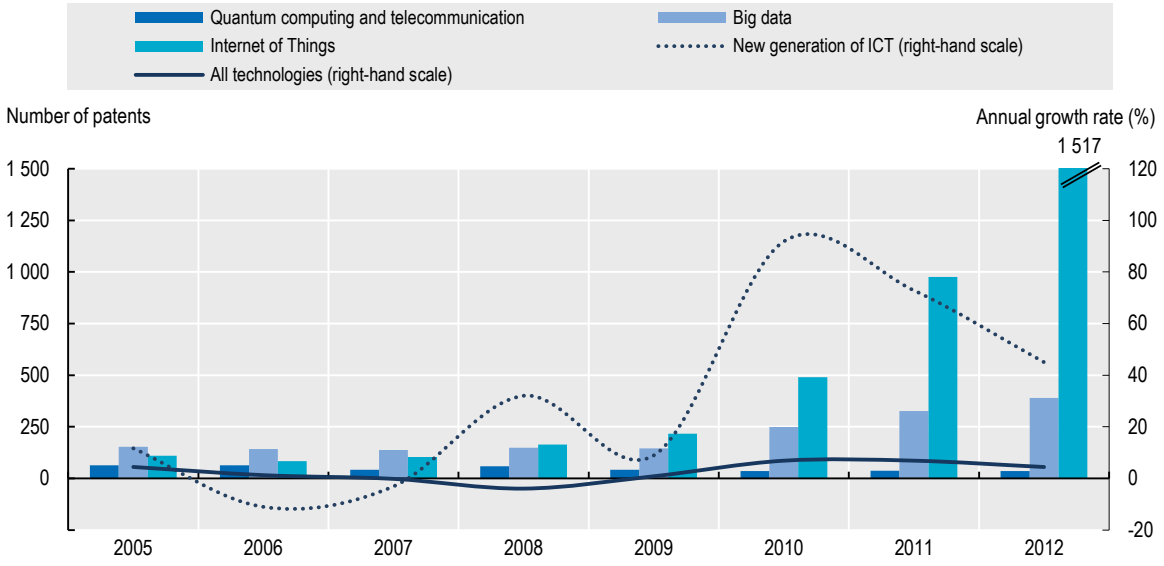
Source: OECD, *STI Micro-data Lab: Intellectual Property Database*, http://oe.cd/ipstats, October 2016.

Innovation in digital technologies underpins future growth of the Internet and Internet-based applications. These technologies often do not develop linearly, with rapid growth followed by periods of slower activity. Inventive IoT grew throughout 2006-12 (Figure 14). Quantum computing and telecommunication activities

seemingly established the basis for the development of other ICTs: patenting in the field peaked in 2006, fell and then stabilised. EU member states, especially the United Kingdom, led developments in quantum computing, whereas the United States led developments in both big data and the IoT. China increased its share of patents in both of these areas significantly over the period (Figure 15).

Figure 14. Patents in new generation of ICTs

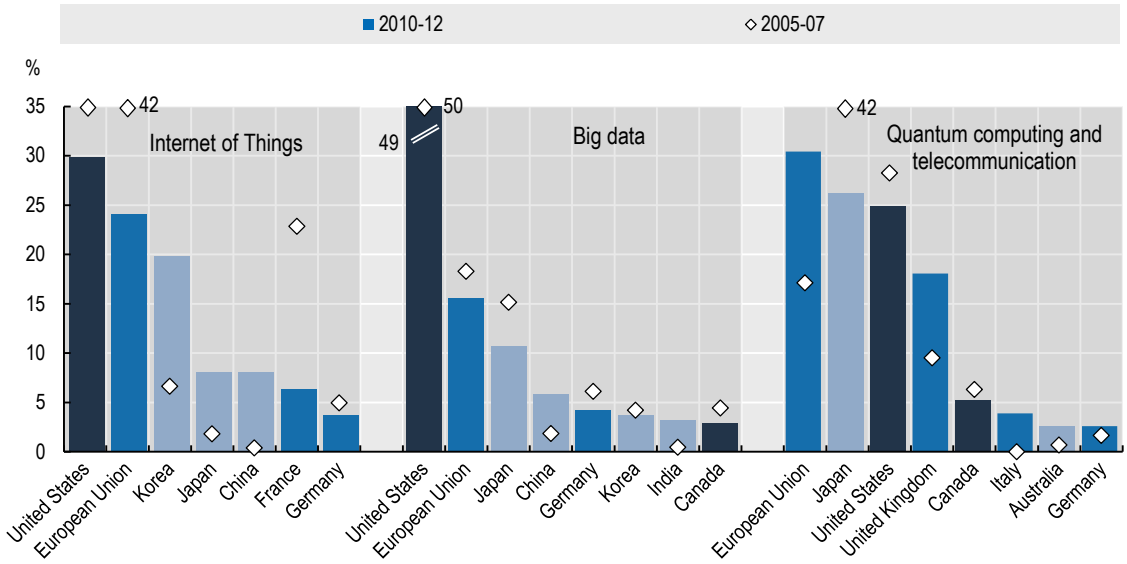
Number of IP5 patent families and annual growth rates



Source: OECD (2015d).

Figure 15. Top players in IoT, big data and quantum computing technologies, 2005-07 and 2010-12

Economies' share of IP5 patent families filed at USPTO and EPO, selected ICTs



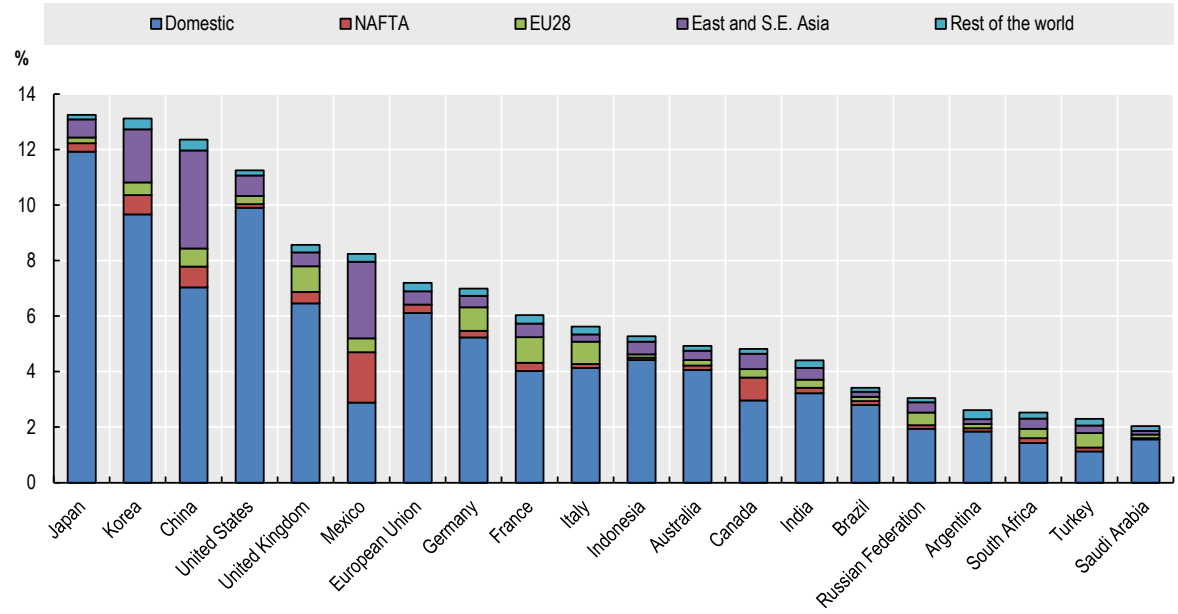
Source: OECD (2015d).

Digital technologies and services play an important role in the manufacturing sector, contributing to innovations. Figure 16 shows the value-added of ICT goods and services in total manufacturing exports, broken down into the domestic and foreign components (the latter is subsequently further decomposed into the regions from which the value added of ICT goods and services originate). The domestic value added

component may include repatriated income (profits) from multinational enterprises (MNEs). These data show that in value-added terms, ICT goods and services represent between 2% (Saudi Arabia) to 13% (Japan) of total manufacturing exports in G20 economies. Japan, Korea, China, and the United States are particularly strong exporters of manufacturing goods with significant ICT-related content.

Figure 16. Value-added of ICT goods and services in total manufactured exports

By country or region of value-added origin, 2011



Notes: ICT goods and services are approximated by ISIC Rev.3 Divisions 30, 32 and 33 for goods and 64 and 72 for services. EU28 excludes intra-EU28 exports. For EU28, domestic = EU28 origin. East and Southeast Asia comprises Brunei Darussalam, Cambodia, China, Chinese Taipei, Hong Kong (China), Japan, Korea, Indonesia, Malaysia, Philippines, Singapore, Thailand and Viet Nam.

Source: OECD, *Trade in Value-Added (TiVA) database*, "Origin of value-added in gross exports (by source country and industry)", http://oe.cd/tiva, 2015.

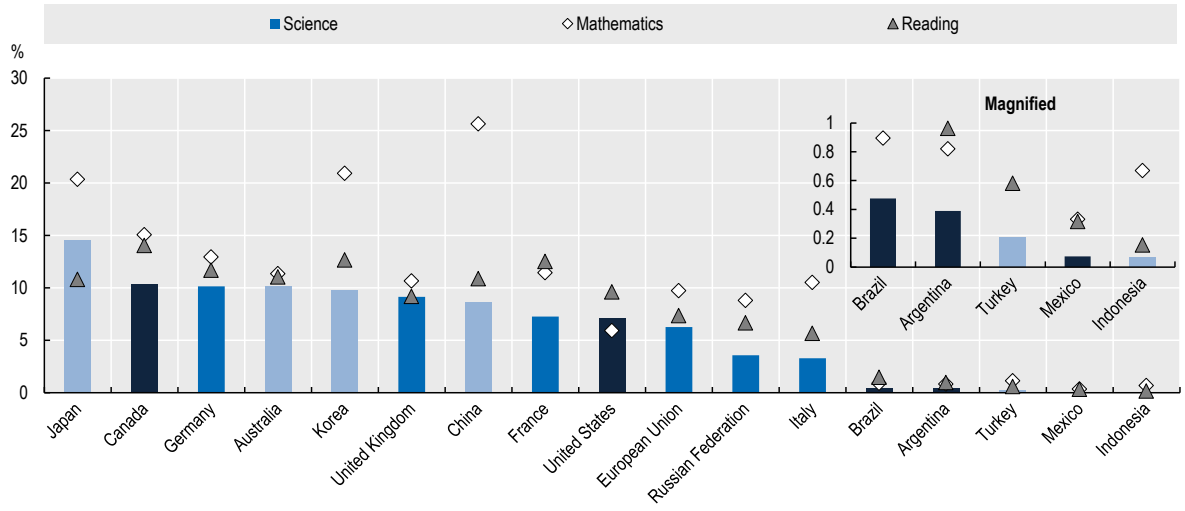
Skills needed to participate in the digital economy

New approaches to education, training, re-skilling, skills use throughout the economy, and adjustment assistance to meet the fast-changing demand for new skills, will be key to maximising the benefits of a digital and inclusive economy and society today and in the future. Basic skills will be important, as will digital and science, technology, engineering and mathematics (STEM) skills and variants such as data analytics, programming and network deployment and maintenance, and softer skills associated with content creation, design, organisational change and entrepreneurial creativity.

With respect to basic skills, evidence suggests that overall science, reading and mathematics performance differs significantly across G20 economies. Performance in mathematics is significantly above reading and science performance for some G20 economies, including China, Indonesia, Korea and Japan, and slightly higher in several others, including Germany, Canada, the United Kingdom, Italy and the Russian Federation. For many others, all three indicators are broadly aligned, albeit with differences across countries, in part linked to levels of overall economic development (Figure 17).

Figure 17. Science, reading and mathematics proficiency at age 15, 2015

Percentage of top performers

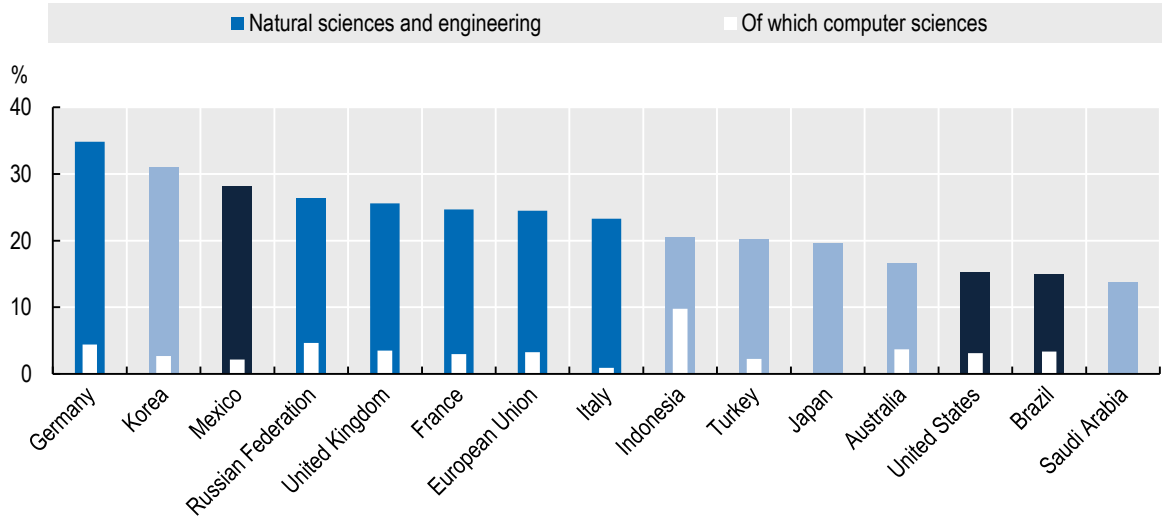


Source: OECD, *PISA 2015 Database*, December 2016.

As people move up the education ladder towards more specialised skills, evidence shows that all countries produce relatively more tertiary graduates in natural sciences and engineering than they do computer science graduates. Germany leads at 35% of all tertiary graduates in natural sciences and engineering, followed by Korea (31%) and Mexico (28%). With respect to computer sciences, Indonesia leads at almost 10% of all tertiary graduates, followed by the Russian Federation and Germany, both at around 4.5% (Figure 18).

Figure 18. Tertiary education graduates in natural sciences and engineering, 2014

Based on ISCED-11 fields, as a percentage of all tertiary graduates

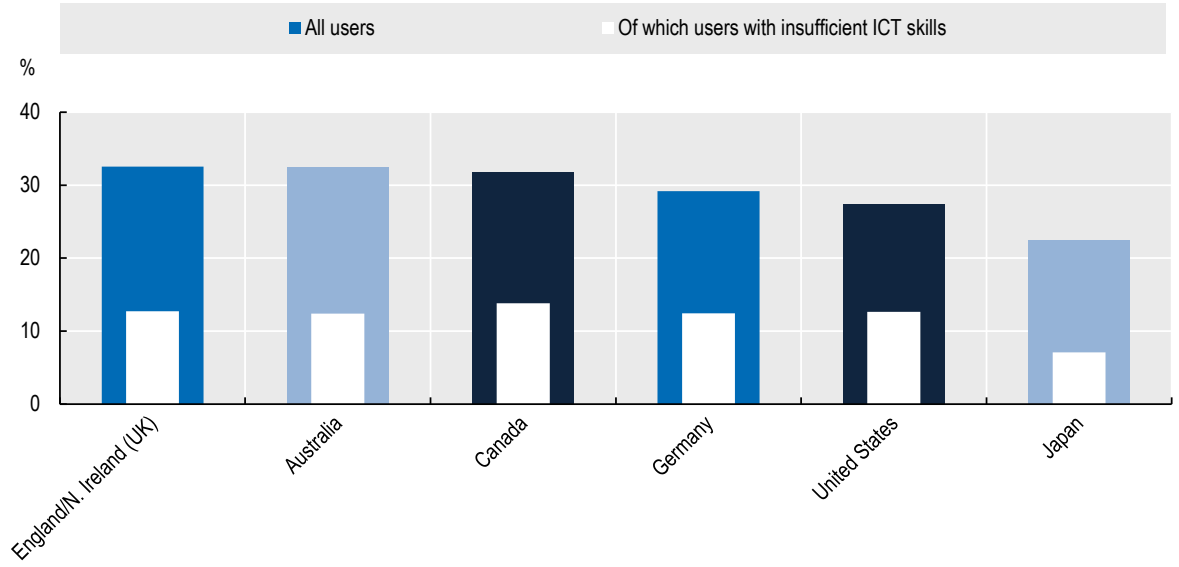


Source: OECD, *Education Database*, November 2016.

As digitalisation deepens, computer skills become increasingly important. On average, only a quarter of all workers use office software daily (Figure 19). Of these, according to the OECD Survey of Adult Skills (PIAAC), a considerable share of workers may lack the skills to use these tools effectively. This could be worrisome unless better software and artificial intelligence help overcome these problems and reduce barriers to computer use as there is no plausible future in which computer use will decline (indeed, it is more likely that reliance on

computers will rather increase). At the same time, "digital natives" are on the rise. On average, 15-year-olds in a range of G20 economies spend about three hours per day on the Internet on a typical weekday.

Figure 19. Workers using office software at work every day, 2012



Notes: Problem Solving in Technology Rich Environments (PSTRE) assessment data for France, Italy and Spain are not available and not included in the average. Individuals in the following categories of the PSTRE assessment are excluded from the analysis: "No computer experience"; "Opted out of computer based assessment"; "Failed ICT core/Missing".

Source: OECD, based on *PIAAC Database*, January 2016.

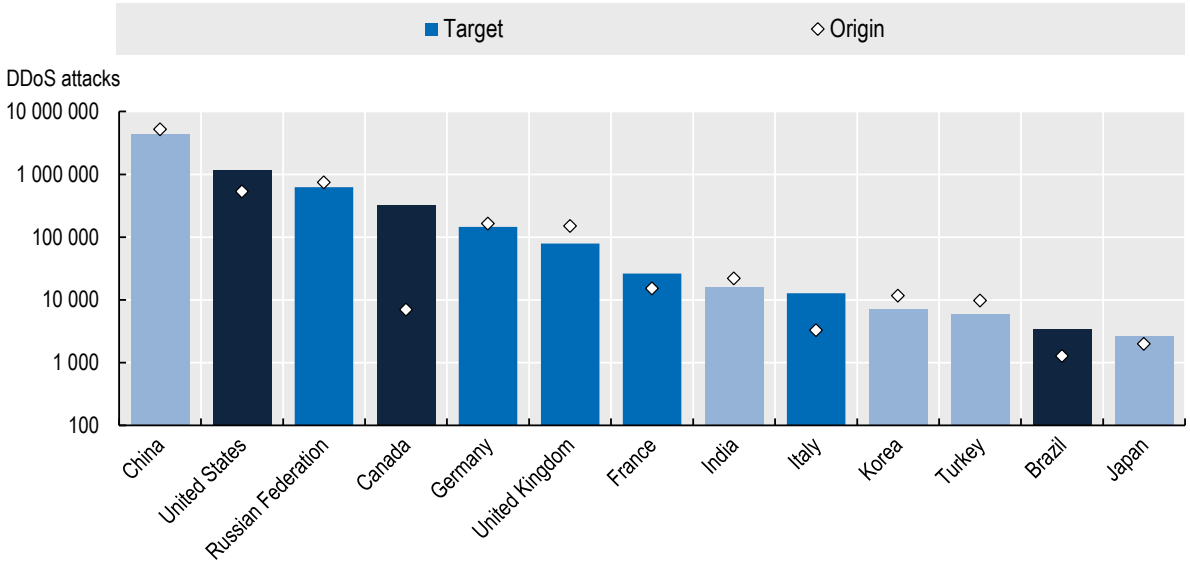
Trust in the digital economy

To realise the potential of the digital transformation for growth and well-being, greater co-operation in developing coherent strategies for digital privacy and security, and implementing privacy and security risk management frameworks, are essential, as is the protection of consumers engaged in the digital economy through e-commerce and other activities. Issues around access to data, use and ownership of data, as well as safety, are particularly relevant as the IoT, and with it billions of interconnected devices, becomes a reality.

Denial-of-service (DoS) attacks are a well-publicised and relatively common form of cyber-attack. These attacks aim to make machines or network resources unavailable by interrupting or suspending the services of a host connected to the Internet by flooding the host site using multiple machines, often remotely controlled via malware. In general, large firms are more prone to DoS attacks. At the global level and in absolute terms, China, the United States and the Russian Federation lead both in terms of DoS attacks originating from or targeting each geographical area (Figure 20). These measures are highly correlated, suggesting to some extent the domestic nature of many attacks. Exceptions include Canada, Italy, and Spain, which receive many more attacks than they originate.

Figure 20. Distributed denial-of-service attacks originating from or targeting each geographical area, April 2014

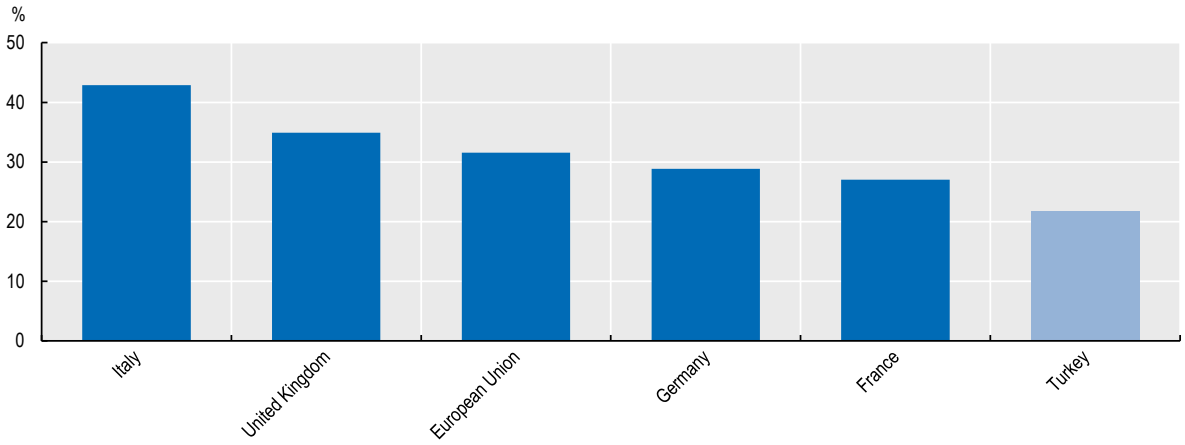
Numbers based on the location of command and control points, logarithmic scale



Source: OECD (2014b).

Another trust-related metric includes the share of firms that that have a formally defined policy that deals with digital security. On average, just over 30% of all EU firms had such a policy in place, compared to just over 20% in Turkey (Figure 21). While currently available only for some European countries and Turkey, this data underscores that while challenging, it is possible to develop trust metrics with the active support of governments in carrying out the relevant firm-level surveys (see Box 2).

Figure 21. Businesses with a formally defined ICT security policy, 2015



Source: Eurostat, November 2016.

BOX 2. MEASURING TRUST IN THE DIGITAL ECONOMY

The risk related to cybercrime and digital security incidents moved into the top five global business risks in 2015 (in 2014, cyber risks ranked 8th and in 2013 just 15th), according to the fourth annual Allianz Risk Barometer Survey (Allianz, 2015). In the World Economic Forum's Global Risks 2015 report, digital risk is firmly positioned as a major risk in terms of likelihood and effect (WEF, 2015a). It is recognised as one of the top commercial risks along with geopolitics, the environment, and the economy.

Digital security risk is a concern that the entire business community shares, but it represents an especially serious threat to smaller businesses. While large businesses and organisations may have the institutional and financial capacity to develop appropriate digital security risk management, studies in a number of countries suggest that SMEs, and particularly micro-enterprises, face managerial and financial resource constraints that make the implementation of digital security risk management practices often a secondary preoccupation.

Data limitations, definitional problems and the lack of appropriate sets of indicators are thus a severe constraint in measuring digital security and privacy risks today. In particular, for many of the hypothesised modes by which firms' "bottom line" might be affected by a digital security incident, there is little or no available data which is sufficiently robust and comprehensive to be used with a high degree of confidence for public policy making. Where international surveys exist, they do not take account of how businesses are managing digital security risks or the effectiveness of digital security risk management practices.

While there is a need to develop new and better metrics to better understand the digital economy, the security and privacy areas are particularly urgent. The OECD aims to help address this gap by undertaking work to better measure security and privacy over the 2017-18 period.

Part 2

IDENTIFYING AND ADDRESSING POLICY CHALLENGES ARISING FROM DIGITALISATION

1. ACCESS TO DIGITAL TECHNOLOGIES AND SERVICES

- Despite the rapid spread and uptake of digital technologies, adoption and use vary among G20 economies, demographics, industries and by firm size, raising concerns about the inclusiveness of the digital transformation.
- While G20 economies vary, barriers to the access and effective use of digital technologies typically include some combination of a lack of high-quality and affordable infrastructure; a lack of trust in digital technologies and activities; a shortage of the skills needed to succeed in the digital economy; a more reactive than proactive approach to the openness of the Internet; services trade barriers; high costs and poor access to financing for smaller firms; barriers to the reallocation of resources across firms and sectors; and a lack of interoperability of standards.
- These barriers can be overcome or ameliorated by developing and implementing comprehensive national digital strategies; enhancing competition in telecommunication markets and improving Internet access for disadvantaged groups, SMEs and regions; elevating the importance and clarifying the objectives of policies and practices to address digital security and privacy risks; reducing firm-level barriers and enabling complementary investments; ensuring life-long learning mechanisms to improve workers' skills; ensuring Internet openness and cross-border data flows; and fostering robust firm dynamics within the economy.

1.1. The policy challenge

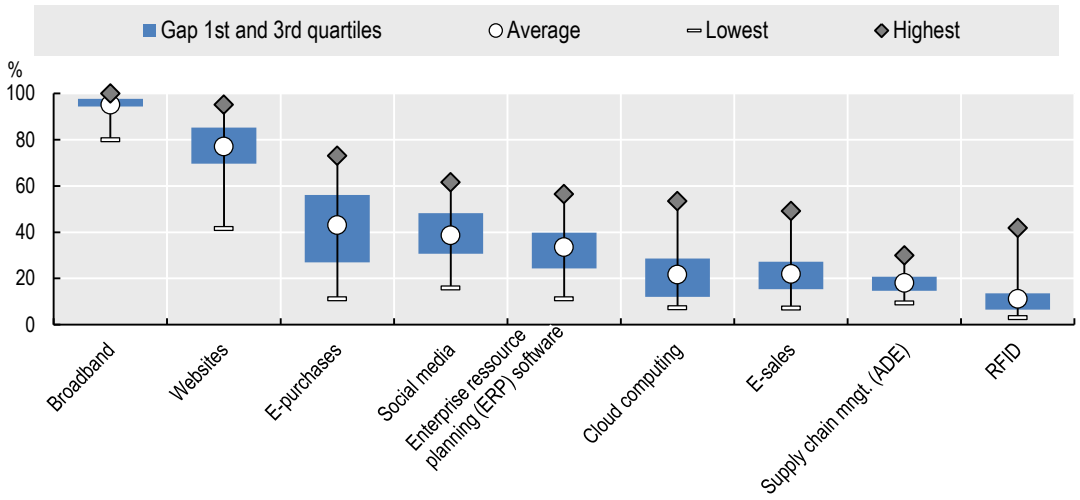
Digital technologies have spread rapidly over the past 20 years, with a large share of the population in G20 economies now having access to fixed or mobile broadband networks, and firms often using several digital applications throughout their businesses (see Part I on digitalisation indicators). Developments in mobile technologies have also enabled people to conduct daily personal computing and communications activities on-the-go. Nevertheless, there is still considerable variation across and within G20 economies in the access of people and firms to digital technologies and services.

The variation within G20 economies across different population groups appears largely linked to incomes, levels of education, age, and region, with gender differences typically playing a more limited role. Many lagging G20 economies have made strong progress in reducing these gaps in the past decade, in large part due to advances in mobile broadband availability. Data on Internet access by income quartiles also show that the diffusion process has also advanced substantially for low-income households in many countries (OECD, 2016c). As the benefits of digital technologies increase with the number of people and firms connected, increasing access and ensuring that all are able to benefit from these technologies and their many applications and services is an important challenge for policy makers.

Within countries, differences across firms appear mainly linked to firm size, but they are also affected by the sectoral composition of the economy. Moreover, while broadband access and basic applications such as websites are common among most firms, more advanced applications, such as enterprise resource planning (ERP) software and radio-frequency identification (RFID) are used by a much smaller share of firms (Figure 22), perhaps in part because a lack of workers with the skills to use these technologies effectively, but also as these applications require a much greater transformation of business processes.

Figure 22. Diffusion of selected ICT tools and activities in enterprises, 2015

Percentage of enterprises with ten or more persons employed



Notes: The data used to construct this figure include 31 OECD economies and the EU28.

Sources: OECD, *ICT Database*; Eurostat, Information Society Statistics Database; national sources, April 2016.

As highlighted in Part I on digitalisation indicators, the uptake of digital technologies remains particularly low among small firms even for technologies that seem particularly relevant for SMEs, such as cloud computing, or for particular industries, such as ERP in manufacturing.

1.2. Potential benefits from enhanced access to and use of digital technologies

As discussed in Part 1 of this report, enhancing access for households and individuals is related to the significant potential of digital technologies to increase incomes and social well-being, and promote social inclusion. Digital technologies can create better access to quality education and offer new opportunities for skills development, for example by expanding access to knowledge for people from low-income backgrounds or disadvantaged areas, supporting new pedagogies with learners as active participants, fostering collaboration between educators and between students, and enabling faster and more detailed feedback on the learning process (OECD, 2014a).

Digital technologies can be particularly important to help connect disadvantaged groups (OECD, 2016d). For example, mobile connectivity is helping reach remote populations as well as those with lower incomes due to its low costs. Pantea and Martens (2014) find that low-income users spend even more time on the Internet than the average, browsing websites that deal with education, career opportunities, health and nutrition, and e-commerce platforms. Potential benefits for low-income groups also relate to improved access to free or low-cost knowledge and information; services that allow consumers to negotiate better prices for products (as well as identify better quality products); as well new consumption opportunities offered by Internet-based platforms, such as peer-to-peer platforms that lower the barriers for individuals to rent, swap, share, barter, lend, exchange and sell goods and services among themselves.

Digital technologies also offer new opportunities for firms, including in lowering important barriers to entry. For example, digital technologies can facilitate cross-border e-commerce and participation in global value chains (GVCs) (e.g. Skype for communications, Google and Dropbox for file sharing, LinkedIn for finding talent, PayPal for transactions, and Alibaba and Amazon for sales). Enhancing access to networks and enabling SMEs to engage in e-commerce can be an effective way for small firms to go global and even grow across borders where they can become competitors in niche markets. For example, M-Pesa, a Kenyan mobile-money service, is now active across Africa as well as South Asia and Eastern Europe.

Digital technologies are also transforming industrial production. They make the sector more productive through automation and robotics, can help reduce disruptions caused by the breakdown of machines (e.g. through automated maintenance) and reduce the need for assembly at some stages (e.g. through 3D printing) (OECD, 2016c). One US provider of laboratory services estimated that "predictive maintenance of assets [can save] up to 12% over scheduled repairs, reducing overall maintenance costs up to 30% and eliminating breakdowns up to 70%" (Sullivan et al., 2010; cited in Daugherty et al. 2015). And more prolific use of digital technologies within production is moving this sector increasingly into service provision, creating new business opportunities. For example, Rolls-Royce has shifted from a product, time and service to a service model that has been trademarked "Power by the Hour" (OECD, 2016a).

The Internet also enables firms, particularly SMEs, to maximise the benefits of digital technologies. For example, the Internet helps firms access markets they could not have otherwise reached, find workers with the particular skills they need, engage in new forms of financing (e.g. crowdfunding), and access technologies they may not have been able to buy directly (e.g. via cloud computing), among others. Chapter 8 on SMEs discusses in more detail the benefits of digital technologies for SMEs.

1.3. Key barriers to access and use

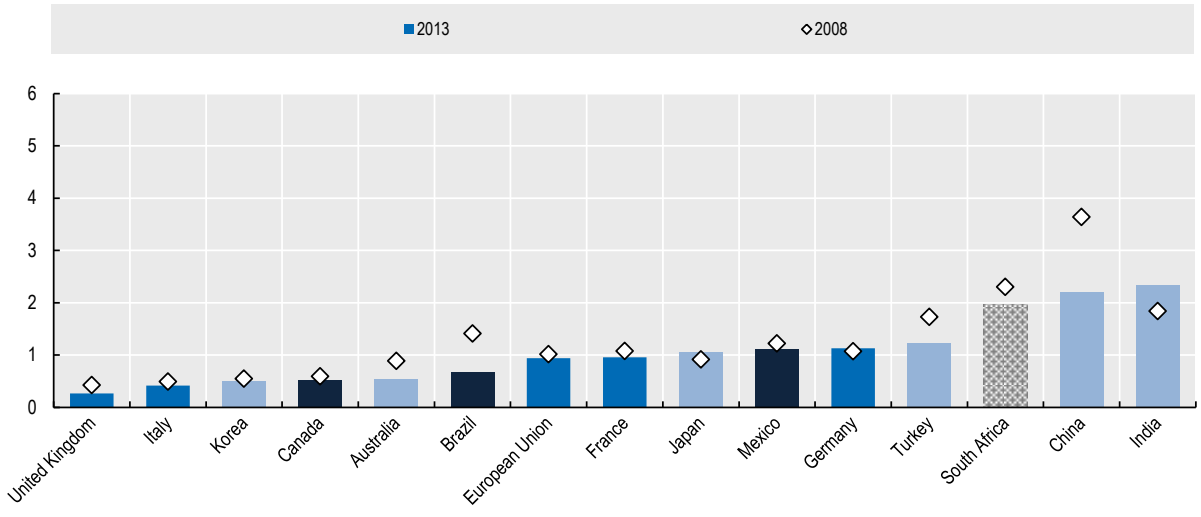
Despite the many potential benefits for firms, households and individuals, the uptake and use of digital technologies still lags for many groups and in many countries. This is due to a range of barriers, some of which can be ameliorated by policy action, both at a national and global level.

Quality and cost of accessing networks

For both firms and households, the spread of high-quality broadband networks and the quality and cost of accessing these networks are particularly important. This is linked to the state and diffusion of broadband networks in a country and the degree of competition in the market. Policies that help encourage the diffusion of networks to all regions and households and that encourage competition are therefore essential.[1] The relative restrictiveness of regulation in the telecommunication sector is important in this regard. Data suggest considerable remaining differences in the degree of regulation in the telecommunications sector across G20 economies, although the restrictiveness of regulation has fallen in many countries over the past years (Figure 23).

Figure 23. Sectoral regulation in the telecommunications sector, 2008 and 2013

Index scale of 0 to 6 from least to most restrictive

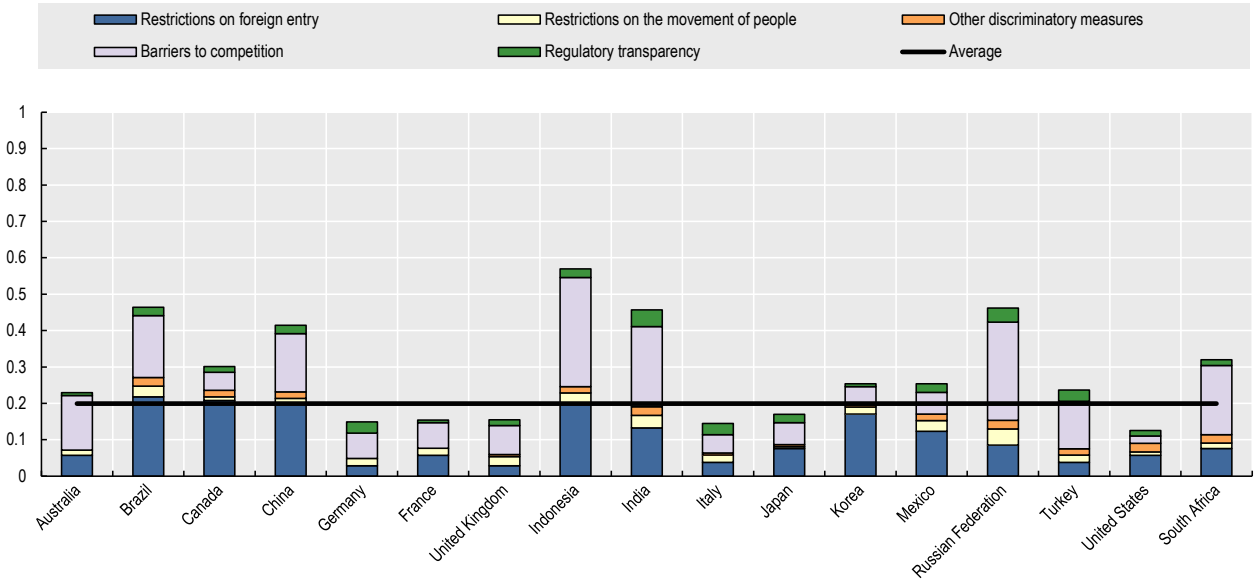


Source: OECD, *Product Market Regulation Database*; Koske et al. (2015).

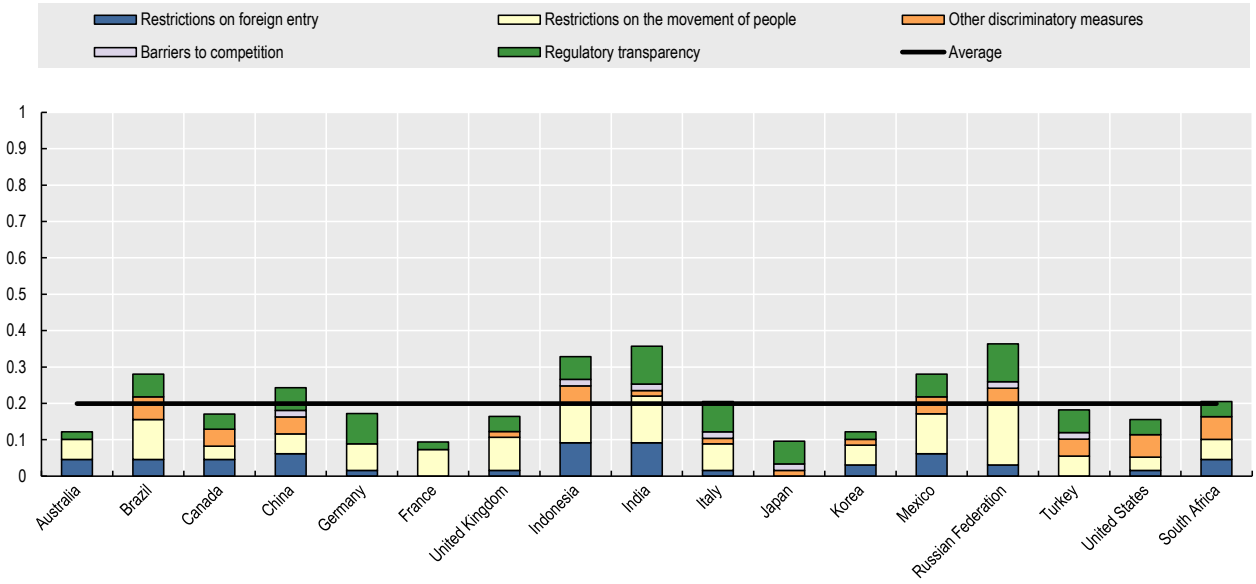
Research has shown that the availability and quality of telecommunications and transport services are strongly related to competitiveness in manufacturing. For instance, more Internet connections are associated with more exports of branded goods at higher prices in several manufacturing sectors, most notably electronics. Estimates suggest that an increase in telecoms density of 10% is associated with between 2% and 4% higher export prices in the electronics sector, and an increase in intra-industry trade in the sector by between 7% and 9%, depending on the initial density (OECD, 2014c). Research using the OECD Services Trade Restrictiveness Index shows considerable differences across G20 economies, in both Telecommunications and Computer Services (Figure 24). The analysis of this data suggests a strong relationship between the services trade restrictions in the telecommunications sector and performance. By implication, more open and better regulated telecommunications result in more competitive manufacturing (OECD, 2014c).

Figure 24. Services Trade Restrictiveness Index, 2015

a) Telecommunications



b) Computer services



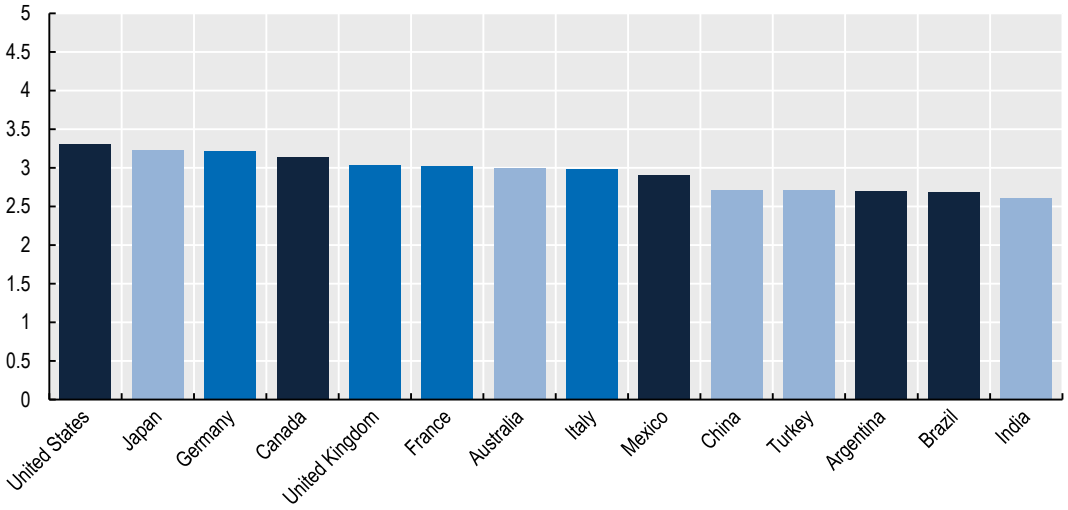
Notes: The Services Trade Restrictiveness Index (STRI) indices take values between zero and one, one being the most restrictive. They are calculated on the basis of the STRI regulatory database which records measures on a most-favoured-nation basis. Preferential trade agreements are not taken into account. The data have been verified by OECD countries and the Russian Federation.

Source: OECD, *Services Trade Restrictiveness Index Database*, www.oecd.org/tad/services-trade/services-trade-restrictiveness-index.htm.

Management

Another challenge at the firm level is management, including the ability of managers to take risks and engage in restructuring. Research shows that implementing and realising the full productivity benefits from new technologies (such as ICT) entails significant organisational restructuring, which requires considerable managerial skill (Bloom et al., 2014). Higher managerial quality raises within-firm productivity (Bloom, Sadun and Van Reenen, 2012) while better managed firms may also be better able to address skills challenges within the firms, e.g. in screening job applicants, developing new work practices, internally reallocating overskilled workers, and retraining or removing under-skilled workers. Competition and product market regulations are a key determinant of managerial quality, but competition may be less effective at facilitating the exit of poorly managed family-owned firms to the extent that they may be subsidised by their family owners through cheap capital (Bloom et al., 2014). Available estimates show considerable variation in management scores across G20 economies (Figure 25).

Figure 25. Average management scores for G20 economies



Notes: Unweighted average management scores, survey waves pooled (2004-2014). The scores can range from 1 (lowest management score) to 5 (highest).

Source: Bloom, Sadun and Van Reenen (2016).

Privacy and security

Increasing connectivity and data-intensive economic activities – in particular those that rely on large streams of data (big data) and the emerging IoT – have the potential to foster innovation in products, processes, services and markets and help address social and global challenges. For example, in the manufacturing sector, sensor data is being used to monitor and analyse the efficiency of machines to optimise their operations and to provide after-sale services, including preventive maintenance (OECD, 2016e). But these developments are accompanied by a change in the scale and scope of digital security and privacy risk with potential significant impacts on social and economic activities.

The growth of digital security risks to economic and social activities, including risks to the security of data assets, as well as concerns that privacy and personal data protection is being violated, reinforces the importance of lack of trust in digital technologies and activities as another barrier to adoption and use of digital technologies by firms, households and across society. These concerns will only become stronger with the introduction of newer, more advanced technologies and processes (e.g. cloud computing, data analytics, IoT) that will in turn raise additional challenges – most notably related to safety and liability.

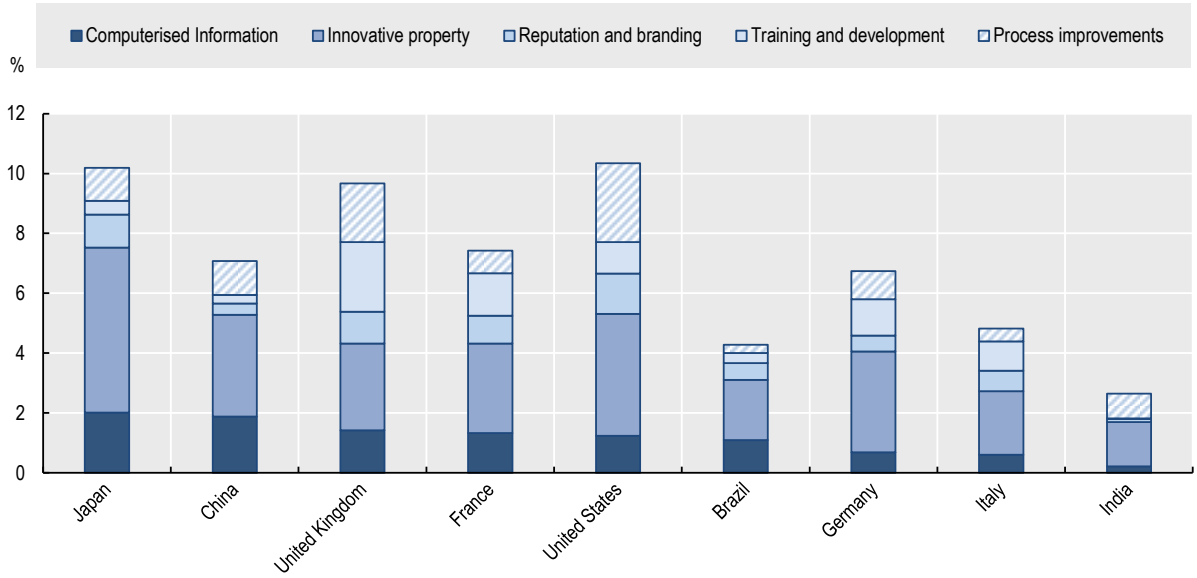
Skills, education and complementary assets

Skills and education also matter in how digital technologies are used. For households and individuals, activities such as sending emails, searching product information, or social networking show little variation across countries. However, the shares of Internet users performing activities usually associated with a higher level of education (e.g. those with cultural elements or more sophisticated service infrastructures) tend to show larger cross-country variability. This is the case, for example, for e-banking, online purchases, news reading and e-government. While users with tertiary education perform on average 7.3 different activities, those with lower secondary education perform only 4.6 activities (OECD, 2016f). Education therefore plays a key role in shaping the range of activities on the Internet.

Available evidence for G20 economies shows that there are large differences in the degree of complementary investment in training and process improvements, compared with investment in ICTs (World Bank, 2016) (Figure 26). More recent estimates for OECD countries (OECD, 2015d) show that the share of investment in

these complimentary knowledge-based assets has continued to grow in many countries, and that such investment showed great resilience during the economic crisis.

Figure 26. Investment in ICTs relative to complementary investment, 2006

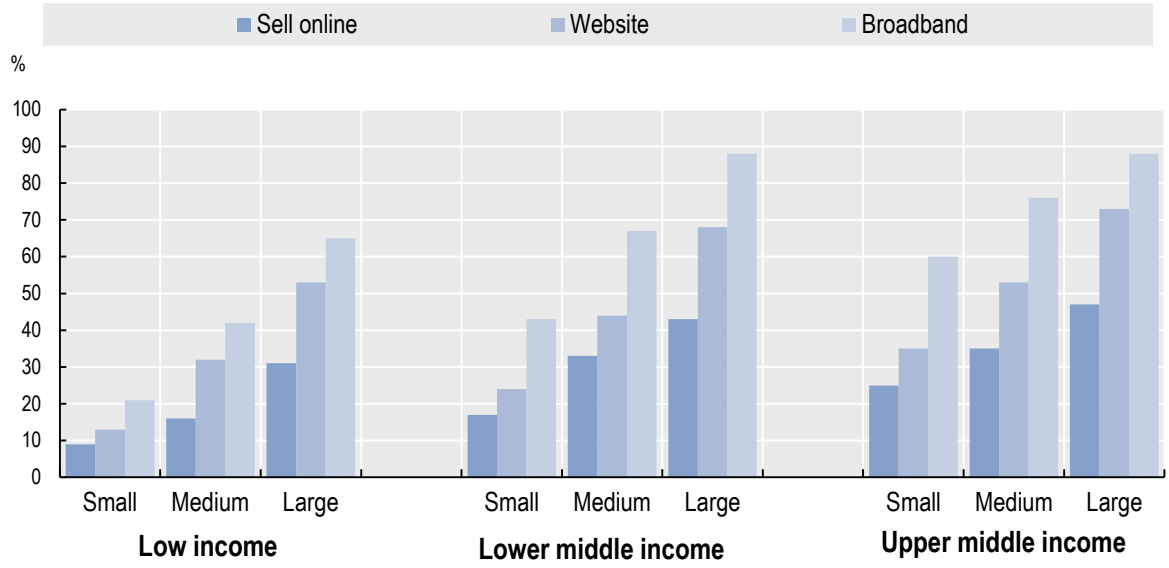


Source: World Bank (2016).

Particular barriers for SMEs

At the firm level, where many large firms use digital technologies quite widely, barriers to access and use are particularly prevalent for SMEs. SMEs lag large firms in their use of digital technologies at every level of economic development (Figure 27). For these firms, the cost of digital technologies, combined with a lack of adequate financing, are important barriers that help explain why they are less likely to adopt digital technologies. Such costs do not just involve the digital technologies themselves, but also the associated costs and investments needed to ensure successful implementation, e.g. costs of related services, investment in training and in process innovation.

Figure 27. Large firms use the Internet more intensively across all income groups, 2006-14



Source: World Bank (2016).

Recent research points to a set of additional challenges for smaller firms: (i) reluctance of managers to adapt to technological change, possibly due to a lack of knowledge, time or mistrust; (ii) a view of the Internet mainly as a tool for cutting costs rather than for expanding markets and commercial opportunities; and (iii) lack of ICT skills and expertise, including lacking motivation or resources to train employees or to recruit specialists (Bordonada, Lucia-Palacios and Polo-Redondo, 2012; Consoli, 2012; OECD, 2010a; Tompson et. al., 2011).

Analysis of the uptake of e-commerce among SMEs, in particular across borders, confirms these barriers and highlights some additional ones. One-third of Internet users in the European Union cite worries about security as their primary concern (OECD, 2014b), with the legal and regulatory framework influencing the level of trust online (UNCTAD, 2016). Consumer mistrust also stands in the way of cross-border purchases, confirming the importance of trust for tapping into the great potential of cross-border e-commerce. In addition, several supply-side obstacles are important, notably trade and regulatory barriers. Some of the most common barriers to foreign market access, including via e-commerce include:

- High customs administration and shipping costs, which obstruct in particular long-tail economic transactions, and thus affect the ability of SMEs to engage in electronic commerce (although they may have less impact on digital goods and services),
- Inadequate property right protection, including copyrights, patents and trademarks, and
- Shortage of working capital to finance exports, information to locate and analyse markets, and managerial time, skills and knowledge (OECD, 2009, 2016g).

Policy measures to reduce these barriers will especially benefit SMEs, which tend to have limited resources and skills to tackle obstacles. At present, SMEs rely increasingly on e-commerce intermediaries and marketplaces such as Alibaba or Amazon. While these intermediaries make it easier for SMEs to access foreign markets and benefit from large network effects and economies of scale, the key role of online intermediaries in online and mobile markets may result in SMEs becoming dependent on such players. Moreover, this risks limiting the potential impact of digital technologies on business transformation. The G20 Trade and Investment Working Group, when discussing the potential of digital trade, will also pay special attention to particular barriers for SMEs.

The openness of the Internet and cross-border data flows

Approaches to dealing with Internet openness also play an important role in enabling access to the full spectrum of goods, services and information available through the Internet (OECD, 2016f). Openness underpins the ability of the Internet to act as a connector on a massive scale. This is what provides opportunities to share, access and co-ordinate knowledge, leverage platforms for new ventures, and source inputs ranging from finance to professional services. Countries and other stakeholders may have different preferences concerning Internet openness, depending on their objectives and their assessment of the benefits and challenges that come with preserving openness. Broad public policy objectives that can affect Internet openness in one way or another include protecting competition, consumers and privacy, and promoting economic development, cultural preservation and Internet access.

Ensuring the free flow of data across border is also important since data can now be accessed from almost any location. Trans-border data flows over the Internet enable firms to co-ordinate their participation in global value chains and have empowered even micro firms to engage in trade. Data show that the now defunct Safe Harbor framework governing data flows between the European Union and the United States was used by a wide variety of firms, with firms from 103 different industries certifying to Safe Harbor at some point from 2000 to mid-2015 (OECD, 2016f). Over half the firms had fewer than 100 employees, highlighting how data flows matter for SMEs (OECD, 2016f).

Recent technological developments have radically altered current data flows. In examining international data transfers that occur today, three main changes can be noted: change in scale, change in processing and a change in management. The role of the individual in these flows has also evolved. Whereas in the past, data transfers tended to be business-to-business or government-to-government, changes in technology and practices have increased the scale of those transactions, and have fostered new business-to-consumer, government-to-consumer, and even consumer-to-consumer relationships. Individuals going about their day-to-day activities online may routinely, and often unknowingly, generate transborder data flows. Organisations offer storage and processing services at a distance to individuals, migrating e-mail, pictures, videos, and documents away from the personal computer and to third-party servers. This allows individuals to have convenient access anywhere in the world where there is Internet access, but it also highlights the costs of barriers to cross-border data flows.

Barriers specific to Industrie 4.0 and the IoT

Challenges highlighted in this chapter, for example access to high-quality infrastructure and skilled labour, are relevant to the digitalisation of production systems, commonly referred to as the Industrial Internet or Industrie 4.0. To be successful, given that adoption of more sophisticated digital technologies (e.g. ERP, RFID) lags more universal applications such as websites, more needs to be done to encourage investments in complementary knowledge-based assets, such as new skills, organisational changes and new business models. In turn, this may require the realignment of framework policies, including product market regulations.

Beyond improving the overall diffusion of digital technologies across production industries, policy measures to address inconsistent data governance frameworks and barriers to interoperability and standards should be considered. Regulations, and their implementation, could also be reviewed to assess their capacity to deal with the complexity of new issues related to liability, competition, privacy and consumer protection (OECD, 2016c). Chapter 4 will discuss in more detail the issues around standards, particularly with respect to Industrie 4.0, and Chapter 6 will look at digital security and data protection more closely.

1.4. *Key areas for policy action*

The discussion in the preceding section points to some productive areas for policy actions that could help enhance access and use of digital technologies. The following areas are particularly important.

Enhancing competition in telecommunications markets

Lack of access to digital infrastructures at competitive prices is often the first key barrier for firms to access and use digital technologies. In particular, access to digital technologies such as (mobile) broadband, including in rural and remote areas, as well as access to data which are becoming an infrastructure for data-driven innovation, are crucial. High-speed broadband is the underlying infrastructure for the free flow of data that enables and fuels digital services. Mobile broadband is essential, as smart mobile devices are becoming a key platform for digital innovation. Moreover, high-speed mobile broadband is especially important to further improve connectivity in remote and less developed regions. The drop in mobile access prices, mainly thanks to enhanced competition, is the prime factor behind the explosion of mobile subscriptions, and calls for continuous efforts to strengthen competition in the telecommunication services markets (OECD, 2014d, 2016d).

The most effective way for policy to facilitate the use of networks by SMEs is improving access, which requires sound policies in the telecommunication area, with a strong focus on competition and fair access. Specifically it is critical to stimulate investments in broadband, smart infrastructure and the IoT as well as in data and analytics with a strong focus on SMEs and high value-added services (i.e. data analytic and data-driven services). Governments should promote digital technologies as general-purpose platforms for innovation and

knowledge sharing by upholding the open, free, decentralised and dynamic nature of the Internet. At the same time, policy makers must assess market concentration and barriers to competition. ICT-driven innovation is challenging traditional approaches to ensuring competition.

Developing and implementing comprehensive national digital strategies

Over the last decade, governments have recognised the importance of addressing the digital economy in a more holistic manner through the development of national digital strategies. National strategies have the flexibility of being able to address both the supply and demand sides of the digital economy through mixes of policies and programmes. Effective strategies generally aim to promote and grow the ICT sector, strengthen trust and e-government, advance e-inclusion and the adoption of digital technologies, improve digital skills and education as well as tackle global challenges such as Internet governance, climate change and development co-operation (OECD, 2015a).

These strategies often exist in parallel with other, more targeted national strategies. For example, while good telecommunications policies are at the core of many of these strategies, many governments also have national broadband strategies more specifically aimed at connecting remote areas and lagging groups in the populations. Such policies can enable such regions and groups to participate and benefit from the digital economy. Another example is national cybersecurity strategies or currently developed national digital security risk management strategies. The development of national privacy strategies in the future may also respond to the specific need to adopt a whole-of-society approach to ensuring privacy and data protection while providing the flexibility needed to take advantage of digital technologies for the benefit of all.

National digital strategies are focused on enabling the positive economic and social conditions necessary for development and growth. As such, they are cross-sectoral by nature and in many instances are designed to boost countries' competitiveness, economic growth and social well-being (OECD, 2015e). They allow governments to set targets, generally related to infrastructure deployment or growth of a sector, and objectives, generally more aspirational, which drive the deployment of digital technologies and infrastructure throughout the economy. These targets and objectives can be set at both the national and international levels. Consistency with broader international digital agendas, such as the G20, reinforces a country's domestic agenda and increases the possibility of meeting these targets.

Addressing privacy and security

The rapid spread of digital technologies has been accompanied by a change in the scale and scope of digital security and privacy risks with potential significant impacts on social and economic activities. These developments underscore the need for an evolution in policies and practices to build and maintain trust (OECD, 2016c). SMEs and early-stage start-ups in particular 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 that they have robust digital security and privacy practices may have a competitive advantage when seeking partnership opportunities with larger organisations. In order to help SMEs realise these opportunities, it is essential to increase SMEs awareness and promote adoption of good practice. Useful approaches include the development of SME-specific risk management guidance tools and incentives, for example, by leveraging digital risk insurance.

Reducing firm-level barriers and enabling complementary investments

There are also several barriers at the firm level that affect the access and use of digital technologies. The effective use of digital technologies typically requires additional investments in complementary knowledge-based capital, in particular in (organisation-specific) skills and know-how, and in organisational change including new business models and processes. Many businesses, and in particular SMEs, therefore lack the necessary skills and know-how, and the financial resources to take advantage of digital technologies, and to introduce the changes needed for their productive use in businesses and across society.

Finance is a particularly important barriers for SMEs, who may not always have access to the necessary finance to make investments in digital technologies, although new sources of finance, including Internet-based financing, and the buying of Internet-based services (including cloud computing) can help mitigate this problem. Policies that strengthen SME financing, developed further in Chapter 3, can therefore play a useful role in strengthening access and use of digital technologies by firms.

Improving skills

Skills are clearly an important factor in the uptake and effective use of ICTs. Evidence suggests that despite increasing diffusion of digital technologies in business, a large proportion of people do not effectively use digital technologies at work or do not have adequate ICT skills (OECD 2015g, 2016g). On average, only 25% of individuals use simple office software, e.g. word processors and spreadsheets, every day at work. Among them, over 40% do not appear to have sufficient ICT skills to use these tools effectively, according to the OECD Survey of Adult Skills (PIAAC). Low proficiency in ICT skills risks limiting individuals' access to many basic services, better-paying and more-rewarding jobs, and the possibility of participating in further education and training. At the national level, if large proportions of the adult population have low proficiency in information-processing skills, the introduction and adoption of productivity-improving technologies and work organisation may be hampered. That, in turn, could stall improvements in productivity diffusion and living standards. These life-long learning skills will also be essential for navigating the digital transformation and structural changes it will induce.

Ensuring that everyone has the relevant skills is therefore key to enhancing the uptake and use of digital technologies and turning it into innovation, productivity and inclusive growth. However, what is becoming increasingly clear is that specialist technical skills are not enough to drive innovation. They need to be coupled with a range of other skills such as entrepreneurship, organisational know-how and design. At the same time, the take-up and diffusion of innovation needs people – as workers and as consumers – to have general skill levels that enable them to make the most of the benefits that innovation generates. This requires not only foundation skills such as literacy, numeracy and problem solving in technology-rich environments but also complementary socio-emotional skills such as openness to new experiences, adaptability, resilience, communication and teamwork, and ability to learn new skills. These same skills are also important to enable people to adjust to the possible negative impacts of innovation on their jobs and not only cope, but thrive, in a rapidly changing world. Addressing the skills challenge requires a broad strategy, that can be inspired by the OECD's Skills Strategy (2013), but that needs to be tailored to the specific needs of each country, and to the challenges that they face.

Ensuring firm dynamics within the economy

Slow overall take-up of digital technologies in an economy can also be affected by a lack of firm dynamics, which can lead to the coexistence of poorly performing firms, with very low levels of digital technology use, and star performers. This can result from a number of factors, such as barriers to firm exit and skill mismatch (OECD, 2016d). The opportunity cost of such barriers and mismatch can be large as at least in the short-to-medium-run, ICT-driven activities draw from a scarce and fixed pool of contestable resources, particularly

skilled labour. Thus, trapping resources in firms that are not able to turn ICTs into growth can hinder the growth prospects of more ICT-based firms (Acemoglu, et al., 2013). Costly delays and slow exit of such poorly performing firms, sometimes supported by government guarantees, and compounded by financial institutions that do not want to realise non-performing loans on their balance sheets, creates a particularly unfavourable environment for effective digital technology use in an economy, and will slow down the impact of ICTs on growth and productivity.

2. DIGITAL INFRASTRUCTURES

- It is essential that G20 economies continually invest in the development of digital infrastructures to meet existing and future demand. They provide the foundation for many new services, applications and business models. They are also crucial in underpinning and enabling the digital innovations that are transforming production, including in the context of Industrie 4.0.
- Key barriers to the deployment of high-speed networks and services include the nature of the infrastructure itself (monopolies, duopolies), which can give rise to high barriers to entry. In addition, geography, administrative barriers, regulatory uncertainty, and high capital expenditure, access to spectrum, and in some countries, a lack of basic infrastructure (e.g. electricity) particularly in rural areas, can be stumbling blocks.
- An important area for policy action involves establishing national broadband plans with well-defined targets and reviewing them regularly. These plans should ideally address all of the key barriers to the deployment of high-speed networks and services identified in the chapter, and include measurable targets to address the policy challenges associated with ensuring competition and investment and that the important technical enablers, such as access to Internet exchange points, spectrum, and take-up of IPv6, are in place.

2.1. The policy challenge

High-speed infrastructures are one of the main building blocks for digital economies, alongside content and applications. These infrastructures are composed of a multitude of local, national and global networks owned by different entities. They provide the foundation for many new services, applications and business models. They are also crucial in underpinning and enabling the innovation that is transforming production, including in the context of Industrie 4.0.

Moreover, the access afforded by Internet infrastructures brings societal gains, enabling new collaborative scientific and social networks, and supporting the free flow of information and knowledge, the freedom of expression, association and assembly, and hence the protection of individual liberties. Collectively, this infrastructure is increasingly a critical component of a democratic society and cultural diversity. For all these reasons, digital infrastructures need to be of high quality, accessible to all and available at competitive prices. It is essential that countries continually invest in the development of digital infrastructures to meet existing and future demand.

Demand for digital infrastructures

The increasingly central role of digital infrastructures to people's lives can be seen in the growth in global Internet traffic. According to Cisco's Virtual Networking Index, by 2020 global Internet traffic will be 92 times greater than in 2005 (Cisco, 2016). Traffic on broadband mobile networks is also rapidly increasing around the world. In OECD countries, the volume of mobile broadband data grew 71% between 2014 and 2015 (OECD, forthcoming a). Alongside access via cellular wireless networks, many users shift seamlessly to fixed connections during their day, with up to 80% of their additional smartphone data usage occurring over a Wi-Fi connection.

This underlines the complimentary nature of fixed and wireless digital infrastructures. Because all wireless access is at its core an extension of fixed networks or, conversely, fixed networks provide the backhaul[2] for

wireless access, the two technologies need to be developed together. This is a challenge for countries with less developed digital infrastructures because even when backbone networks are established, it is still necessary to ensure there is sufficient fixed network backhaul via intermediate links. This enables better performance over mobile cellular access and more efficient use of scarce spectrum.

As shown in Part I (digitalisation indicators), there is a range of networks, differences in the reach of these facilities, and extensive demand still to be met in G20 economies. Historically, some countries built broadband networks based on existing telecommunication or cable television infrastructures. During this period, higher penetration rates for telephony and cable television subscriptions in these countries enabled faster take-up of Internet access and subsequently the ability to more rapidly meet growing demand for fixed broadband access. Factors including population density, such as in Korea and Japan, or the challenge of providing services in an archipelago, such as Indonesia, also play a role.

While the gap between developed and emerging countries for 2G mobile services was overcome with unprecedented speed, new differences emerged as cellular wireless networks further developed to 3G and then 4G. Each of these generations required more backhaul to meet growing demand for data usage. This was easier where backhaul existed or could be upgraded based on demand from both fixed and wireless subscriptions. While an international standard is yet to be agreed for so-called 5G, it is widely expected that cells will be smaller and the need for improved backhaul even more essential than in previous generations.

Today, increased data usage is due to existing users downloading more data as well as more and more devices being connected to networks. In many G20 economies, a long-term decline in traditional fixed telephony subscriptions has been more than offset by growth in broadband connections for fixed, mobile and, more recently, M2M services, such as the ones used by smart meters and the automotive industry. The total figure for these telecommunication access paths in OECD countries reached 2.3 billion in 2015, an increase of 6.9% since 2013 (OECD, forthcoming a). While fixed and mobile broadband subscriptions increased in that two-year period in the OECD area (7.8% and 9.5% respectively), the most notable growth was the 47.8% increase in M2M subscriptions (OECD, forthcoming a).

Much of the future growth in demand for devices connected to digital infrastructures is expected to come from the IoT. Cisco's Visual Networking Index projects that M2M devices globally will grow from 4.9 billion in 2015 to 20 billion by 2020, i.e. more than 400% in five years (Cisco, 2016). The automotive industry is a case in point regarding IoT use and increased data generation. In-car Wi-Fi hotspots connected with 4G LTE have been introduced in a growing number of countries. In the United States, Chevrolet customers consumed more than 3 million GB of data in the two years to June 2016 (Chevrolet, 2016). While average US use per vehicle is currently less than the overall average per subscription to smartphones, this may not be so in the future.

Sensors are being used on board modern vehicles, for IoT communication between devices, to share information such as traffic and road conditions or parking spaces. Some of the data needs to be transmitted in real time, while other data can be offloaded to a fixed connection using Wi-Fi when a vehicle is garaged. The volume of data produced by semi-autonomous vehicles suggests that such IoT data usage will only increase with the advent of driverless cars. This automotive example is just one reason why the dramatic growth of IoT underlines the need for further developments in infrastructure to support them if policy makers are to achieve the goals they have in these areas.

A second promising area in relation to digital infrastructures and the IoT is the digitalisation of industrial production methods, including manufacturing plants (smart factories) and the way in which people, equipment, machines, logistic systems and products communicate and co-operate with each other (Platform Industrie 4.0, 2016). The digitalisation of supply chains and the availability of comprehensive, real-time information systems will enable companies to make manufacturing more efficient and flexible. Therefore, digital infrastructures that enable different forms of real-time communication are also key.

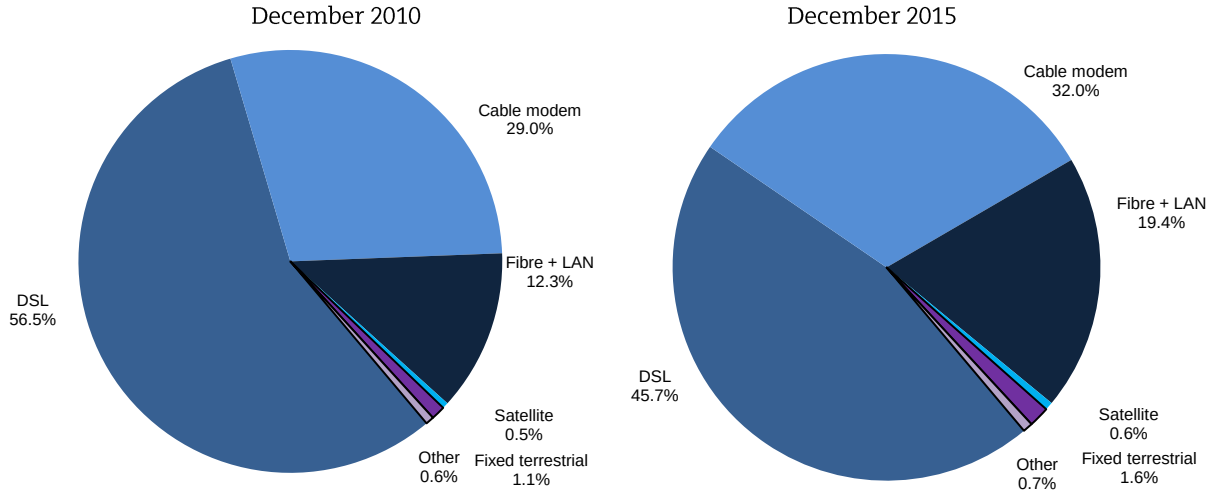
The state of digital networks

As end-user demand for capacity increases, the response of fixed Internet service providers (ISPs), whether their networks are based on coaxial cable or copper technologies, is reasonably clear – to build fibre backhaul closer to businesses and homes. At the maximum extent, this approach takes fibre all the way to the premises (often called fibre to the home [FTTH]), but there are many points along a network to which the fibre could be extended, such as the node (FTTN) or the street cabinet (FTTC). While different operators are following different approaches depending on a range of factors and may not agree on which point to take fibre to in any given network, they are uniform in deploying fibre deeper into their networks. This is why any fibre deployment is regarded as being "future-proof" because, however the final connections evolve, fibre is needed to ensure effective backhaul.

Deepening the deployment of fibre is not just for fixed networks, but also for wireless networks, which use wireline capacity for backhaul connectivity. In addition, expanding capacity over the "first mile" (between the user and the cell site) means the building of new cell sites and/or the expansion of the amount of spectrum available for wireless broadband. The development of mobile networks, and particularly the success of 5G, will therefore rely on access to spectrum and developments to both mobile network infrastructure and fixed backhaul networks. Thus, even with individuals increasingly accessing the Internet via wireless devices, fixed-line networks will continue to play a crucial role in digital infrastructures.

The transition from copper (DSL) and cable to fibre is occurring at a gradual pace, despite increasing adoption of FTTH technology in some countries. By 2015, DSL made up 45.7% of fixed broadband subscriptions in the OECD area as it continues to be gradually replaced by fibre, by then accounting for 19.4% of subscriptions, up from 16.2% in December 2014 (Figure 28). Cable (32%) made up most of the rest. Among G20 economies, Japan and Korea have the highest shares of fibre in fixed-line broadband at 73% and 71%, respectively.

Figure 28. OECD fixed and mobile broadband subscriptions, by technology



Source: *OECD Broadband Portal*, www.oecd.org/sti/broadband/oecdbroadbandportal.htm.

2.2. Key barriers to the deployment of high-speed networks and services

There are a range of obstacles to the deployment of high-speed networks and services, some pertinent to both fixed and wireless infrastructure, and some more relevant to one or the other. A basic obstacle for both fixed and wireless can be that the nature of the infrastructure itself can give rise to high barriers to entry. For fixed networks in particular, this is partly because of the historical legacy that networks generally began life in the 20th century as government-owned or state-sanctioned monopolies. Nonetheless, both fixed and mobile

network infrastructure sometimes has certain features akin to a natural monopoly, such as it not being practical or economical for particular assets to be duplicated by new entrants.

Geography can also be an obstacle when it comes to rural and sparsely populated areas. The longer distances and sometimes-challenging topography make it more expensive to roll out infrastructure and the smaller number of potential users makes it less profitable to serve these communities. Furthermore, because of the challenges and reduced economic incentives to serve these locations, there are generally fewer connectivity providers, which often results in lower levels of competition. In some countries, this problem is addressed by public initiatives that provide funding or incentives to invest in underserved areas, and to the extent practicable for this infrastructure to be open to the use of competitive service providers. At the same time, policy makers must also pay attention to a potential resulting obstacle that publicly funded infrastructure might crowd out commercial roll-out of high-speed networks. Wherever possible it is better to encourage such private investment given scarce public resources.

High capital expenditure is of the main barriers to the deployment of digital infrastructure. This is an issue for mobile networks, with the costs of passive infrastructure, such as masts and backhaul capacity. It is particularly challenging for fibre roll-out, where the capital costs of FTTH deployment typically exceed USD 1 000 per home served in urban areas.

Telecommunication markets also need long-term investment, and this requires that all stakeholders know in advance the applicable rules and regulations. Regulatory uncertainty can therefore be an obstacle to infrastructure roll-out in both fixed and mobile networks, making it important that regulatory frameworks are designed and reviewed to ensure they promote stability and predictability of regulation and its implementation.

A further significant obstacle involves administrative barriers faced by those seeking to deploy infrastructure, such as complicated or outdated rules and procedures to get licenses for deploying networks and the necessary approvals from municipal authorities. Again, while this can be an issue in mobile (e.g. compliance with planning rules for new masts), it is particularly challenging for building out new fixed infrastructure, where operators are often faced with the complexity and cost of obtaining rights of way to deploy new equipment or install new street cabinets. A related obstacle can be challenges in gaining access to passive infrastructure, whether that is for companies deploying fibre to obtain access to the infrastructure of public utilities such as railways and energy companies, or other telecommunication providers seeking access to passive infrastructure owned by telecommunication operators themselves (e.g. dark fibre, ducts, masts).

There are also some obstacles specific to the mobile market. One of the highest barriers to entry is access to spectrum due to limited availability of frequency bands and the time it can take for administrations to carry out assignment processes for the available spectrum. The scarcity of spectrum and its value in deploying new high-speed networks is particularly pertinent in remote areas where fixed infrastructure sometimes struggles to reach. Finally, some G20 economies may also face challenges of the lack of basic infrastructure (e.g. electricity) in rural areas, which cannot be solved by policy measures specific to broadband. This means that concurrent public policies in other areas must be considered at the same time to promote the deployment of broadband infrastructure.

2.3. *Promoting competition and investment in a converged environment*

Policy makers and regulators must recognise and harness the relationship between investment, competition and innovation. This is a particularly complex task in an increasingly converging market. Competition between communication networks and service providers generally leads to greater consumer choice, better quality communication services and lower prices. However, some argue that over-the-top (OTT) provision of voice and video services discourages infrastructure operators from investing in further network expansion and content

creation. Others believe that it spurs innovation, competition in communication markets and generates traffic and demand for broadband services, and hence collectively encourages more investment. A dynamic interplay of competition, investment and innovation is essential to create a virtuous circle. This section will consider the impact of convergence on infrastructure, and then suggest the ways in which investment and competition can be promoted and sustained.

Convergence

Few sectors have experienced more change in recent years than the communication industry, with much more set to come. Business models that were built on separate fixed, wireless and broadcasting infrastructure have converged, services provided over different networks are now offered over a single pathway – the Internet. While these single-purpose networks dedicated to telephony or television used to be offered by distinct companies, market players are now able to offer combinations of voice, data and television, including providers that have no local access infrastructure.

This convergence has resulted from infrastructure investment and technological developments leading to broadband Internet networks capable of supporting multiple platforms, services, and market participants. It has been facilitated by the IP in which "bits" are the building blocks for transmission of all applications, content and services. This process of convergence is steadily deepening as technology evolves and as more and more economic activity shifts online.

There is convergence between fixed and mobile networks, with the ability to shift data from the wireless networks with scarce spectrum, to fixed networks with lower costs for network operators, relieving pressure on mobile networks and improving performance for users. At the same time, mobile provides competition to fixed-line services, in both voice and broadband markets. Finally, the rise of M2M connections in recent years also shows the convergence of the Internet with other areas of the economy, such as automotive, logistics or healthcare delivery.

The issue of how to promote competition while fostering innovation and investment remains crucial for policy makers and regulators. In a converged scenario, however, traditional approaches for assessing and regulating telecommunication and television markets may not be optimal. For example, industry consolidation, including mergers between communication, applications and content providers, is raising new challenges for competition. In addition, bundles and market concentration may reduce competition, especially if some providers cannot replicate the bundles offered by merged companies (e.g. a bundle containing premium television content). Finally, convergence of markets and business models has also led to the convergence of regulators across the world, which is discussed in Chapter 5 on ICT regulation. Convergence is therefore changing the dynamics and relationships between competition, innovation and investment.

Investment

Capital markets apply the same criteria for investment across the economy – fundamentally, their willingness to finance investments, and the terms they give, will depend on the risks and rewards associated with the investment. The role of regulators is not to second-guess markets but rather to provide clear decision-making processes and outcomes against broader goals set by policy makers.

For investment in high-speed networks, the market structure is a key component in assessing risk and reward, and will therefore influence levels and types of investment. There have been a number of different approaches taken by countries with respect to market structure in this area, strongly influenced by the structure of the legacy networks. For example, in some countries the structure is focused on competition between different technology infrastructures, such as a provider of broadband over copper lines competing with a cable provider – known as facilities-based or infrastructure-based competition. Elsewhere, market structure is focused on the

separation of infrastructure and services, which generally entails high levels of regulation for the infrastructure component where the barriers to market entry are high. In competitive markets, investors expect higher rates of return from firms with seamless provision of infrastructure and service.

Governments can take a longer-term and broader view of investment returns than the private sector, and might identify positive societal externalities not taken into account by private investors in investment decisions. Some countries have, therefore, concluded that there will not be sufficient private investment to build high-speed networks in a way that meets public policy objectives, such as speed or coverage, and have made public infrastructure investments, either directly or in partnership with private investors. Others believe that they should enable the private sector to do as much of the "heavy lifting" as possible, promote infrastructure competition and use public funds only when there is a demonstrated market failure.

There is no single solution for encouraging investment in high-speed infrastructure – the best approach will depend on an assessment of the levels of competition, taking into account the market structures and inherited infrastructures, as improved networks are deployed. Investment in network infrastructure has remained stable in recent years in most G20 economies and information on current levels of investment can be found in Chapter 3 on financing.

Competition

Investment and pricing decisions are clearly influenced by the degree of competition among ISPs. Competition is also important for driving up the overall quality and speeds of broadband offers. In general, the wireless broadband space is characterised by greater competition than fixed broadband. Some countries have just one fixed infrastructure; a few, such as Korea, have several. Others, such as the United States, are served by two wireline infrastructures, one based on the telephone network and one based on cable television operators.

Despite increasing coverage of fibre networks, most fixed broadband subscribers still rely on copper. Cable broadband networks can be upgraded with DOCSIS 3.1 technology,[3] making it a potential substitute to fibre networks and providing an important source of competition in high-speed networks in countries with widespread cable coverage. The challenge for policy makers and regulators is to ensure that the market is responsive to demand by ensuring effective competition between end-to-end infrastructure providers or ensuring that wholesale providers maximise the ability of retailers to respond to demand in the same manner as end-to-end providers in a competitive market.

In fixed networks, open access policies – in the form of mandated regulated access, such as local loop unbundling or other wholesale access products – undeniably play a leading role in the development of competition in countries where these markets are liberalised. They will continue to have a role in promoting competition in the market for fixed high-speed Internet access, particularly where there is insufficient infrastructure competition. However, some wholesale access products will be different for fibre technologies and some of them (e.g. dark fibre, access to ducts or in-building wiring) may be more technically difficult or less economically viable for entrants to use. Regulators will need to be conscious of the potential implications for competition if access for alternative providers becomes more difficult with fibre networks. Municipal networks can provide alternative high-speed infrastructure to open up retail ISP markets and boost competition, but the impact of publicly funded networks on investment decisions should be taken into account – see he discussion on role of public-private partnerships (PPPs) below.

There are a number of competition issues associated with wireless networks. In recent years, there has been a trend towards industry consolidation, especially in mobile communications. Regulators and competition authorities in G20 economies have assessed the pros and cons of industry consolidation in mobile markets, especially with regard to merger cases. For mobile markets, the higher the number of mobile network operators (MNOs), the higher the likelihood of more competitive and innovative services being introduced and

maintained. Few feel that more consolidation would improve competition, but in some cases authorities have obtained commitments from merging parties aimed at facilitating the presence of mobile virtual network operators (MVNOs) or a more equitable distribution of spectrum resources among operators, to address the reduction in the number of competitors.

Another competition issue in the mobile sector relates to commercial dealings among market players, whereby MNOs have been found to set unreasonable technical or pricing conditions or unfair limitations to make it harder for MVNOs to compete. This could be addressed by prohibiting restrictive provisions in wholesale roaming arrangements and allowing full MVNOs to acquire mobile network codes. Mandating MNOs to host MVNOs is another way to improve the level of competition in national mobile markets.

A final competition issue in the mobile sector involves international mobile roaming. For many years, roaming prices were very high with resulting low levels of usage of mobile devices when traveling. The OECD adopted a Council Recommendation in 2012 outlining various potential ways to reduce roaming prices, and has since seen significant progress in this area for a number of reasons. Regulation has played a role, certainly in the European Union, where regulated pricing caps have been introduced and progressively reduced for voice, SMS and data roaming between European Union countries. The extent of the European Union's initiatives is unique, but there have been other governmental initiatives aimed at reducing prices, such as bilateral agreements between countries to regulate mobile roaming rates, including between Australia and New Zealand (2013) and within the Australia-Singapore free trade agreement (2016), and ongoing discussions about agreements between countries in Latin America.

Demand has played a role, with more people expecting to use mobile devices abroad. One of the first countries to experience substantial changes in the prices for international mobile roaming was China. Alongside increased travel and growing demand, China's mobile operators negotiated lower wholesale rates and passed these reductions on to their customers. In addition, competition has also been a factor, both from some MNOs in countries such as Mexico and the United States, and MVNOs offering "Roam Like at Home" (RLAH) plans with which a subscriber uses their domestic mobile package when abroad, and from alternative IP-based platforms for voice and SMS, such as Skype, FaceTime and WhatsApp.

Backhaul Internet connectivity markets play a critical role in guaranteeing competitive prices for users of both fixed and mobile broadband services. The Internet is a decentralised network of networks, with each network an autonomous system (AS) bearing its own costs to reach the rest of the Internet. The Internet's model for traffic exchange works extremely well and has been a major ingredient in enabling it to scale so rapidly and pervasively.

2.4. Ensuring that the key technical enablers are in place

In addition to promoting competition and investment in a converged environment, it is also critical consider some technical enablers, such as access to Internet exchange points, spectrum, and take-up of IPv6, to ensure high-quality and affordable access to digital infrastructure.

Internet exchange points

At its core, every user of the Internet pays for his or her own access. In turn, their ISP undertakes to provide connectivity to the rest of the Internet either through peering (direct interconnection, often without a fee) or paying for transit. The purchase of transit enables an ISP to reach all networks around the world. Peering enables two ISPs to directly exchange traffic while bypassing the transit providers. Through the use of peering, ISPs can reduce their costs, as they do not need to purchase transit for that traffic. This system enables global connectivity and the ability of each of over 55 000 ASs on the Internet not to have to negotiate with every

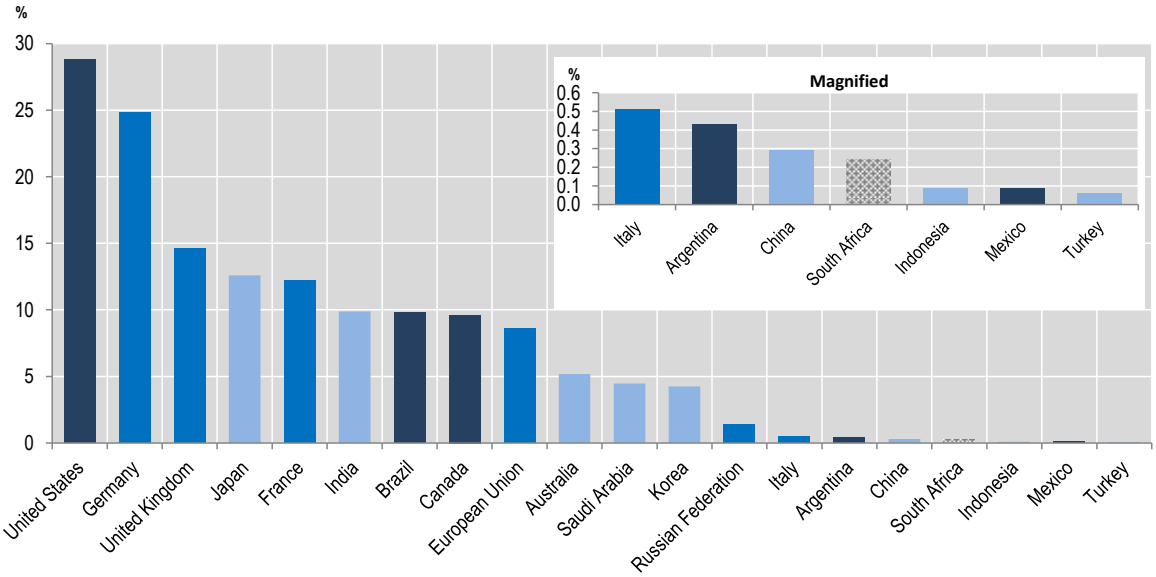
other network on the Internet (CIDR, 2016). The Internet has thus achieved global interconnection without the development of any international regulatory regime.

To save costs and improve performance, ISPs establish or make use of Internet exchange points (IXPs), where they can peer with multiple networks at the same time. Recent OECD analysis of 4 300 networks, representing 140 000 direct exchanges of traffic on the Internet, found that 99.5% of "peering agreements" were made on a handshake basis, with no written contracts, and exchange of data occurring with no money changing hands (Weller and Woodcock, 2013). Moreover, on many IXPs, multilateral agreements are in place, using a so-called route server where hundreds of networks accept to exchange traffic for free with any network that joins the agreement.

Under the current voluntary system, operators have an incentive to invest and expand their network to reach new peers, and to co-operate with other networks to establish new IXPs in areas where there are none, because they save on transit costs. Expanding the number of IXPs helps to keep local traffic local, unburdens interregional links and stimulates investment in local networks. For this reason, it is important to encourage countries to develop and use IXPs.

In 2016, from the 464 active IXPs worldwide, 275 are operating in G20 economies. A closer look of the number of IXPs shows significant differences among G20 economies (Figure 29). The United States is the country with the highest number of Internet exchange points, representing a very densely populated mesh of interconnections between ISPs. Brazil, Germany and the Russian Federation are next due to different factors. Brazil and Russia are geographically vast countries that require IXPs to reduce transit costs and latency. Germany, with a high population density and the largest IXP by traffic exchanged, is a strong net exporter of Internet bandwidth. Following the lead group, there are a number of countries that have several exchanges per country, generally one per capital city and main urban areas such as in France, Japan, Australia, Argentina, Canada and the United Kingdom. Such groups have well-functioning exchanges that produce roughly enough bandwidth to meet the local demand. Lastly, some countries have only a few exchanges that produce very little Internet bandwidth and hence bandwidth will have to be imported, to the extent that domestic traffic is exchanged in foreign countries.

Figure 29. Internet exchange points in G20 economies

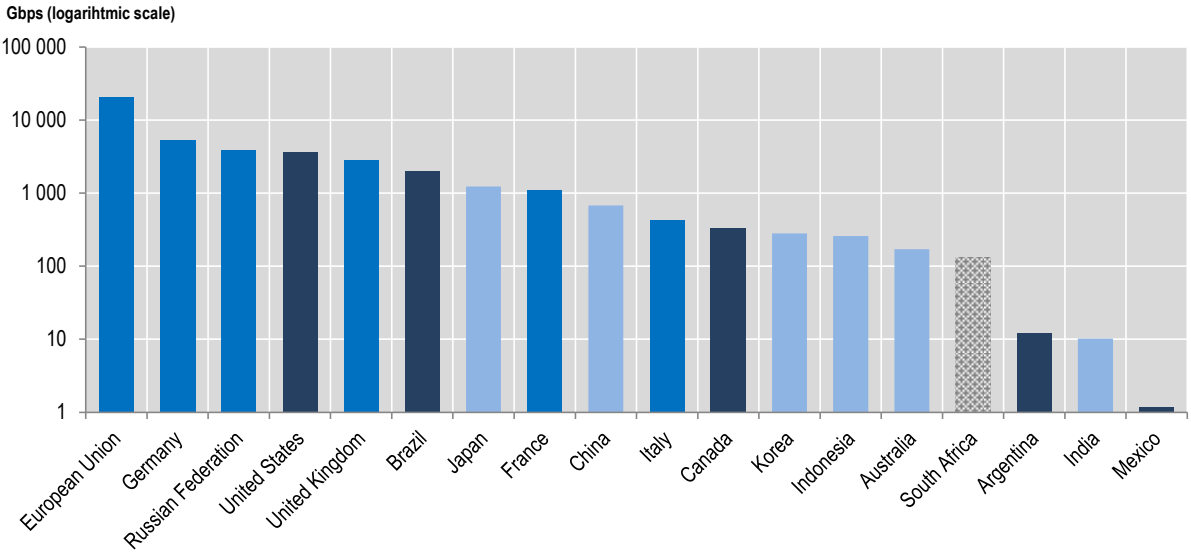


Note: It is important to note that even though most IXPs adhering to best practices provide statistics on the number of networks connected and the traffic exchanged, some data might be missing or inaccurate.

Source: Packet Clearing House (2016).

The amount of bandwidth produced domestically per country can be useful to indicate the development of Internet-related infrastructure at large, including data centres, cloud services and more generally ICT services (Figure 30). If Internet bandwidth is treated as a commodity, some countries will be net importers or net exporters depending on their ability to satisfy domestic demand. In Germany, for example, a portion of the bandwidth produced will be exported and consumed in neighbouring countries. Statistics gathered from IXPs, however, do not reveal all data exchanged in a country. This is because many network operators have private peering arrangements in addition to or instead of using the main switching fabric. Such is the case of the United States, where many networks have established direct interconnections.

Figure 30. One day of Internet traffic exchanged at IXPs in G20 economies, 11 September 2016



Source: Packet Clearing House (2016).

While the system of Internet traffic exchange itself works well, and many G20 economies are relatively well-served, with the presence of multiple international routes and intense competition, other regions – especially those outside major international routes – sometimes need public support for the deployment of backhaul and international connectivity infrastructure. Once infrastructure is in place, countries must implement and monitor open access policies to ensure that international connectivity routes, which often require significant investment, are provided by a sufficient number of market players.

Spectrum

Spectrum is a scarce natural resource, which is essential for providing wireless services, among many other things (e.g. broadcasting, aviation, defence). The allocation and use of spectrum is therefore tied up with important social and economic trade-offs that need to be carefully considered. Due to the increase of mobile voice and data traffic as well as the growing market for smartphones and smart devices, such as sensors and RFID tags, the need for an efficient allocation of spectrum is becoming more acute. There are a number of ways in which spectrum could be more efficiently managed to enable deployment of more and better high-speed wireless services.

Spectrum inventories are an important tool for the governments and regulators that manage spectrum to identify spectrum that is underused or could be potentially shared, or could be reallocated to different uses (spectrum "refarming"). In carrying out these inventories, it is important to carefully evaluate the potential uses of spectrum that will be released and balance multiple factors regarding investments, competition issues and consumer choice before decisions are taken on defining the particular use of released spectrum.

Certain policies promote good use of spectrum, such as transparency in terms of assignment procedures, conditions of use and renewal, and statistics on actual use, allocating spectrum in a way that promotes competition (e.g. providing a level playing field for competition through a balanced assignment of spectrum between different market players). Another includes allowing for the flexible use of spectrum to avoid hampering competition and innovation, i.e. service and technological neutrality so long as the use is compatible with the spectrum band. The allocation of spectrum can also be used to meet important policy objectives, such as conditions requiring a certain amount of coverage by mobile operators as one of the conditions for acquiring spectrum to better connect underserved areas.

Using a market-based approach has proven effective in maximising public value and efficient use of spectrum. One example is permitting spectrum trading and the development of secondary markets, allowing spectrum to be transferred to those that value it the most. Using auctions is an important way to capture the market value when allocating spectrum. One way of promoting more efficient use of such spectrum is to create incentives that mimic market-based incentives, a good example of which is an "administered (or administrative) incentive pricing" regime, where fees are replaced by prices set by a regulatory authority attempting to reflect the opportunity cost of the spectrum.

Finally, spectrum agencies should increase the efficiency of spectrum management through various means. Sharing of spectrum is a valuable and fairly recent development. It can be done through licensed-shared access, which allows spectrum that has been licensed to be used by more than one entity, introducing additional users on a given band to unlock spectrum capacity. Another promising innovation uses under-utilised spectrum, known as "white spaces". These intentionally unused parts of spectrum had been important historically to avoid interference, but technological developments are enabling the use and sharing of these white spaces.

IPv6

IP defines the address space for the Internet. The number of addresses defined by Internet Protocol version 4 (IPv4), the version of IP that has been used since the start of the commercialisation of the Internet, has almost run out (the African Regional Internet Registry is the last to hold IPv4 addresses and these are projected to be depleted by 2018).

A successor to IPv4, known as Internet Protocol version 6 (IPv6), has been available since 1998, but the uptake of IPv6 has been very slow. The worldwide traffic over IPv6 stood at 13.60% in September 2016, compared to 3.91% two years earlier (Google, 2016). As noted in Part I (Figure 3), there are significant differences among G20 economies. While only two countries had a user penetration higher than 20%, eight countries had less than 2% penetration. As of October 2016, the United States is the leading G20 country with 28.78% of IPv6 adoption, followed by Germany and the United Kingdom with 24.83% and 14.60% respectively. Overall, the slow uptake among G20 economies is an ongoing concern, as they should have a leadership role in its deployment.

An encouraging development in recent years includes ambitious deployment initiatives by different players over a number of years. These include governments, NGOs and the technical community facilitating the transition by encouraging IPv6 deployment through sharing good practices for IPv6 implementation, publishing information about levels of IPv6 deployment and including IPv6-related conditions for public procurement. It also results from actions of the part of industry, with much of the infrastructure of the network, including backbone transmission paths and the domain name system infrastructure, also IPv6-capable, and support for IPv6 in the operating systems provided by the Windows, Mac and Linux operating systems.

However, the incentives are not so clear-cut for ISPs, which face economic and technical challenges in converting large numbers of interconnected IP networks to IPv6. While some ISPs have made substantial

efforts to extend IPv6 services through their access networks, many are not deploying IPv6 infrastructure in their mainstream product set, and instead focusing on technologies that conserve their remaining IPv4 address stocks by deploying address-sharing middleware (e.g. Carrier Grade Network Address Translation) to share IPv4 addresses across multiple customers. The resulting effect of parts of the network using different communications protocols is not desirable if the Internet is to continue functioning as an open, decentralised network where any end user can reach any other.

2.5. Mechanisms to foster investment in digital infrastructures

There are a range of tools and other mechanisms to foster investment in digital infrastructures. This section focuses on two important elements: national broadband plans and the involvement of digital platforms in infrastructure development.

National broadband plans

National broadband plans are an important tool for creating a policy environment conducive to promoting digital infrastructure development and deployment. In September 2016, the United Nation's Broadband Commission for Sustainable Development reported that over 80% of countries have established or are planning to introduce national broadband plans or digital strategies. These are generally set in terms of speed of service offered and percentage of coverage, penetration and specific groups contemplated. Such plans should set measurable targets and broadband coverage maps are an important tool for identifying current gaps and measuring progress towards access availability and speed targets.

National broadband plans have increasingly played a role in infrastructure policy in recent years and targets are being reviewed and updated. In September 2016, the European Commission proposed new targets for a European Gigabit Society by 2025. Under these proposals, all schools, transport hubs, main providers of public services and digitally intensive enterprises should have access to Internet connections with download/upload speeds of 1 Gigabit of data per second (Gbps). In addition, all European households should have access to networks offering a download speed of at least 100 Mbps, and all urban areas as well as major roads and railways should have uninterrupted 5G wireless broadband coverage.

The United States aims for 100 Megabits per second (Mbps) to 100 million homes by 2020, while Canada's plan is focused on boosting coverage in underserved areas by investing CDN 500 million over 5 years. In Asia, Korea's goal is 1 Gbps to 90% of urban areas (85 cities) and 100 Mbps to 100% of households (including rural areas with 50 households) by 2017, while, by 2020, Australia aims for speeds of 50 Mbps to 90% of households and businesses, and at least 25 Mbps to the whole population.

As well as setting targets, many national broadband plans also include plans for public investment in infrastructure projects. As discussed above, in certain cases public support and investment may be needed to ensure the greatest practical availability of high-speed networks, or to solve critical bottlenecks, such as addressing the availability of high-speed backbones or backhaul infrastructure, when they cannot be addressed adequately by private initiatives. However, such public intervention should support market competition and promote private investment initiatives.

While private investment has been the overwhelming source of finance for high-speed networks in developed countries, public authorities have acted in various degrees to complement these investments. This ranges from publicly owned operators constructing networks in Australia, New Zealand and Singapore to, in other countries, subsidies from governments to fill gaps in rural and remote areas where private financing had not been attracted based on an assessment of likely returns. Municipal authorities or utilities have also played a key role in these developments by either initiating their own networks or attracting new entrants, such as Google's fibre and wireless projects in a growing number of cities in the United States. The "Broadband for San

Francisco Project", for example, aims to establish speeds of 1 Gbps for every subscriber in the city by 2018, with the municipal authority to announce in early 2017 whether this will be achieved through a public, private or public-private model of funding (Sabatini, 2016).

Many of these examples of national or municipal government involvement take the form of PPPs, a contractual agreement whereby the private party agrees to design, build or operate an asset (often an infrastructure asset) and to bear some of the risk associated with these activities. That being said, caution is necessary as public involvement can have implications for private investment and distort competition – the *OECD Council Recommendation on Broadband* recognised the primary role of the private sector in the expansion of coverage and the use of broadband, with complementary government initiatives that take care not to distort the market. Overall, policy makers need to strike a balance between four key objectives when relying on public investments: improving connectivity, increasing competition, stimulating innovation and growth and increasing well-being.

It is also important that there is co-operation between the funding authority and the telecommunication regulator, to guarantee coherence between ex-ante regulation, competition law and public funding schemes for broadband networks. This would leverage the expertise of telecommunication regulators and ensure a consistent approach at all levels.

Involving digital platforms in infrastructure development

Digital platforms play a key role in providing choice and spurring competition in communication services, such as Voice over Internet Protocol (VoIP) as an alternative to fixed and mobile telephony or the many video-on-demand providers that compete with traditional broadcasting and cable television. Sometimes their applications come embedded with a purchased device, such as a smartphone, or using an application, which users add to a device. Often the latter are called OTT services. For their part the user pays their ISP to provide them access to the Internet and use of that connection and much of demand for this connectivity is to use digital platforms or access OTT services.

On the Internet, all of these entities have their own networks with which they carry their traffic to the networks of users of their services. Some of the larger digital platform or OTTs have their own extensive fibre networks to carry this traffic to points where they interconnect with networks that provide Internet access for their own customers. If they do not have such facilities, they pay other networks to provide transit or content distribution (i.e. transit or content distribution networks (CDNs)). All of these endeavours -- over their own networks or when they pay others to store or carry traffic for them -- are aimed to take OTT services closer to their users.

For their part, ISPs carry the traffic from the networks of the digital platforms or OTT (or their transit/CDN provider) to their own customer. Some ISPs provide their own transit or CDN services to OTTs delivering the traffic to their own end customers or carrying it to other ISPs for them to deliver to their customers. In this way each of the 55 000 ASs on the Internet contribute by investing in their own digital infrastructure or paying others to deliver that traffic. At the same time, each end user pays for their own access to the Internet via their ISP and that should be the main source of investment funds for building access.

In commercial negotiations between networks each party has an assessment of the value of what they and others bring to the table. They all take into account the potential for competitors to supplant their own role in part of a value chain, the demand of their own customers, the prices they can charge them and so forth. These dynamics have been remarkably successful in expanding the Internet while at the same time encouraging all users to reduce their costs by peering or purchasing transit depending on what provides the best outcome for their relations with specific networks or the rest of the Internet. This does not mean that all players will be satisfied from such negotiations, but the system has enabled the Internet to scale in a manner that would not

have been possible if this sector was regulated in a similar manner to traditional telephony markets in the 20th century.

Some players involved on the Internet as digital platforms are working on initiatives to fill gaps in the infrastructure and extend connectivity to people in rural and remote areas, e.g. Google's Project Loon is a network of balloons traveling on the edge of space, Facebook's Connectivity Labs is looking at deploying satellites and drones, and Microsoft has been involved in research into the dynamic use of spectrum in television white spaces to provide Internet access in underserved areas. In addition, digital platforms are investing in backbone infrastructure. Amazon, Facebook, Google and Microsoft have all made recent and substantial investments in submarine cable construction projects, working with other companies to improve infrastructure capacity across the Atlantic and Pacific oceans.

Nonetheless, the primary way digital platforms or OTTs contribute to stimulating infrastructure development is by creating demand for Internet access and use. All ISPs benefit from this increased demand and this is reflected in the success of the Internet's model for traffic exchange and growth. This works best when, in a competitive market, ISPs structure pricing in a way that leverages increasing demand for infrastructure development. In Finland and Switzerland, for example, some mobile providers charge by the tier of speed users elect rather than the amount of data they download. The mobile providers in these countries therefore welcome digital platforms and OTT services because they stimulate demand for faster services with higher charges. At the same time, ISPs increasingly offer their own services that mirror those of OTTs, such as video-on-demand services, growing the entire market.

These various involvements of digital platforms in infrastructure development can all be welcomed as ways to increase competition in the provision of networks, to bring in more investment, or sometimes even to address gaps in the infrastructure. The evolving technological and market trends behind this increasing involvement of digital platforms in infrastructure development, however, have caused some ISPs and policy makers to raise questions about a level playing field in the regulatory framework, which is discussed further in Chapter 5 on ICT regulation. In addition, some content or platform providers, ISPs or policy makers, have raised the question of whether the revenue received by a particular part of a value chain fairly compensates or encourages investment in the creation of that content, service or its delivery.

Experience shows, however, that allowing market forces to take precedent is the best way to encourage investment in digital infrastructures. Nonetheless, if market forces are not meeting policy objectives, governments or their authorities have options at their disposal, such as public investment in locations without sufficient access or increasing competition. Examples, where public investment is involved, include national broadband networks, municipal networks, PPPs or subsidies to private players. Such initiatives often entail open access requirements for other network providers to ensure competitive choice.

2.6. Key areas for policy action

Given the importance of digital infrastructures for economic and social development, it is crucial that governments ensure that the infrastructure is meeting the growing demand for high-quality connectivity now and in the future. A key area for policy action involves establishing national broadband plans with well-defined targets and reviewing them regularly. These plans should ideally address all of the key barriers to the deployment of high-speed networks and services identified earlier in the chapter, and include measurable targets to address the policy challenges associated with ensuring competition and investment and that the important technical enablers mentioned above are in place. Specific elements to be included in these plans are outlined below.

For fixed networks

- Encourage the deployment of more fibre deeper into the network to drive a substantial increase in speeds experienced by users across all access technologies.
- Reduce the administrative obstacles to high-speed infrastructure roll-out by simplifying licenses and facilitating efficient access to rights of way.
- Ensure access to passive infrastructure deployed by other actors, whether that is for operators deploying fibre gaining access to the infrastructure of public utilities such as railways and energy companies, municipal facilities or new entrants seeking access to passive infrastructure owned by other operators themselves (e.g. dark fibre, ducts, masts).

For mobile networks

- Produce national and regional action plans with a specific date (e.g. 2018) to spur the rapid deployment of 5G networks, acting quickly to free up sufficient spectrum, as well as facilitating the industry investment required to provide the necessary infrastructure and wireless backhaul capacity.
- Exercise caution with potential mergers that would reduce the number of mobile operators in a market below four, and consider obtaining commitments from merging parties that would facilitate the presence of MVNOs or lead to a more equitable distribution of spectrum resources among remaining or new operators.

3. FINANCING DIGITAL INFRASTRUCTURES AND NEW BUSINESS MODELS

- Further investments in digital infrastructures, especially high-speed broadband networks, is essential to supporting vibrant, innovative and inclusive digital G20 economies. Financing hurdles related to digital infrastructure investment include high capital costs, susceptibility to changes in market conditions, low rates of return in rural and remote areas, and a lack of accurate data for making informed investment decisions.
- Encouraging investments in and sharing of data – itself an important 21st-century infrastructure – is also needed. Challenges to doing so include issues related to data curation and investment incentives, trust (privacy and digital security risk management), data evaluation, pricing, data ownership and intellectual property rights (IPRs).
- Access to finance is also a key challenge for innovative enterprises that are seeking to implement new business models based on digital technologies. There are a number of areas in which the G20 could play a role to help address some of these concerns, including by strengthening infrastructure deployment through public and private financing and improving framework policies to foster financing of digital infrastructures and new business models.

3.1. The policy challenge

Digital technologies, and the infrastructures that supports them, are essential for success in today's global economy. Despite the critical importance of digital infrastructures, there are a number of challenges facing governments and companies with respect to how to finance them, in part because they are relatively expensive and have a longer-term time horizon. While financing digital infrastructures is attractive to some investors who have a preference for predictable returns in the long-term – similar to those found in utility industries (e.g. energy, water) – it shares some of the challenges associated with any infrastructure investment, especially those characterised by dynamic technological change.

At the same time, the current environment of slow global growth and low interest rates for cash deposits, gilts, and bonds may well continue for some time. This, coupled with market volatility, has made investing in infrastructure relatively attractive as a way to reap higher returns. Nonetheless, infrastructure investment can also be risky. It can be a challenge, for example, to attract the large capital outlays required for expanding or upgrading communication networks or to meet the substantial ongoing capital expenditure requirements of such networks. In addition, returns are often influenced by changes in government policy, and the long-term nature of infrastructure investments therefore becomes more uncertain since they are subject to changes in the regulatory environment.

3.2. Investments in digital infrastructure (including data)

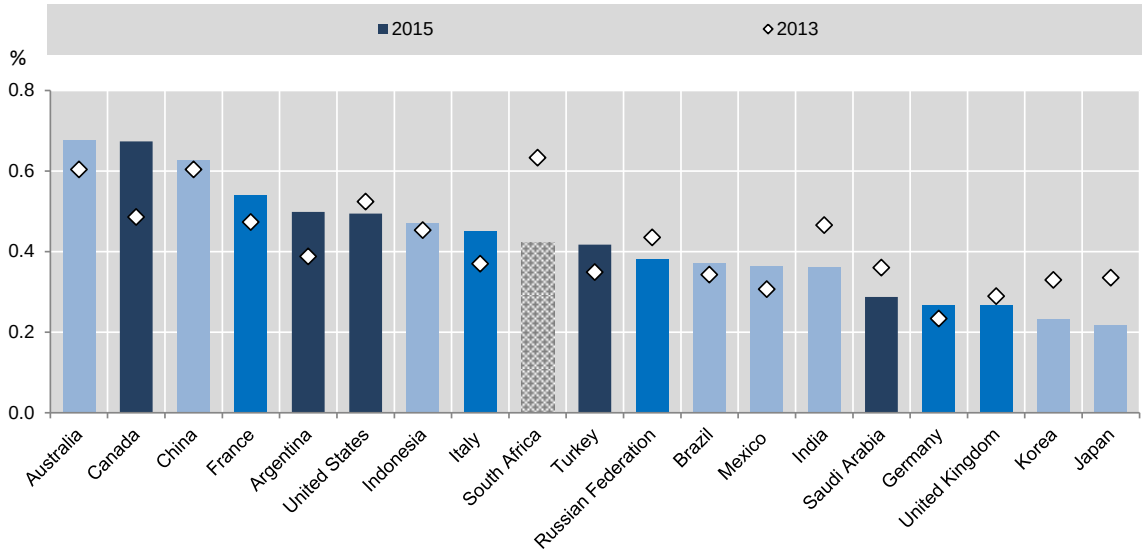
Digital infrastructures encompass a range of elements. At its core, digital infrastructure includes telecommunications infrastructure, both fixed and mobile. Another important digital infrastructure is data, which is increasingly a foundational element in data-driven economies and societies.

Investments in telecommunications infrastructure

In telecommunications, both fixed and wireless networks rely on passive infrastructure – such as ducts, cables, masts and tower sites – and on active equipment components used to implement the technology, e.g. routers and switches, control and management servers. Both fixed and wireless networks make use of fibre cables for backhaul and backbone segments of network infrastructures. To connect local and national facilities to other networks around the world, operators also need access to regional and international high-speed networks (submarine fibre optic or satellites). Alongside infrastructure, an essential asset in wireless communications is spectrum, which is needed for the delivery of wireless services. As spectrum is a scarce resource, government policies in this area can have a significant influence on financing.

In G20 economies, there was a total of USD 262.5 billion invested in telecommunication infrastructure in 2015, a slight decline from 2013 (USD 266 billion) (Figure 31). The overall average share of telecommunication revenue devoted to telecommunication infrastructure among G20 economies was 18% in 2015. While telecommunication infrastructure investment has remained relatively constant in the G20 as a whole over the past several years, the share of revenue devoted to investment varies for any given country. This is because the proportion can increase due to factors such as additional market entry or the introduction of a new generation of mobile network infrastructure.

Figure 31. Telecommunication infrastructure investment as a percentage of GDP, 2015 or latest year



Note: Non-OECD G20 economy data are for 2014 instead of 2015.

Sources: OECD for OECD economies; ITU for the other G20 economies.

In recent years, there has been substantial investment by some countries in national broadband networks. For example, Australia invested 26% of total telecommunication revenue in 2015. This reflects the development of a national fixed broadband network and upgraded mobile infrastructure, the largest share of which was a public investment. India invested 22% of telecommunication revenue in 2014 reflecting extensive investment in 4G, including by a new market entrant, and the associated fibre backhaul. Meanwhile, countries such as Korea and Japan – which have the highest penetration of fibre in fixed networks and well-developed mobile broadband coverage – are devoting a relatively lower proportion of telecommunication revenue to infrastructure investment. In these countries, future digital infrastructure investment is likely to be in forthcoming 5G mobile networks.

Investment in digital infrastructures comes from various sources, primarily from the private sector. Much infrastructure investment is financed by network operators, sometimes in partnership with other operators to

share costs (e.g. network sharing arrangements between mobile operators), or with equipment manufacturers (e.g. agreements for manufacturers to operate parts of a mobile network for an operator). Investments are also made indirectly through intermediary financial institutions such as pension funds, banks, and insurance companies. These institutions are often attracted to investments in wholesale infrastructure, under conditions where these facilities are less likely to be replicated and therefore more likely to produce stable, low-risk returns.

Trends in data-related investments

As the cost of data collection, storage and processing continues to decline dramatically, ever larger volumes of data will be generated from the IoT, smart devices, and autonomous machine-to-machine communications. We will need to recast how we think about infrastructure in the 21st century, and expand it to encompass broadband networks, cloud computing and data itself, which is a driver for productivity growth (OECD, 2015f).

In the United States, for instance, Brynjolfsson, Hitt and Kim (2011) estimate that output and productivity in firms that adopt data-driven decision making are 5% to 6% higher than what would be expected from their other investments in, and use of, ICTs. A study of 500 firms in the United Kingdom found that firms in the top quartile of online data use are 13% more productive than those in the bottom quartile (Bakhshi, Bravo-Biosca and Mateos-Garcia, 2014). Overall, these firm-level studies suggest that using data and data analytics raises labour productivity faster than in non-using firms by approximately 5% to 10% (OECD, 2015f).

The growing importance of data is also reflected in current trends in venture capital (VC) investments related to big data, which is growing despite an observed slowdown in total VC investments since 2014. Big data start-ups (primarily in the United States) received more than USD 6.5 billion in VC investment in 2015, accounting for 11% of total technology-related VC investments (Turk, 2016). This includes large scale VC investments in start-ups such as DataDog (USD 94 million), BloomReach (USD 56 million), Qubole (USD 30 million), and PlaceIQ (USD 25 million) (Turk, 2016). After a strong increase in 2012, merger and acquisition activities have recently slowed down, pointing to the consolidation in the market for big data-related goods and services (OECD, 2015f). Similarly, the number of financing activities has increased rapidly from 55 deals in 2008 to almost 164 deals in 2012, with almost USD 5 billion being invested over that period. In the second quarter of 2013, a slowdown in the number of deals and their total volume could be observed, although big data companies raised already more than USD 1.25 billion across 127 deals in the first half of 2013 (Orrick, 2012).

3.3. Financing hurdles related to telecommunications infrastructure investment

There are general challenges for utility investments that hold true in the context of telecommunications infrastructure – the substantial capital costs and the susceptibility to policy or regulatory changes that occur over a long time period. There are also some hurdles that are particularly relevant to the telecommunication sector, namely the sometimes lower rates of return from rural and remote areas, as well as a lack of accurate data for making informed investment decisions. Governments have a range of tools at their disposal from the expenditure of public funds (e.g. addressing market gaps), should resources permit, to ensure that the market is used to the maximum extent possible to reduce the size of such requirements to meet policy objectives. Such an approach, for example, can introduce competitive bidding to see who can provide improved access to underserved locations at the lowest cost.

Capital costs

One challenge related to infrastructure investment involves the large initial capital outlay requirements and substantial ongoing capital expenditure needs, and this is true of digital infrastructures. The costs of deploying and operating Internet infrastructure can be substantial, and maintaining, upgrading or expanding networks generally requires additional investment. With fibre deployment, for example, the business case may not be

sufficiently compelling for operators reluctant to face the significant investments involved, in turn encouraging them to instead leverage the assets of the existing copper infrastructure, potentially diverging from government policy preferences for higher-speed networks.

A response to this can be seen in the European Union, where a 2014 directive on measures to reduce the cost of deploying high-speed electronic communications networks contained measures to create conditions for more cost-efficient network deployment. These include the sharing and reuse of existing physical infrastructure, including those belonging to utility companies; enhanced co-ordination between civil engineering projects to reduce the number of occasions roads need to be dug up; and requiring all new buildings to be equipped with accessible high-speed-ready physical infrastructure.

Susceptibility to changes in market conditions

The long-term nature of infrastructure investment increases the exposure of investors to a major change in regulation or policy that can influence the rate of return. This is also true for the telecommunications sector. Given the importance of digital infrastructures, specific policy objectives, such as ambitious targets for increased access to high-speed networks, are often put in place. If the pace of deployment is insufficient to meet such policy objectives, regulation can be adjusted to provide more incentives for market participation, such as by increasing competition under some market structures or changing a market structure. This is why regulatory frameworks need to be periodically revisited to ensure that they encourage the investment needed to meet policy goals, though in a manner that is transparent and evidence-driven.

In addition, government policies with respect to spectrum can have a significant influence on financing decisions. As discussed in the Chapter 2 on infrastructure, spectrum is a scarce natural resource, which is essential for providing wireless services among other uses. It is therefore vitally important that it is managed efficiently by using mechanisms such as auctions to ensure that it is assigned an accurate market value. Therefore, spectrum prices should not be set with the aim of maximising income for governments, but rather through market mechanisms that provide an appropriate rate of return based on market valuations.

Low rates of return in rural and remote areas

The lower number of potential subscribers in rural and remote areas, coupled with the sometimes higher costs of deploying infrastructure over greater distances, frequently lower the rates of return and deter private investment. In some countries, public investment has stepped in to finance or co-invest in PPPs. Some municipal authorities have played a role by attracting new entrants, such as through fibre or wireless projects in a growing number of cities in the United States, which has in turn driven incumbents to increase their own investment and improve the quality of their services in these areas.

Lack of accurate data for making informed investment decisions

An impediment to investment in fixed, wireless and backhaul networks can be the difficulties in accurately predicting traffic growth and required capacity, and the consequent challenges in assessing rates of return. The period around the turn of the century, for example, was typified by excessive investment in backbone networks in some countries in anticipation of high demand that did not materialise. Meanwhile, it took some time before smartphones developed to the extent that they stimulated demand for 3G mobile networks. By way of contrast, 4G investments were driven by such demand. There is a lack of government-collected statistics on the data traffic flows within and between countries, with the Australian Bureau of Statistics being an outlier in providing annual data on all traffic downloaded within the country. It is widely acknowledged that markets need information to work properly, and better information about the use of digital infrastructure would enable more informed investment decisions for all stakeholders.

3.4. Barriers to investments in and sharing of data

The volumes of data that will be generated from the IoT, smart devices, and autonomous machine-to-machine communications hold many promises in a wide range of areas, including health, agriculture, public governance, innovation, tax administration and compliance, business financing, education, and the environment. There are a number of challenges to encouraging investments in and sharing of data, including issues related to data curation and investment incentives, trust (privacy and digital security risk management), data evaluation, pricing, data ownership and IPRs.

Data curation and investment incentives

The provision of high-quality data can require significant upfront and follow-up investments before the data can be shared. Data curation, which embodies data management activities necessary to assure long-term data quality across the data life cycle, is needed to assure to sustainability of data-related investments. However, analytical activities using particular datasets are frequently beyond the scope and timeframe of the original projects for which the data were initially collected and used. This can lead to disincentives for data curation and put at risk long-term access and reuse of data. In science and research, where the long-term quality of data is essential, data curation is seen as a key part of the provision of research infrastructure (OECD, 2013c).

Effective data sharing is, however, not limited to data curation. In many cases a number of complementary resources may be required, ranging from additional (meta-)data to data models and algorithms for data storage and processing, and even secured IT infrastructures for (shared) data storage, processing, and access. Therefore, the costs involved may discourage sharing data more widely, particularly when the benefits of sharing are not obvious. This, in turn, may result in lower incentives to invest in data in the first place (OECD, 2016g).

Privacy and digital security risk management

Opening up systems to share data can include a number of risks related to digital security and the protection of privacy – both to the infrastructure and the data itself. Most commonly a traditional approach to data sharing is used. This approach aims to create a secure digital environment or perimeter to protect data's availability (accessibility and usability upon demand by an authorised entity); integrity (accuracy and completeness); and/or confidentiality (prevention of data disclosure to unauthorised individuals, entities or processes). However, this could impact innovation as it generally requires a higher degree of openness and interconnectedness (OECD, 2016g).

Where personal data are made available (even through access regimes with limited scope such as data portability) digital security risks may be higher. These incidents come along with significant costs to individuals but also to the firms suffering the data breaches. Additionally, advances in data analytics make it increasingly easy to generate inferences from data collected in different contexts, even if individuals never directly shared this information with anyone and even if the data have been (pseudo-) anonymised (OECD, 2016g).

Data ownership and IPRs

Data are an intangible asset; like other knowledge-based assets, they can be reproduced and transferred at almost zero marginal cost. So in contrast to the concept of ownership of physical goods, where the owner typically has exclusive rights and control over the good (including, for instance, the freedom to destroy the good), this is not the case for intangibles such as data. For these types of goods, IPRs are typically suggested as the legal means to establish clear ownership. In the case of data in particular, legal regimes such as copyright as well as other IPRs applicable to databases and trade secrets can be used to a limited extent. Furthermore, technologies such as cryptography have dramatically reduced the costs of exclusion, and thus are often used as a means to protect data (OECD, 2016g).

However, data provides additional challenges with respect to different stakeholders having different rights. For example, some stakeholders have "the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others" (Loshin, 2002). In cases where the data are considered "personal data" the situation is even more complex, since certain rights of the data subject cannot be waived.

3.5. *Financing new business models resulting from digital technology adoption*

Companies are increasingly using new business models to seize the opportunities created by digital technologies. Framework conditions are key to business innovation, particularly by new and small enterprises, since these are disproportionately affected by market failures, regulatory complexities and policy inconsistencies (OECD, forthcoming f). In particular, entrepreneurs may suffer greatly from liquidity constraints because of their lack of credit history and collateral to secure a loan.

The adverse consequences of credit constraints are particularly severe for firms specialising in digital and other "intangible" activities, such as innovation and services, as young innovators often lack physical assets (e.g. buildings, machinery, real estate, etc.) to offer as collateral. Even if their prospective business models were profitable, they are often unable to access credit (Cabral and Mata, 2003, Bottazzi, Secchi and Tamagni, 2014). These market failures justify the need for policy interventions aimed at facilitating access to finance, especially for new – often small – innovative entrepreneurs, including those whose business models rely heavily on digital technologies. In addition, information asymmetries typically lead to financing constraints for established SMEs with significant investment in intangibles, intangible-based business models, or which diversify into new lines of business or markets, including digital ones.

Difficulties in accessing financing are extensively recognised as one of the major obstacles for starting and growing a new business (OECD, 2006; Kerr and Nanda, 2009). Lack of finance typically prevents new ventures from investing in innovative projects, improving their productivity, financing their growth, covering working capital requirements and meeting market demand. Access to finance and start-ups' financial structures at inception are intrinsically linked to the characteristics of a start-up's assets and entrepreneurs' attributes. The difficulties that innovative entrepreneurs experience stem from several sources: they typically lack collateral and a track record; they are involved in innovation processes whose outcomes are uncertain; they deal with a non-rival good – knowledge – whose returns are highly unpredictable; and they own assets whose nature may be intangible and difficult to evaluate, particularly as entrepreneurs might not want to disclose information to investors about their innovations, due to the risk of imitation.

As advocated in the *G20/OECD High-level Principles on SME Finance*, a broad range of financial instruments is needed to seize growth opportunities and boost innovative investments. The importance of different types of finance varies across the stages of business development and across different business activities. During the seed and start-up stages, entrepreneurs, especially in technology-driven high-growth areas, can often obtain financing only from their own resources or from personal connections, as the information asymmetry is generally too high to be manageable for professional investors and creditors. Subsequently, once the business project is more advanced, self-financing may be supplemented by seed capital investment from informal private investors (e.g. business angels) and to a lesser extent by seed financing funds and venture capitalists for high-risk, low capital-intensive ventures, and by credit institutes (e.g. banks) for high capital-intensive, low-risk activities. In the expansion stage, young firms generally require increasing amounts of equity to maintain R&D and to expand marketing and sales activities, amounts that are typically only available through other sources, such as initial public offerings on stock exchanges and project financing.

Public equity markets for SMEs are especially suited for young, fast-growing companies, although compliance costs, which are often disproportionately high for small issuers, a general lack of awareness and ability to access these markets, as well as illiquid markets, constitute important obstacles. Hybrid instruments like

mezzanine finance, which combine debt and equity into a single vehicle, can also serve young and established companies that seek expansion capital, but that cannot increase their leverage, are not suitable for public listing or in cases where the owners do not want the dilution of control that would accompany equity finance. Other financing techniques exist in the broad risk/return spectrum that may serve credit-constrained innovative companies. These include: asset-based finance, whereby firms obtain funding based on the value of specific assets, including intangible assets, rather than on the firm's overall credit standing; and alternative forms of debt, such as corporate bonds, which can provide mid-sized to large firms with liquidity to undertake innovative investments (OECD, 2015g).

Digitalisation has the potential to overcome some of the market failures that limit the financing of innovative businesses and increase SME access to a range of financial instruments. The emergence of FinTech – combining technology and innovative business models in financial services – can enhance risk-assessment and the financing of small businesses at reasonable costs. While at a very nascent stage, the innovative credit scoring systems introduced by FinTech companies are promising to provide finance to business ventures that are often excluded from other sources of finance, at short notice and with relatively flexible conditions (OECD, 2016r).

Digitalisation has also directly resulted in new forms of external funding with the most prominent being crowdfunding, by which external finance is raised through web platforms from a larger audience than only specialised investors. Although it still represents a minor share of all business financing (and serves to finance specific projects rather than enterprises as a whole), crowdfunding may play a growing role, including for the financing of innovative ventures, as the online interaction with large numbers of customers may help entrepreneurs to validate untested products. Furthermore, venture capitalists, business angels and institutional investors are increasingly finding investment opportunities through crowdfunding platforms, usually through the largest and more developed platforms (OECD, forthcoming e).

External financing is especially important when innovative firms, particularly young firms, begin to grow, at which point financing requirements become too large to be met by family and friends. Indeed, the financing gap that affects innovative firms is often a "growth capital gap". Traditional debt finance generates moderate returns for lenders and normally requires tangible capital as collateral and is therefore more appropriate for established businesses with a low-to-moderate risk profile (OECD, 2015n). Recent evidence has shown that availability of financing, in particular access to VC and to loans, is one of the key conditions for young businesses to grow in sectors characterised by high-growth volatility and high-growth dispersion, such as IT-intensive sectors (Calvino, Criscuolo and Menon, 2016).

The development of diversified financing instruments and markets for innovative start-ups and SMEs requires appropriate framework conditions, in terms of regulation, taxation, transparency and connectivity. The design of financial regulations that optimally balance financial stability with the opening of new financing channels for entrepreneurs is essential, since the regulatory framework is a key enabler for the development of instruments that imply a greater risk for investors than traditional debt finance. This is even more the case in the face of a rapidly evolving market, where new financing models and risk mitigation measures are emerging and relatively unexperienced investors access financial markets. Empirical evidence has showed that policy settings, for instance on securities regulation, have important implications for the use of innovative financial instruments to support start-ups using innovative business models in the digital economy (Hornuff and Schwienbacher, 2015).

Since low levels of liquidity in SME growth markets (inherent in the SME asset class) act as one of the main deterrents to investment in SMEs, the development of equity markets for innovative young firms and SMEs strongly depends on specialised ecosystems that foster links between growth-oriented companies and a variety of specialised financial institutions and service providers. To address the lack of liquidity, in many countries policy has sought to increase connectivity and broaden the base of investors in innovative businesses, including through fiscal incentives for investors, such as front-end tax incentives (i.e. tax

deductions on investments in seed and early-stage ventures) and back-end tax relief (which relate to capital gains and losses).

Regulatory impediments to retail and institutional investors have been lifted in many constituencies. For instance, retail investors are encouraged to enter risk capital markets by increased threshold levels at which public disclosure and related requirements kick in, or by tax breaks for investment in unquoted companies that may subsequently list. Recent regulatory approaches recognise that public equity listings for SMEs may require tailored regulation and infrastructure to facilitate access by SMEs while preserving investor interest. In some countries, new markets offer growth-oriented entrepreneurs dedicated services, such as the introduction to experienced investors, or the possibility to retain a higher level ownership than a traditional IPO. Furthermore, policies to develop private and public equity markets for SMEs increasingly target training, mentoring, coaching and networking for investors (G20/OECD, 2016). In addition, governments increasingly recognise the importance of addressing the fragmentation of financial markets, by removing barriers to cross-border investment, to help SMEs tap into more diverse sources of capital and lower their costs of funding, as well as to broaden opportunities for investors and savers (G20/OECD, 2016).

Governments have also increased direct interventions to sustain the supply-side of the venture capital market by creating new government VC funds, and introducing fund-of-funds and public/private co-investment funds. The *G20/OECD High-level Principles on SME Finance* recognise the importance of public programmes to catalyse and leverage the provision of private resources and competencies in risk capital markets, and call for adopting principles of risk-sharing and mitigating mechanisms that ensure proper functioning of public measures, including the allocation of resources to their most efficient use, while avoiding excessive risk-taking against the public interest and potential crowding-out effects.

While the demand side of equity markets has received overall less policy attention in recent years, it is now increasingly recognised that to sustain the development of alternative financing instruments, demand- and supply-side impediments need to be addressed in tandem. On the demand side, many entrepreneurs and business owners lack financial knowledge, strategic vision, resources and sometimes even the willingness or awareness to successfully attract sources of finance other than traditional debt instruments. The *G20 High-level Principles for Digital Financial Inclusion* call for supporting and evaluating programs that enhance digital and financial literacy in light of the unique characteristics, advantages, and risks of digital financial services and channels. In this regard, investment readiness programmes can help entrepreneurs to better understand the advantages and risks of diverse sources of finance, the needs and expectations of potential investors, as well as to improve the quality and presentation of their business plans.

3.6. Key areas for policy action

Further investment in digital infrastructures, especially high-speed networks and data itself, is essential to support a vibrant, innovative and inclusive digital economy. Innovative enterprises that are looking to implement new business models in their production activities, distribution, etc. are also critical in this regard. At the same time, access to finance is a key challenge. There are a number of areas in which governments could play a role to help address some of these concerns including ensuring that that the right frameworks are in place to incentivise investment in infrastructure, particularly in unserved areas, and reducing barriers where possible.

Strengthen infrastructure deployment through a mix of public and private financing

There are a number of areas in which governments can take action to encourage further investments in telecommunication infrastructures, especially high-speed networks. In particular, governments have a role to play in unserved and underserved areas. Such investment can take the form of PPPs, where public funds are invested in co-operation with private actors, ranging from utility companies and network operators to local

businesses or co-operatives of local residents (PPPs are discussed in more detail in Chapter 2 on infrastructure).

There have also been some cases in which governments have largely financed new infrastructure, such as the national wholesale fibre networks in Australia and Singapore, although private investment provides the largest contribution in most G20 economies, such as in Canada, India and the United States. Regulatory frameworks should be reviewed to ensure that they are appropriate for the levels of investment necessary to achieve their policy goals. Regulators should promote an optimal level of investment and robust competition in high-speed networks and services. Spectrum is another area where consideration could be given to focus less on generating revenue for governments and more on establishing an accurate market value.

Additionally, a role that is best placed with governments and international organisations is strengthening the collection of internationally comparable statistics on the use of digital infrastructures, particularly global data traffic flows. Better understanding of the evolving state of fixed and mobile broadband across the world will lead to better, more targeted policy actions by governments. A call to the G20 to work with international organisation such as the OECD and the ITU could advance this work.

Improve framework policies to foster financing of digital infrastructures and new business models

The availability of financing for innovative and new business models is influenced by a range of policies (OECD, 2015g). Framework policies are one important factor that affects the financing of innovation: significant benefits arise from increased access to seed and early-stage financing, as well as from increased efficiency in the judicial system. Promoting effective and predictable insolvency regimes to ensure creditor rights can strengthen the confidence of a broad range of investors in SME markets. In addition, taxation, product market as well as employment protection legislation, policy-induced barriers to exit (e.g. excessively strict bankruptcy laws) are found to impact the financing opportunities for companies. Reducing such barriers will accentuate competitive pressures, encouraging inefficient firms to exit, and channel resources to firms that are best able to make use of the resources. While such measures are typically implemented with other policy objectives in mind, their unintended implications for innovation have to be taken into account. Types of policies that could be considered include:

- **Supply-side interventions**: A number of countries have had grants, loans and/or guarantee schemes in place for many years, for example increasing tax incentive programmes. These include front (investment) and back (capital gains) end incentives for investments in young firms. There has been a noted increase in the use of equity instruments, particularly in co-investments funds and fund-of-funds which seek to leverage private investment (Wilson and Silva, 2013). The work on identifying effective approaches for the implementation of the *G20/OECD High-level Principles on SME Financing* can provide evidence on common and innovative policies to sustain the financing of innovative start-ups and SMEs.
- **Demand-side interventions**: The demand side is often overlooked in favour of supply-side actions. Many entrepreneurs and business owners lack financial knowledge, strategic vision, resources and sometimes even the willingness or awareness to successfully attract sources of finance other than traditional debt instruments. Developing human capabilities and social capital is critical to success of early-stage ventures, as well as to enhancing digital financial inclusion, as advocated by the *G20 High-level Principles for Digital Financial Inclusion*. Initiatives to create a more entrepreneurial culture are also vital as in many countries the fear of failure is higher than perceived opportunities. There has been growth in programmes such as incubators, accelerators, business angel networks and matchmaking services in several countries (Wilson et al., 2013). G20 could share best practices and facilitate connections between these programmes across countries.
- **Addressing regulatory and administrative barriers**: Regulatory and administrative barriers to seed and

early-stage investment can affect institutional investors, VC funds, angel investors and high-growth firms. Bankruptcy regulations, labour market restrictions and other framework conditions all play a role. Securities legislations and increasing restrictions on institutions investors, particularly those on banks, pension funds and insurance companies, can also be barriers to investment in seed and early-stage companies (Wilson et al., 2013).

- **Evaluating and assessing the full policy mix**: Despite the growth of supply-side interventions, there is little evidence of the impact of these instruments and whether or not they crowd out private investors. Policy interventions should not be seen in isolation but as a set of interacting policies (supply side, demand side and framework conditions). Effective evaluation and periodic adjustment of the specific policy instruments as well as the full policy mix is needed.
- **New platforms for financing innovative business**: In recent years, FinTech developments, such as crowdfunding and peer-to-peer lending, have been increasingly used for both debt and equity funding. Related regulatory reforms have aimed to ease the development of this emerging financing channel, while addressing concerns about transparency and protection of investors. In addition to regulatory changes, public action may also take the form of support to industry networks or aim at improving information about funding opportunities (OECD, 2015h). In particular, it is important to encourage investor participation in crowdfunding and innovative firms' uptake of alternative investment instruments increased which will overall imply new infrastructures to reduce information asymmetries. In this regard, broader developments in FinTech may contribute to enhance risk-assessment in financing markets and reduce the costs of financing new and small innovative businesses.

4. DEVELOPING STANDARDS FOR A DIGITAL WORLD

- Open, voluntary standards, grounded in bottom-up and market-led approaches, are an important tool especially when dealing with fast developing technologies and shifts in markets. Such standards and related guidelines are needed to maintain current levels of safety, ensure trust based on enhanced levels of digital security and privacy, improve energy and resource efficiency, and address emerging social and organisational challenges brought on by the digital transformation.
- The development of standards and standards-based interoperability is critical for the development of Industrie 4.0 and the IoT, including smart cities and smart mobility. The key to success lies in inclusive standards development, built on collaboration and co-operation among the many players that make up the standards ecosystem. G20 leaders could support the adoption of best practices and policies that enable groups/actors, including SMEs, to more effectively work together within the variety of processes used to develop standards.
- Advanced governance frameworks – building upon both existing public- and private-sector-led processes – and new multi-stakeholder initiatives for the benefit of all, as well as improved or new policy and implementation tools, are necessary to effectively address the complexity of today's interlinked issues in successful Industrie 4.0 development and deployment. The G20 could play a role in creating an architectural framework for Industrie 4.0.

4.1. The policy challenge

Standards impact many different policy areas and help foster increased innovation and productivity; promote competition in open markets; enable international trade; and reinforce trust among stakeholders. Standards are particularly critical in highly technical areas, including those that make up Industrie 4.0 and the IoT. In the case of sophisticated manufacturing and the IoT, machines need to be able to communicate with each other seamlessly, and with respect to the IoT, applications span a wide range of policy domains, including health, education, agriculture, transportation, manufacturing, electric grids, among many others.

4.2. Developing standards in an interconnected environment

It is anticipated that the IoT will usher in a revolutionary, fully interconnected "smart" world, with integrated relationships among objects, people, and their environments. This complexity will be compounded by multiple factors: the fact that no single company possesses enough expertise to address the entirety of the IoT picture in a timely and economically viable fashion; the emergence and adoption of new technologies and disruptive business models; and, the addition of billions of people coming online as a result of both world population growth and digital development across geographic regions and industry domains.

Although consumer and integrated commercial-consumer IoT systems and devices, such as self-driving cars and connected thermostats, receive the most prominent coverage in the popular press, the largest impact of the IoT may well be in business applications for the commercial/industrial IoT. Cyber-physical systems – machines that sense their environment; collect, analyse and act on data; and collaborate with each other and with humans – stand to transform industrial sectors as varied as manufacturing (e.g. Industrie 4.0), energy, and agriculture, which together account for nearly two-thirds of global gross domestic product (WEF, 2015b). McKinsey Global Institute (2015) estimates that approximately 70% of the USD 4 trillion to USD 11 trillion total value derived from the IoT will be captured by business-to-business applications.

The development of standards and standards-based interoperability is no less than a linchpin to Industrie 4.0 proliferation. While some companies perceive competitive advantages and economic incentives in building proprietary systems for the IoT, overall economic opportunities would be constrained in a marketplace of disparate silos. In a World Economic Forum study, 47% of respondents indicated that establishing and promoting common standards is an important action that governments can take to accelerate the adoption of the Industrial Internet (WEF, 2015b). Ultimately, Industrie 4.0 will demand no less than a neutral, standards-based reference architecture, if the production industry is to successfully create value-added networks. Moreover, appropriate standards and guidelines are also needed to maintain current levels of safety, ensure trust based on enhanced levels of digital security and privacy, improve energy and resource efficiency, and address emerging social and organisational challenges brought on by digitalisation.

As economies move towards an IoT-enabled future, reinforced by standards-driven interoperability and by societal acceptance, the various actors involved need to think and act strategically and in a co-ordinated and collaborative fashion so that the maximum advantages and benefits of Industrie 4.0 can be realised. It is likely that unco-ordinated and non-collaborative standards-setting actions – be it by public or private actors – would inhibit interoperability and slow down the adoption of better security and privacy practices, with potential negative effects on human rights and ethics. If these concerns are not addressed in a way to garner user confidence, IoT deployment and advances in sophisticated manufacturing could be significantly hindered.

While a co-ordinated approach is the best way in which to develop fully interoperable standards, it is not always possible (or necessary) to do so. This is in part because buyers may be cautious in purchasing (and using) products and services that are connected to the IoT ecosystem if the IoT integration mechanisms are inflexible and they will in turn become "locked in" to the ecosystem, among other issues (Internet Society, 2015a). There are also additional concerns with respect to poorly designed and configured IoT devices and the disruptive impact they could have on the broader Internet and the digital economy (Internet Society, 2015a). Using standards that are generic, open, and widely available as technical building blocks for IoT devices and services would benefit economic opportunities and innovation.

While such standards are not policy objectives unto themselves, they become a priority as a means to transition technology to, and develop, markets and there is an increasing interplay between standards and policy. Depending on the particular governance model, standards can provide support to many kinds of policy actions, including innovation and productivity, trade and competition policy, investment policy, technical regulation, consumer protection, security, safety, and environmental protection. In such ways, standards can serve as powerful instruments of governance, because of the effects their use can have on regulations, goods, services, and quality of life.

These effects are evident whether standards are employed by the private sector or by the public sector. In the private sector, standards create market incentives for actors to follow internationally accepted practices by applying competitive pressure (while allowing fair competition) and also encourage innovation and growth by fostering technological development when based on broadly available and open technology platforms. In the public sector, standards can enable greater transparency and competition in public procurement and provide essential guidance for industry via their referencing into regulations and laws. In either context, standards can considerably improve efficiency and cost-effectiveness and support consumer protection (in areas such as security, privacy, safety, competitiveness, etc.) as well as reduce transaction costs (Hufbauer, Kotschwar and Wilson, 2001).

4.3. The global standardisation landscape

Given that the development of standards and standards-based interoperability are such key components in the IoT and Industrie 4.0, a review of the global standardisation landscape is worthwhile. There are many standards families, which may cause difficulty in determining whether a standard fits a situation well or whether it will be supported industry-wide and in the future. All actors, including researchers of IoT technologies and solutions, would gain from familiarising themselves with existing standards and standardisation initiatives to avoid duplication of efforts.

In the world's increasingly elaborate and complex landscape of standards and standardisation, there are many fora or avenues for the development of standards. In the Internet era, the categorisations of the past (*de jure, de facto,* formal, informal, etc.) are less relevant. Instead, organisations have emerged focusing on several broad areas.

There are organisations that are based on different modes of national representation, both at national or regional level, such as the European Committee for Standardization-European Committee for Electrotechnical Standardization (CEN-CENELEC), European Telecommunications Standards Institute (ETSI),[4] Telecommunications Industry Association (TIA), InterNational Committee for Information Technology Standards (INCITS), etc., as well as the globally acting International Electrotechnical Commission (IEC), International Organization for Standardization (ISO) and International Telecommunication Union (ITU).

There are other globally active organisations but with direct membership models, such as IEEE (a technical professional organisation that among other things, develops standards), Internet Engineering Task Force (IETF), Organization for the Advancement of Structured Information Standards (OASIS), and World Wide Web Consortium (W3C). Generally, pursuit of public interest plays a more or less explicit role in the missions of these organisations.

There are also fora in the form of consortia or alliances within industries or businesses coming together to develop and support a standard by mutual agreement. These are usually formed by companies aiming at developing standards to their specific interests. The degree of openness of their membership models varies, but they often have similar processes as traditional Standards Development Organisations (SDOs) (DeNardis, 2011).

In addition, the new era of standards development is progressing to requirements-development communities striving to build global ecosystems to address necessary standardisation (such as those within the Industrial Internet Consortium and OpenFog Consortium). These communities address architectural framework deployment requirements and necessary go-to-market support, along with consideration for education and compliance.

BOX 3. CO-OPERATING AND COLLABORATING ON INTERNATIONAL STANDARDS

A positive example of co-operation among standards bodies took place in July 2016 in Singapore where representatives of IEC, ISO, ITU, IEEE, CEN-CENELEC and ETSI convened at a meeting initiated by IEC to discuss means of accelerating and better aligning their standardisation work in support of smart cities. With over half the world population now living in cities, ICTs, mass transport and renewable energy are becoming ever more important. In today's cities much of the infrastructure is installed by a diverse set of suppliers and maintained by different agencies that sometimes work in isolation. The interconnection of city systems will demand standardised interfaces, and this is where standards bodies such as IEC, ISO, ITU, IEEE, CEN-CENELEC, ETSI and others will have an important role to play as they work as a collective.

At the national level, there are also examples of co-operation on standards. In the United States, the National Technology Transfer and Advancement Act (NTTA), signed into law in 1996, recognised the value and impact of voluntary, co-operatively developed standards. It mandated that all federal agencies use technical standards developed and adopted by voluntary consensus standards bodies, as opposed to using government-unique standards.

Another example is the European Union Regulation on European Standardisation, approved in 2012, which included a framework to reference ICT technical specifications in policy and procurement, which essentially recognised the value of referencing voluntary, global technical specifications to help benefit European consumers and promote European competitiveness.

In the China Standardization Reform, a five-year plan initiated in 2015, a reorganisation of Chinese standards encompasses a greater emphasis on social organisations, which include standards developed by federations, associations, and consortia, in addition to mandatory national standards where the government plays a leading role. The reform encourages qualified social organisations and industry alliances to develop standards, replacing government-led standards development.

4.4. Approaches to developing standards in the digital era

It will be particularly important to take into consideration the forthcoming integration of new and emerging technologies on the IoT horizon, including those associated with artificial intelligence and robotics, and body area networking (i.e. a wireless network of wearable computing devices), together with the societal and ethical challenges they are bringing with them. Furthermore, the convergence of ICTs, as evidenced by innovations such as software-defined networking and virtualisation, points to dramatic changes over the next decade for current market models. The synergy of these new technologies – along with advances related to battery/energy efficiencies, coupled with rapid progress in more mature technologies – will provide the IoT enablement for consumer, commercial/industrial, and integrated commercial-consumer applications.

The diversity of potential IoT applications and device technologies may lead many to conclude that it would be detrimental to be tied in at an early stage of technological development to one-size-fits-all type of standards or standards that might prove burdensome or conflicting. However, a certain level of standardisation and interoperability will be necessary to achieve a successful IoT ecosystem and, over time, technological maturity will help identify the most promising standardisation approaches. In addition, standardisation areas for the IoT such as orchestration, protocol management, identification, spectrum requirements, hardware-based security guidelines, plug-and-play management, etc. could transcend specific technologies and would involve ongoing assessments.

Today, the global state of play for IoT standards is marred by a definitive lack of integration and alignment, as well as by a lack of actors considering the broad picture. Many protocols and limited interoperability exist across the disparate technologies and markets of the IoT, and many bodies, specialised in relatively narrow fields of technology, are striving to establish themselves as leaders in the space. This could result in a continued lack of interoperability among existing systems and would significantly increase complexity and cost in Industrie 4.0 deployments while limiting performance. A fully functional digital ecosystem requires at least seamless data sharing between machines and other physical systems from different manufacturers. The drive towards seamless interoperability would be further complicated by the long life span and capitalisation policies associated with typical industrial equipment, which would require costly retrofitting or replacement to work with the latest technologies.

There is an increasingly complex relationship between digital standards and patents in some areas. Compliance with some standards may require the use of one or more patents, called "standard-essential patents". Therefore, standards organisations often require members to disclose and grant licenses on fair, reasonable, and non-discriminatory (FRAND) or royalty-free (RF) terms to their patents and pending patent applications covering a standard that the organisation is developing. However, determining which patents are essential to a particular standard can be complex. If a standards organisation fails to get licenses to all patents that are essential to complying with a standard, owners of the unlicensed patents may demand or sue for royalties from companies that adopt the standard (Blind and Kahin, forthcoming). Such situations may create barriers to standards adoption and reduce incentives to participate in standards making processes (Blind and Kahin, forthcoming).

Key policy issues related to standards include:

- Facilitating IoT/Industrial Internet/IIoT interoperability with minimised fragmentation.
- Fostering a bottom-up, inclusive, and transparent approach of open standards development to more fully address the needs of industry.
- Encouraging industry actors to think and act strategically and in a co-ordinated and collaborative fashion.
- Encouraging multidisciplinarity and inclusivity of a variety of cultures and generations in open standards' development processes.
- Fostering broad standards that result from public/private partnerships rather than narrow, special interests.
- Understanding relationships among integrated vertical markets.
- Aligning better open source and open standards.
- Approaching standards – without making their use mandatory – as a means to support policy actions and as a tool, among others, to support certification and regulatory compliance requirements.
- Addressing issues related to the relationships between standards and patents.
- Incorporating privacy, digital security, and consumer issues at the very beginning of technology and standards development.
- Supporting inclusivity for SMEs, academia, and emerging economies.
- Encouraging new actors to participate in standards development for social, ethical, environmental and other issues to be sufficiently taken into account.
- Addressing trust and ethical issues collectively, in an open and transparent manner.

As actors navigate the IoT space, they would need to consider that just as the standards for the Internet evolved to open standards, the same is likely to happen for IoT. As integration grows more complex, systems become globalised, and technological innovation continues, a gradual, ongoing migration is likely to take place through interrelated cycles:

- An experimental stage where organisations are trying and testing proprietary protocols and mechanisms, some of which may not lend themselves to standards,
- Consolidation, where some protocols merge and some become redundant, and
- Commoditisation of open standards, in which a foundation or system of standards is established upon which new developments are made and advanced.

Throughout this lifecycle-management process, the common values of openness, transparency, and inclusiveness that led to the development and refinement of the today's foundational, open Internet standards are also likely to be the crucial building blocks on which interoperability of standards, approaches, and policies can be jointly developed for the IoT and Industrie 4.0 more broadly.

The case for voluntary standards

Voluntary standards are typically set by open SDOs, based on the consensus of the participants who develop or intend to use them, and they are adopted by voluntary compliance – as opposed to being mandated by regulation. There are instances in which government authorities may decide to refer to a voluntary standard to guarantee a minimum level of protection, but in general, the market decides the adoption and use of voluntary standards.

Experience shows that voluntary standards have helped create ecosystems that promote economies of scale and healthy competition. This is essential to help ensure that markets remain open, allowing consumers to have choice and new entrants to successfully enter markets. The development and evolution of technologies on which the Internet is based deliver a compelling example of the power of voluntary, bottom-up standardisation. The Internet evolved from a networking community to a global collection of communities, and its widespread information infrastructure has resulted in today's digital economy. Following an initial incubation period, the standards on which the Internet was built evolved within a globally open, inclusive, and decentralised model. This process has allowed for diversity of opinions and approaches as well as flexibility to acknowledge and address change and varying needs, opening the door to innovation by leveraging and expanding knowledge.

The suite of standards that form the foundation of the Internet are deployed through the collaboration of many participants from all around the world. Together, they have been a key facilitator of the growth of a global economic and social model that has touched billions of lives. The Internet economy of the G20 nearly doubled between 2010 and 2016 and it employs 32 million people today. All signs point to continued, strong growth in the Internet economy in the G20 in the coming years. Further, the Internet enables the IoT where actors in manufacturing, mining, oil, gas and utilities are rapidly moving in with investments in the Industrial IoT market, spanning industries representing 62% of GDP among G20 economies (BCG, 2012).

Thus, voluntary standards have helped to make progress in key areas such as enhanced public health and safety; technology innovation; market expansion and job growth; and the roll-out of more sound and interoperable products at a lower cost. A specific example of the impact of this type of voluntary open standards can be found by examining the many applications for the global suite of Ethernet technology standards. Ethernet ranks highly among those technologies that affect day-to-day life on a global scale. From data centres, personal computers (PCs), laptops, and smartphones to power infrastructure and smart meters, personal medical devices, connected cars and more, Ethernet touches all established and emerging

technologies through the collective contributions of individuals in industry, academia, and government. These types of standards provide the underpinnings of social well-being, and their value and necessity are coming into sharper focus in the age of globalisation.

BOX 4. DEVELOPING STANDARDS: THE EXAMPLE OF WI-FI

IEEE 802.11, more commonly referred to as Wi-Fi, is an IEEE standard for communications in wireless networks that is voluntarily deployed around the world, and whose technology has become ubiquitous. It has generated significant market growth and impact through innovation, providing economies of scale.

The Wi-Fi market is expected to show tremendous growth in the next five years. The hotspot 2.0 and IEEE 802.11c Wave 2 will offer great revenue generation opportunities for the mobile service operators (MSOs). The usage of IEEE 802.11ac is becoming a common standard for service providers, mostly used for smart devices to connect with each other via Wi-Fi. Wi-Fi standards are important for the ISPs to maintain and understand its limits. The standards offer uninterrupted Internet speed and service to the consumers.

The upcoming changes and advancements in the wireless standards will only offer better Internet experience to the consumers. Compared to the mature markets such as North America, the Asia-Pacific and Latin American regions are expected to grow at quite high rates in the next five years with compound annual growth rates of 22.6% and 20.2%, respectively.

The growth rate of the Wi-Fi market in the Asia-Pacific is propelled by factors such as high development in wireless and smart devices, increase in construction of smart highways and cities, and increasing government participation and support, among others. In developing countries such as China, India, and Brazil, among others, the deployment and usage of Wi-Fi is increasing due to intervention and support of the government. The wireless hotspots for the citizens have been booming in these developing countries.

Citizens in many countries such as the United States and Singapore, among others, have been offered municipality networks to stay connected and use this connectivity during any crisis or emergency situation. The local and regional police departments are benefiting from the city-wide municipality networks and hotspots deployed. The companies in the Wi-Fi market are thriving to offer the largest Wi-Fi network in various countries, starting with the United States and Canada. Various cities such as Boston, Chicago, Houston and Philadelphia, among others, have municipality networks deployed on public transportations to increase the ridership and offer better travel experience to the public (MarketsandMarkets, 2015).

Standardisation processes that are universally open and transparent from the beginning can help establish trust in platform adoption and use, which in turn can strengthen the “network effects” of digital platforms. The voluntary standards-development paradigm also serves as a best practice model – grounded in a bottom-up and market-led approach – to provide open access and respond quickly to the accelerating pace of technology change and shifts in markets.

Voluntary standards are often driven by the private sector, in which private-sector actors work across the various SDOs, trade associations, consortia, or alliances in the standards ecosystem. In times of accelerated rates of technology development and convergence, the private sector is often better suited than governments to develop standards in many areas. However, the emerging explicit intersection of ethics and technology in the field of standardisation demands new models of open and collective collaborations, with inclusion of new actors.

The private-sector-led standards paradigm of development of technical specifications within industry consortia or alliances is considered more focused on particular market needs or opportunities, as well as targeted technology integration. As noted, consortia standards-development bodies' members are primarily enterprise actors. Their output has been increasingly influential in the past decades due to several factors. These include increasing market influence of transnational corporations and the emergence of GVCs across various countries. Often co-ordinated by "lead firms", members of consortia use common technical specifications as a means to govern market-deployable value chains across the globe to help ensure coherence between value chain partners. In the consortia model, technical specifications can often be developed and deployed in the market more rapidly than those developed in other paradigms since the actors are not seeking wide industry input or consensus, and are focused on particular vertical markets or specific technology domains and solutions.

Voluntary standards can serve as tools to help users meet regulatory requirements. In cases in which the law requires a particular outcome, voluntary standards may offer an effective means to achieve this, but without these means ever being mandatory; they are simply recognised as valuable. Any organisation remains free to use any means other than those in the voluntary standard, provided that the outcome required by law is achieved.

The current standardisation system reflects the more traditional industry supply chain focused on products and the efficient movement of physical goods. Industrie 4.0 and IoT applications are forging new paths to standardisation systems that are more aligned with industry efficiency, serviceability, and supply and value chains focused on an outcome economy.

In the emerging "outcome economy", businesses compete more on their ability to help customers achieve quantifiable results than on the product used to achieve those measurable outcomes. To thrive in this environment, companies will increasingly rely on business partners, connected ecosystems, advanced analytics, and new data management streams from smart products in the field to gain timely insights about customer needs and behaviours.

At the same time, a more agile standardisation system for the IoT and Industrie 4.0 is taking shape. In a time of exponential change driven by the rapid rate of technological development in IoT, the capacity of open standardisation processes to become more agile will be essential, especially to reach the level of interoperability necessary to realise its full-scale benefits.

4.5. *Ecosystems, SMEs, and overcoming standards-related barriers*

How, and to what extent, companies invest their time in standardisation is contingent on the role that they specifically play. No one company or government can build the IIoT alone. And developing the technology and related capabilities to deliver business outcomes is a challenging task. Few companies, even the world's largest ones, are in a position to entirely "own" Industrie 4.0's emerging digital value chains.

To be successful, companies increasingly need to have a clear strategy on how they want to participate in emerging industry platforms and ecosystems. There are a number of possible lead and supporting roles: platform owner, data supplier, service aggregator, and so on. Since delivering outcomes often demands problem solving above the level of an individual product or solution, companies will gain from working together to meet the needs of customers and societies at large. For example, in an application space as complex as IoT for smart cities, the corporate logic of an individual manufacturer/supplier will need to account for potentially far-reaching social, environmental, ethical, and socio-political questions. Such questions will be best addressed collectively in requirements-oriented communities of interrelated actors.

As IoT and Industrie 4.0 comprise a cross-disciplinary and cross-industry sector, increasing levels of collaboration across ecosystems of business partners will be expected to bring together players that combine

their products and services to meet customer needs. Software platforms will emerge that will better facilitate data capture, aggregation, and exchange across the ecosystem. These platforms will help create, distribute, and monetise new products and services at unprecedented speed and scale. To avoid winner-take-all outcomes and encourage a fair sharing of the value created by the participants in the emerging networks, some basic rules may need to be set, both by bottom up (self-regulation) and top down (suggestion of some broad principles by regulators). Also, being part of an ecosystem will allow participating companies to specialise in their core competencies and work together to quickly adapt to changes in external environments.

Open, voluntary standardisation with clear rules of engagement will foster the creation of ecosystems that promote economies of scale, healthy competition, and participation by SMEs and emerging economies. A promising role for SMEs in Industrie 4.0 would be to become the research engine for technology and application development, with large enterprises addressing infrastructural frameworks and drawing on SMEs' innovative research. In this respect, the effective integration of SMEs into the evolutionary technology standards process is crucial to the overall success of the Industrie 4.0 endeavour, and requires helping SMEs to better understand the complexity of the standards ecosystem and the globally offered possibilities, thereby unleashing their direct engagement in global standards-setting activities.

Ensuring trust is essential to fostering uptake of the IoT

An important consideration is that the IoT will not flourish without consumer trust (security, privacy, and safety) in IoT devices, systems, and use, and G20 leaders and governments may consider acknowledging and encouraging open, inclusive, and agile standardisation paradigms and resulting standards that fuel interoperability and competition and provide customer choice. In this respect, the Internet Society's Collaborative Security[5] -- which frames an approach to addressing Internet security -- could be a useful reference (Internet Society, 2015b). It notes that any digital security framework needs to start with an understanding of the fundamental properties of the Internet (open standards, voluntary collaboration, reusable building blocks, integrity, permission-free innovation and global reach, and an appreciation of the complexity of the digital security landscape). An overarching objective could be to foster trust and protect opportunities for economic and social prosperity.

Furthermore, improving security on the Internet needs to be considered within a broader context of trust and respect of fundamental human rights and values, such as privacy. In this regard, the *OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity* (OECD, 2015k) and *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013d) may be helpful as they provide a set of internationally agreed high-level principles that can be used to drive the development of standards that support security, privacy and trust (see Chapter 6 on digital security).

Finally, multi-stakeholder cross-border collaboration is essential. Commercial competition, politics, and personal motivation play a role in how well collaboration happens. But, as collaborative efforts have demonstrated, differences can be overcome to co-operate against a threat. Such voluntary, as-needed "working for the benefit of everyone" collaboration is remarkable for its scalability and its ability to adapt to changing conditions and evolving threats, yielding unprecedented efficacy.

4.6. Key areas for policy action

As mentioned above, standards are not policy objectives onto themselves. They are, however, a means to promote economic development, and their role extends to public policy, including fostering increased innovation and productivity. Open standards, in particular, enhance competition in open markets, support international trade and help reinforce trust among trade actors.

Promote open, voluntary standards through collaborative mechanisms

Co-operation among standardisation actors, encouraged by policy makers, help facilitate market development by promoting diffusion of enabling technologies. This would improve efficiency, foster interoperability, and address needs such as safety, security, and accessibility. G20 leaders and governments may call for policies that recognise global, open, voluntary standards developed under direct participation models with a view to reinforcing developments among governments in this realm.

As industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, governments could encourage national industry to collaborate in globally open standardisation efforts to develop technological best practices and standards. Specifically, they could encourage the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. The emphasis on commercially available solutions and market-adopted voluntary standards would allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner. PPPs could leverage existing industry standards and investments and utilise both public and private resources to facilitate the research, leadership, and governance to advance respective nations' IoT vision.

The IoT will produce a considerable amount of data that can improve productivity across industries through predictive maintenance on equipment and machinery. This data will hold valuable potential to develop important insights into new business risks and opportunities as correlations and associations are made. A challenge will be finding ways to analyse the volume of performance data and information. To keep up with IoT-generated data and gain the promise of its insight, machine learning will be critical. In short, artificial intelligence will emerge as the standard way of managing, interpreting, and acting on IoT. From a standards perspective, this will bring to the forefront the need for a new type of "hybrid" standard to emerge – standards that go beyond technical aspects to encompass trust and ethical dimensions, among others. This will require unprecedented collaboration and co-ordination among multiple disciplines.

G20 leaders and governments could support best practices and policies that enable groups/actors within the variety of forms of standardisation to more effectively work together. The various forms of standardisation serve a purpose, especially in the ICT sector where there is the need for stability (provided by the arena of open standards bodies), a need for coping with fast change and the need for specific intellectual property and marketing environments (provided by consortia and alliances), and the need for robust community involvement (provided by Open Source Initiative). To tackle the vast emerging standardisation needs for large-scale systems, such as integrated digital platforms, as well as the IoT, 5G, smart cities, and other smart "Xs" (homes, vehicles, connected person, government, health, etc.) the groups within each arena will need to more effectively work together, also in order to achieve the public good character of standards through open systems. In order to accomplish this, open standardisation is likely to be more appropriate than tightly controlled proprietary solutions (Schoechle, 2009).

Encourage an interoperable environment in support of the IoT and Industrie 4.0

The IoT will become as commonplace as electricity in daily life, with many billions of interactive objects connected to devices, equipment, machines and infrastructure. It is expected to bring many economic and social benefits such as fostering the creation of start-ups, generating new economic value, helping meet the needs of an increasingly elderly population or paving the way for environmentally friendly and inclusive smart cities. At this still early stage, the G20 may have a unique opportunity to help usher in the IoT in an enabling environment that both promotes its many benefits and addresses the challenges, particularly around safety, security and privacy.

As a result of the vast diversity of IoT application topic areas and domains, and the vast heterogeneity in their goals and requirements, many IoT devices and techniques will exist, and interoperability will be crucial. While

the current explosion of products and services is the signal of a growing IoT marketplace to some, a fragmented ecosystem with non-interoperable technologies could undermine the efficiencies achieved by large economies of scale and significantly delay the deployment of IoT. The IoT ecosystem will employ hardware and software from many different vendors, and the ability to employ functionality from many devices and vendors will be key for IoT techniques to reach their full potential. To solve this problem, an effective approach would be to rely on global, voluntary interoperable standards developed by standards-development organisations or industry consortia aiming at such interoperability.

Interoperability at the semantic level[6] is an area of particular concern. Standards and vibrant ecosystems fuelled by diversity are key to developing semantic interoperability for the IoT. For example, the IEEE Standards Association (IEEE-SA), Alliance for Internet of Things Innovation (AIOTI), oneM2M and W3C are collaborating on a joint white paper addressing this need. The diversity of potential IoT applications, device technologies, and business and operational models will require flexible approaches, and avoiding to tie the IoT ecosystem prematurely to burdensome or conflicting standards, particularly those of a one-size-fits-all nature. Furthermore, rapid technology innovation in this domain may mean that early approaches will be quickly surpassed.

In this regard, the G20 may wish to agree on the importance of working together to prepare for the IoT and begin to foster a common, interoperable environment in support of it, and the regulatory challenges that the IoT represents. In a second step, G20 economies may consider taking specific collective actions in this regard.

Enhancing core competencies

Given that ecosystems are critical to the success of the IoT/Industrie 4.0, G20 leaders and governments may consider policies that support participant actors and companies in enhancing their core competencies while efficiently working together. As SMEs could effectively serve as the research engine for technology and application development in Industrie 4.0, G20 leaders and governments may consider the merits of policies that support SMEs' integration into the IoT evolutionary process and encourage and promote standards bodies to have open and inclusive processes, with clear rules of engagement that elicit SME participation. The European Union Regulation on European Standardisation framework facilitates representation and participation of SMEs in the standardisation process, redressing the situation where, in general, SMEs were under-represented in European standardisation activities, may be a useful reference.

5. REGULATION OF THE ICT SECTOR

- Fixed-line communications, wireless communications and broadcasting used to be separate regulated services provided over different networks, but they are now converged in many G20 economies on one general-purpose network: the Internet. This has created a need for countries to review their regulatory frameworks and public policy objectives in a more holistic manner to ensure they optimise incentives for all market participants to continue to innovate, compete and invest.
- Ensuring a 21st-century approach to the ICT sector may involve removing regulation where it is no longer necessary or extending the scope of regulation to new service providers. It may also entail creating converged regulators and /or adjusting regulatory powers so they can oversee all elements of bundled services and ensure consistent consumer protection.
- Promoting competition in the converged communications environment is another important challenge. In mobile network markets, solutions may include blocking mergers between mobile operators that would harm competition, introducing conditions to facilitate market entry of new providers, facilitating consumer switching, and enabling network sharing as an alternative to consolidation. With respect to fixed network markets, one solution may be to facilitate efficient access to passive infrastructure to increase the number of providers able to offer high-speed services.
- At the G20 level, a comparative analysis of the effects of convergence on competition and innovation across countries would help to further inform policy actions. The analysis could include elements such as the regulatory environment, mergers and acquisitions, investment and revenue, access paths (fixed, mobile and M2M) and network neutrality rules among others. The development of a "converged analytical framework" to benchmark G20 countries could contribute to a more informed debate on the effects of specific policy actions.

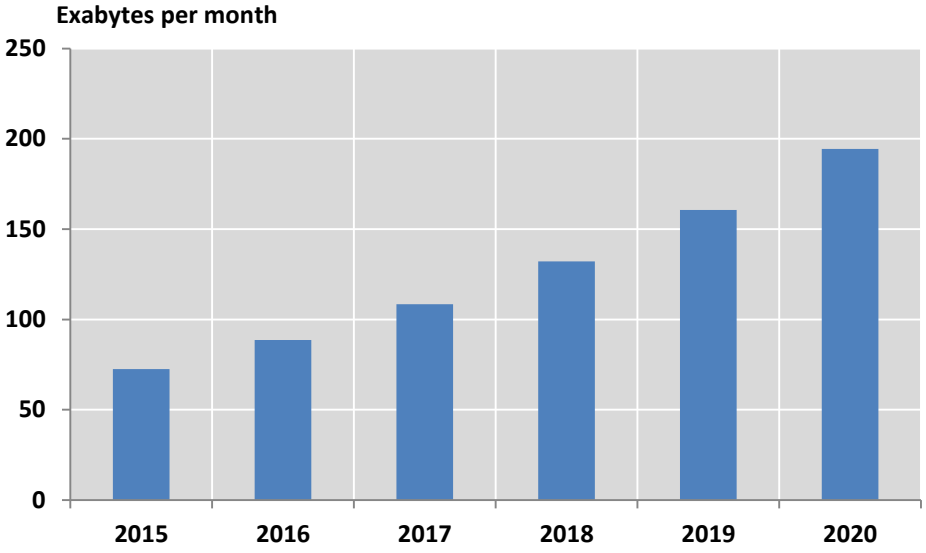
5.1. The policy challenge

In today's ICT sector, successful innovators can grow into global giants in just a few years while dominant incumbent firms can evaporate in the same time span. Where the next giant comes from depends on many factors, but a major one is related to the capacity of regulatory frameworks to further digital development, as part of a policy mix of regulatory best practices and market mechanisms to promote competition, innovation and investment in the ICT sector.

Few sectors have experienced more change in recent years than the ICT sector and more is on the way. Business models that were built on separate fixed, wireless and broadcasting infrastructure have converged, and services that were formerly provided over different networks are now offered over a single pathway – the Internet. In this environment, policy makers and regulators are challenged to promote competition and consumer choice while fostering innovation and investment. In the converged scenario where innovation at the core and at the edge of the network is more prominent and often disruptive, where services and applications are decoupled from the network, and where industry consolidation is increasing, traditional approaches to regulating communications and television markets may no longer be fit for purpose.

The growing dependency on communications highlights the criticality of high-quality connectivity for economic and social development and there is consensus that future demand for data will continue to grow substantially. The increasingly central role of digital infrastructures to people's lives can be seen in the growth of global Internet traffic. According to Cisco's Virtual Networking Index, global Internet traffic in 2020 will have increased nearly threefold since 2015 (Figure 32).

Figure 32. Global Internet traffic forecast, 2015-20



Source: Cisco (2016).

While demand is likely to grow across all segments of society, it is particularly pressing among individuals living in less densely populated areas, vulnerable consumers and SMEs (see Chapter 1 on access). As a result, the need for universal availability of communication services has come to the fore, along with a variety of approaches employed to ensure that consumer demand can be met, either through commercial provision or, where this is impossible, through public intervention.

A comprehensive assessment of existing legal and regulatory frameworks may be warranted to optimise incentives for all market participants to innovate, compete and invest in the digital economy as well as to maintain social objectives such as universal service, emergency services, privacy and security, and to address new challenges, such as meeting the growing demand for high-quality connectivity.

5.2. Adapting policies and regulation to the rapidly-evolving ICT sector

Adapting policies to promote competition, innovation and investment in the ICT sector is challenging because the sector itself is evolving rapidly. Innovation, investment, and competition in mobile, video and traditional fixed voice marketplaces are causing markets in this general-purpose network world to change faster than the non-converged markets did in the past. Considering that there is greater potential for innovation today, policy makers tend to give more attention to encouraging more investment rather than focusing excessively on short-term considerations such as price-cost margins. They also take the local context into account, applying regulation with an eye towards avoiding unintended consequences.

In addition, they use a targeted approach that focuses on identifying and reducing regulatory barriers to entry where possible. This involves considering investment and innovation when deciding where in the value chain to intervene to promote competition. Policies to promote competition, innovation and investment may include:

- Identifying and removing or lowering barriers to entry to the market,
- Evaluating existing public interest criteria to see whether the objectives are still relevant, and
- Examining the continued relevance of regulatory tools to achieve these objectives.

An additional new challenge involves ensuring that targeted sectoral regulation is also fit for purpose in light of evolving technological and market trends while continuing to protect consumers and citizens. Innovation in

the ICT sector tends to outpace regulatory evolution, creating situations in which not all firms that compete in a market are subject to the same regulation even though they should be, and other situations in which some firms are subject to a certain regulation even though none of them should be. Accordingly, regulation may need to be reconsidered to make sure that it is appropriate where it applies and inappropriate where it does not.

Fostering competition and innovation as the ICT sector consolidates

Consolidation in the communications and media industry is not a new trend, but it has been picking up speed, especially in mobile markets. Between 2010 and 2015, 20 mobile mergers took place in OECD countries compared to fewer new entries for the same period (OECD, forthcoming a). Consolidation between fixed and mobile operators is another trend mirroring fixed-mobile convergence, particularly with cable and MNOs looking to merge or acquire one another. The most recent example is AT&T's October 2016 announcement that it agreed to buy Time Warner Cable (having already purchased satellite TV company DirecTV in 2015). The cable industry has also consolidated. See Table 2 for a sample of large, recent mergers in the communications industry in G20 economies.

Table 2. Selected G20 communications mergers, circa USD 500 million or above, 2014-16

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.
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 acquired the related entity Bell Aliant.
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.
Italy	The two MNO's "3 Italia" and Wind Telecomunicazioni (VimpelCom) merged in 2016.
United Kingdom	BT, a fixed network provider, acquired Everything Everywhere (EE), an MNO.
United States	In 2016, the three cable providers Charter, Time Warner Cable, and Bright House merged. In the same year, United States and international cable providers Altice and Cablevision merged. In 2015, Altice had merged with Suddenlink, another cable provider. In the same year, the Federal Communications Commission (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.

Source: OECD (forthcoming a).

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

In mobile markets, all OECD countries have at least three MNOs and many have four. In addition, MVNOs provide some degree of competition for established providers. However, the recent spate of mergers has

raised concerns about the level of effective competition, which prompted the OECD to examine the implications of an increase or decrease in the number of players in mobile markets. It found that in countries where there is a larger number of MNOs (i.e. more than three), there is a higher likelihood of more competitive and innovative services being introduced and maintained.

While it would be preferable for market forces to determine the number of players, the scarcity of spectrum resources and the need for significant network deployment investments suggest that policy makers may have to determine, or at least influence, the number of players in mobile markets. This seems to have been a factor in the European Commission's 2016 decision to block the proposed mobile merger between Hutchison Whampoa and O2 in the United Kingdom, which would have otherwise seen the market in that country go from four to three MNOs.

If the current number of MNOs is unsustainable or new facilities-based entry is unlikely, it is worth considering voluntary network sharing agreements – either as an alternative to a merger or to allow a new player to enter a market. Recent years have witnessed the growing use of network sharing between MNOs in a number of G20 countries, which can decrease costs to a single operator of network deployment and extend coverage, especially in rural areas that might otherwise be underserved. Network sharing can be a valuable tool for significantly reducing costs at a time when there are demands on operators to invest in new networks or extended coverage. However, network sharing can affect competition, e.g. through potential co-ordination and information sharing. For example, in a market with four MNOs, two sharing agreements may effectively result in a wholesale duopoly. Telecommunication regulators and competition authorities need to be vigilant, monitor sharing agreements and assess whether MVNOs exert sufficient competitive pressure on MNOs.

Policy makers have addressed low levels of competition in fixed markets through the use of regulatory tools such as unbundling of local facilities, or measures such as functional or structural separation. In some cases, countries have opted for public investment in networks, usually linked with open access requirements. In France, for example, the national broadband scheme "Plan Très Haut Débit" aims to connect all households and businesses to very high-speed broadband. Public funding is provided in those areas where the private sector is not expected to invest, with the wholesale infrastructure being open to use by any player.

In fixed markets, competition can be promoted by facilitating efficient access to passive infrastructure, either by operators accessing the infrastructure of public utilities such as railways and energy companies, or by other telecom providers seeking access to passive infrastructure owned by telecoms operators themselves (e.g. dark fibre, ducts, masts). Open access policies – in the form of mandated regulated access, such as local loop unbundling or other wholesale access products – will continue to be an important regulatory tool in promoting competition, particularly where there is insufficient infrastructure competition. However, some wholesale access products will be different for fibre technologies and some of them (e.g. dark fibre, access to ducts or in-building wiring) may be more technically difficult or less economically viable for entrants to use. Regulators will therefore have to be conscious of the potential impact on levels of competition if access for alternative providers becomes more difficult with fibre networks.

In addition, switching is an important issue across both fixed and mobile networks. Policy makers can facilitate demand-side competition by making sure it is easy for consumers to switch between providers. There is a range of ways that this can be done. First, the time it takes to switch can be reduced, including by promoting effective and rapid number portability in fixed and mobile markets. Ideally, switching processes would be led by the gaining provider, which would create incentives for operators to focus on winning new customers rather than only keeping existing customers, thereby boosting competition. Second, policy makers can prevent switching costs from being used as a tool for deterring competition by monitoring these costs and controlling retention clauses and penalties for switching providers. Third, consumer protection regulation can be reviewed to ensure that all parts of a bundle are subject to the same rules, as proposed by the European Commission in its 2016 review of the European Electronic Communications Framework.

5.3. Assessing policy and regulatory frameworks in the era of convergence and Industrie 4.0

Digitalisation is associated with fundamental changes to economies and societies, in part from the innovation enabled by communication infrastructures and services. As noted above, there is a growing convergence of networks and services and a growing ability of different providers along communication value chains to provide competing services. Meanwhile, manufacturing processes continue to evolve in the context of Industrie 4.0, with greater adoption of cloud computing, the development of the IoT, and deeper integration of physical and software components.

These trends raise countries' potential to increase competitiveness, bridge digital divides, and boost innovation, but they also raise certain policy and regulatory challenges. These include protecting competition and consumers, and managing security and privacy risks. In the case of Industrie 4.0, the challenges also include promoting interoperability and transparency because the manufacturing environment is characterised by incompatible connectivity and communication protocols. Standard, open, and complementary communications technologies and processes that enable machines to communicate with each other and the cloud, whether the machines are produced by the same company or not, is essential to capitalising on the efficiencies that Industrie 4.0 and the IoT make possible. Therefore, in light of convergence and Industrie 4.0, G20 economies may wish to assess current policy and regulatory frameworks to ensure that they are able to address these challenges.

Promoting technological neutrality

Convergence, whether between fixed and mobile, telecommunication and broadcasting or telecommunication and OTTs, inevitably leads to the joint provision of multiple communication services in bundles. Network operators can spread joint costs across different services, and experiment with new, innovative services, such as home monitoring for security or heating and various OTT services. Bundling can also be attractive to consumers because of unified billing and the discount applied to a bundle of services rather than paying full price for each standalone service.

The provision of bundled communication services can bring more choice, higher quality, and lower prices to consumers if it increases competition among the facilities-based networks providing bundled offers. On the other hand, bundling may lead to increased consolidation between fixed and mobile network providers and result in less competition in wholesale and retail markets, possibly leading to the exclusion of other operators if they are unable to offer a full range of services. Bundling also renders market analysis and definition more complex, making it more challenging for regulators to monitor and ensure sufficient levels of competition.

Furthermore, the principle of technological neutrality suggests that similar services should operate under the same rules and conditions, but most current regulatory frameworks have difficulty implementing technological neutrality in a converged environment. This is because television and traditional telecommunication services are usually subject to different regulatory environments and OTT services are typically not included in either. Monitoring the effects of convergence with a view to applying the same rules to similar services would help to promote technological neutrality.

Empowering regulatory authorities to address convergence effectively

In response to convergence, an increasing number of countries have brought regulation of the telecommunication and audio-visual sectors under one regulatory body. In the G20, this includes Canada, Italy, Korea, the United Kingdom and the United States. The benefits of doing so include more coherent enforcement and regulatory approaches, with the converged regulator able to examine the full value chain from networks to content.

As convergence continues to alter communication markets, regulators are finding they need to better understand how services are evolving to meet their responsibilities in the area of security and privacy. In 2016, for example, research by the Canadian regulator revealed privacy concerns for consumers stemming from the transition from traditional communications to digitised services delivered over mobile networks. In the United States, the communications regulator is examining whether the privacy rules that apply to telecommunication providers should also apply to cable network operators. In Europe, operators are required to report incidents related to network security and resilience, and in some countries the reports must be submitted to the communications regulator. In general, countries may wish to consider whether the currently assigned roles and responsibilities of national regulatory authorities equip those authorities to deal properly with converged markets and networks.

Enabling opportunities for all actors in a converged environment

In addition to bundling, convergence has led to the emergence of new OTT voice, text and video service providers. Online video distributors, such as YouTube or Netflix, and Internet on-demand television offer content distribution over broadband networks, beyond traditional cable and broadcasting services. These offers benefit viewers in different ways: increased choice of devices to receive content; availability of different pricing models; broader choice of time and location to consume content; and increased interaction with that content. In telecommunication markets, the changes have been equally profound, with voice (VoIP) and text services such as WhatsApp, Skype or KakaoTalk offered over broadband networks. Similarly, both video and voice services may be bundled on social media digital services platforms such as Facebook. Twitter, once solely a short message service, now streams live sporting events around the world.

OTT offerings both supplement and compete with services traditionally provided by telecommunication, cable and broadcasting companies, and they are deemed valuable by consumers. They have, however, raised the issue of the applicability of traditional communication regulations to these new service providers. These regulations were designed to promote efficient communication markets as well as other public policy goals such as the protection of children, access for the disabled, emergency services and universal service obligations in telephony markets. Today's greater convergence and integration across multiple services, applications, platforms and devices suggest that the time is right for reassessing existing communication and digital services regulations and examining whether the regulatory tools are still adequate and relevant to achieve their objectives.

In particular, there may be a need for a review of symmetric regulation – that is, regulation applied to all providers of the same type of communication service. This may include examination of rules governing sectoral consumer protection, emergency calls, interconnection, number portability, privacy, security and media content. In some cases, rules may need to be reconsidered, as they may no longer be necessary given changed market conditions; there may be more efficient ways of delivering the intended public policy objectives given the legitimate needs of consumers and citizens.

Such reviews could also assess whether to extend existing rules to new parties, while being mindful of the inherent trade-offs between protecting consumers and citizens on the one hand, and the potential for damage to competition and innovation on the other. In this respect, market analyses play a crucial role in ensuring a better understanding of competition and innovation dynamics before any regulatory intervention. Therefore, whether extended powers to gather information are needed would be an important consideration. Finally, public interest goals that remain valid would still need to be fulfilled.

How regulation relates to OTT services is one of the questions to be addressed in the current review of the European Union framework for electronic communications, with the authorities examining a September 2016 proposal for a light regulatory approach which allows all actors, from traditional telecommunication operators to online players, to provide interpersonal communication services with the same level of protection for the

end user (European Commission, 2016). In Australia, the competition authority is conducting a market study into the communication industry, looking at the impact of significant changes in the market, including the widespread availability of OTT services.

5.4. Developments in network neutrality

Recent years have also seen extensive debate and new rules on network neutrality in many countries across the world. Network neutrality is about the extent to which the principle of non-discrimination should apply to Internet traffic across networks. Network neutrality potentially involves two main aspects. The first, network neutrality in Internet access services, concerns the ability of users to access content and services, which could be affected by discriminatory pricing, quality of service or blocking (e.g. blocking VoIP services). The second, network neutrality in traffic exchange between networks, concerns the degree of discrimination, if any, in the commercial arrangements that enable traffic exchange (i.e. peering and transit). Both issues relate to the relationship between users and their ISP, whom they pay for access to the Internet, as well as to the terms and conditions by which networks agree to exchange traffic.

Network neutrality in Internet access services

If ISPs change access terms, including quality, to some content, services or networks, that might create different limitations for network users and affect the capacity of users on other networks to communicate with them. Such limitations, if unreasonable, could lead to different quality levels for alternative network paths because not all of them would treat traffic in the same manner. In addition to a potential "fragmentation" effect, access limitations could affect the Internet as a platform for innovation.

There is no unified approach towards network neutrality, so policy frameworks vary from country to country. A number of G20 economies have introduced legislation or regulation to ensure network neutrality and have prohibited blocking and unreasonably discriminating against services. Guidelines were adopted in Canada (2008) and South Korea (2011) and network neutrality rules were included in Brazil's 2014 Civil Rights Framework for the Internet. Most recently, rules have been put in place in the United States and the European Union.

In the United States, the 2015 Open Internet Order established three "bright line" rules prohibiting blocking, throttling and paid prioritisation. It also introduced transparency requirements. Although the rules were challenged by operators, the order was upheld by a 2016 court decision. EU rules came into force in 2016 requiring ISPs to treat all traffic equally and to establish a right for all end users to access and distribute lawful content, applications and services of their choice.

One emerging practice that features highly in network neutrality discussions is zero-rating, which occurs when some of the traffic sent and received by consumers over the Internet is unmetered. Zero-rating can take a number of forms. For example, it can be applied by ISPs to their own content or to that of pre-selected partners, such as video or music services. When customers access that content, it does not count against the data cap in their broadband plans. Alternatively, if the customer of another ISP accesses that content over the Internet, they would pay a subscription charge to the service and their ISP would count these data against their allowance.

A further example of zero-rating involves a large difference in price between on-net and off-net traffic (i.e. traffic supplied by the ISP itself or its unpaid peers, and content obtained via an IP transit network, respectively). These kinds of arrangements tend to be popular in countries that have broadband offers with low data caps in monthly allocations. In Australia, after the turn of the century, lower data caps due to high IP transit rates resulted in the use of zero-rating as a competitive tool. Smaller ISPs and content providers, such as radio stations, directly exchanged traffic and ISPs passed on the lower costs to their customers through

zero-rating. This enabled consumers with low data caps to stream audio from these stations – an option that would have been unattractive with metered pricing. Had regulation required these ISPs to treat this traffic like that of any other content provider not directly interconnecting with them, it would have distorted the incentives for peering and transit.

Zero-rating is on the rise in developing and emerging economies in a different form. A well-known example is Free Basics, originally launched as Internet.org, a service offered by Facebook and six technology companies in partnership with local ISPs. With the stated aim of bringing affordable Internet access to users in less developed countries, it provides free access to a limited range of Internet content and services. Its effect on Internet openness is potentially both positive and negative. On the one hand, it increases access by giving people who may otherwise not be able to afford Internet access a way to connect. On the other hand, what they are connecting to is only part of the Internet and that part is determined by the commercial operator; the rest is sealed off unless the user upgrades to a paid access plan. While Free Basics is currently operating in 53 countries, it is noteworthy that India's regulator banned it in February 2016, ruling that differential pricing for data services was unacceptable.

Elsewhere, regulators have taken varying positions on zero-rating. In many countries the practice exists among various operators in different forms and regulators have not taken action. The extent to which there will be a uniform approach to zero-rating across Europe remains to be seen. Under the European Union Regulation, zero-rating is considered problematic in some circumstances and the implementation guidelines for regulators set out criteria to assess when and whether it should be allowed. However, in October 2016, the Netherlands announced a ban on all zero-rating practices.

Previous experiences in some G20 economies have shown that zero-rating becomes less of an issue with increased competition and higher or unlimited data allowances. Indeed, it can be a tool to increase competition in markets for data transit services, so prohibiting zero-rating may harm competition and reduce the effectiveness of peering. However, allowing zero-rating can harm competition among content providers in markets with limited competition for Internet access. For example, any situation where a dominant content provider is zero-rated and its competitors are not (and the provider's position enables it to opt for paid-peering rather than peering) may impede new or innovative content providers from entering the market. Likewise, a situation where an ISP offers a high-volume service while setting a low data cap could also impede competition.

Network neutrality and traffic exchange between networks

The Internet's model for traffic exchange is, at its core, that every Internet user pays for his or her own access and, in turn, their ISP undertakes to provide connectivity to the rest of the Internet either through peering (direct interconnection) or transit. To save costs, ISPs establish or make use of IXPs, where they can peer with multiple networks at the same time. This model works extremely well and has been a major ingredient in enabling the Internet to scale so rapidly and pervasively.

A survey by Packet Clearing House (2016) found that 99.93% of peering agreements are realised on a handshake basis, with no written contracts and no exchange of payment. Of the agreements analysed by the survey, 99.98% had symmetric terms, in which each party gave and received the same conditions as the other. Moreover, multilateral agreements exist for many IXPs, enabling hundreds of networks to exchange traffic for free with any network that joins the agreement. Parties to these agreements include Internet backbones, access and content distribution networks, as well as universities, non-governmental organisations, branches of government, businesses and enterprises. Under the current voluntary system, operators invest in and expand their network to reach new peers, and co-operate with other networks to establish new IXPs in areas where there are none because they save on transit costs.

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

Where there is little or no competition for retail access service, a key issue is whether consumers are really receiving the service they pay for through their subscription. Resolving this question can be difficult given that the Internet is a network of networks with each network responsible for delivering connectivity and traffic to its own customers. Nevertheless, computer scientists are developing tools to help inform stakeholders about issues such as the existence of online congestion. The preliminary report of a joint project undertaken in 2014 by the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory and the Centre for Applied Internet Data Analysis (CAIDA/UCSD) did not reveal widespread congestion among ISPs in the United States (Clark et al., 2014). Similar projects in other parts of the world could contribute greatly to informing policy makers and regulators.

Although disagreements over interconnection are not new, vigorous peering disputes between powerful players have increased in recent years, including in the United States between Netflix and Comcast (2014) and between Verizon and Cogent (2013). The aforementioned CAIDA/UCSD report concluded that this raised questions about appropriate network management practices as well as concerns about intentional degradation of performance as a business strategy to obtain interconnection fees. Despite these conflicts, traffic exchange markets have developed well in many countries in competitive markets without the need for regulation.

5.5. *Key areas for policy action*

The foregoing discussion suggests certain areas in which policy actions would be especially helpful for improving regulation of the ICT sector.

Foster competition and innovation as the ICT sector consolidates

Competition is a central policy issue regarding regulation in the ICT sector. In particular, competition between communication networks and service providers is important because it generally leads to greater consumer choice, better quality communication services, lower prices and more innovation. Innovation, in turn, is essential because it leads to new services and drives down costs, which means it can also extend consumer choice and spur competition. Convergence can be seen as an impetus towards industry consolidation in recent years, which can create a need for policy actions to protect both competition and, potentially, innovation.

The continuing trend toward sector consolidation is likely to cause regulatory challenges, in particular where it reduces competition. That may lead to calls for greater regulation, for example, in oligopolistic markets. Part of the response to this challenge lies in a careful review of mergers. Other policy responses may include protecting consumer choice through net neutrality rules (such as those recently promulgated in Chile, the Netherlands and the United States), or fostering competition and consumer choice through mandated network access, for instance, in Europe, or measures to facilitate consumer switching. Which approach is most appropriate in a given market will depend on the specific circumstances in that market.

Develop regulatory approaches for the ICT sector that are adapted to a converged environment

In recent years, trends in convergence have been observed mainly between fixed and mobile networks (i.e. the joint provision of fixed and mobile communication services), and between telecommunication and television service offers, with market players tending to offer triple-play services (voice, video and broadband). Services such as voice, video, music and other data-based applications are now offered over the Internet (so-called OTT services). Content, such as music and video, is increasingly integrated with devices or software applications such as search and navigation. These transformations enable innovative services and applications, but also call for policy action, notably to address problems such as decreased competition and greater complexity in defining markets.

Ensuring that current legal and regulatory frameworks are still fit for purpose in light of convergence, and that they are harnessing the potential of interconnected and converged infrastructures and digital services to bridge digital divides and foster innovation, is overall a worthwhile endeavour. To avoid unintended consequences, it helps to apply regulation in a targeted fashion, with a focus on identifying and reducing, rather than increasing, regulatory barriers to entry where possible. This could include considering investment and innovation in decisions about when and where in the value chain to intervene to promote competition. For example, given that some services may be start-ups, aspects such as proportionality could be taken into account.

6. DIGITAL SECURITY

- G20 economies could develop strategies, supported at the highest level of government, to create the conditions for all stakeholders to manage digital security risk to economic and social activities and to foster trust and confidence in the digital environment. Such strategies should incorporate a whole-of-society perspective while providing the flexibility needed to take advantage of digital technologies for the benefit of all. G20 economies could also initiate international arrangements that promote effective privacy and data protection across jurisdictions, including through the development of national privacy strategies that would foster interoperability among frameworks.
- G20 economies could also take action to encourage SMEs to leverage the opportunities of the digital environment for their business and at the same time promote good practice to minimise potential adverse effects. National digital security strategies can in particular help address the specific needs of SMEs by providing them with practical guidance and the appropriate incentives to adopting good practice. There is, for example, increasing interest in tailored standards and certification schemes developed by or in co-operation with business, and in leveraging digital risk insurance.
- Digital security risk has traditionally been approached as a technical problem calling for technical solutions but the changing nature and scale of digital security risk is driving governments in G20 economies to re-evaluate their strategies and policies in this area. In recent years, many governments and stakeholders have shifted their focus on the importance of digital security to minimise the risk to their economic and social activities. This approach recognises that digital security risk as a multifaceted policy area and emphasises the importance of considering this risk from an economic and social perspective.
- There is an urgent need for better evidence on digital security and privacy risk to learn what frameworks and actions work best. G20 economies could explore opportunities for strengthening co-operation and international arrangements that promote greater sharing of good practice and information.

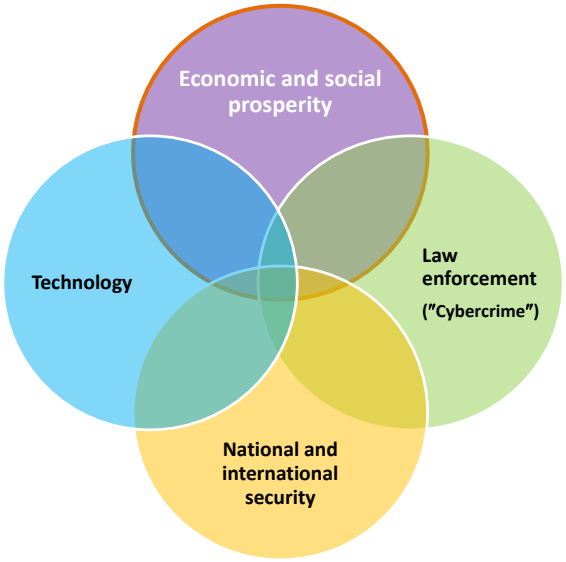
6.1. The policy challenge

Our economies and societies increasingly depend on the digital environment for economic growth and enhanced societal benefits. Realising the potential benefits brought by digital technologies and related innovation requires a more secure and resilient digital ecosystem. However, digital security threats and incidents continue to grow in number and sophistication, with significant consequences. These incidents can affect organisations' image, finances, and even physical assets. They can undermine business competitiveness, ability to innovate and position in the marketplace. Individuals can suffer physical or economic harm from data breaches as well as intangible ones such as intrusion into private life, and damage to reputation. In addition, security incidents can impose significant costs on the economy as a whole by eroding trust and creating large scale crisis should they affect critical infrastructures such as water, health, energy, or finance.

Recently, digital security incidents have interrupted essential utility services such as electricity distribution (e.g. 2015 attack against Ukraine power grid), destroyed physical industrial facilities (e.g. 2014 attack against a German steel mill), interrupted for several hours broadcasting of an international television channel (e.g. 2015 attack against TV5 Monde) and access to over 60 major online services (e.g. 2016 "Dyn attack"), undermined large firms' reputation (e.g. Yahoo in 2016, Target Store in 2013) and functioning (e.g. Saudi Aramco in 2012), and exposed the privacy of millions through numerous personal data breaches. Attackers have also affected the functioning of governments (e.g. US Office of Personnel Management in 2015) and stolen millions to financial institutions, including central banks (e.g. Bangladesh Bank in 2016).

Digital security risk has traditionally been approached as a technical problem calling for technical solutions but the changing nature and scale of digital security risk is driving governments to re-evaluate their strategies and policies in this area. In the last few years, governments and stakeholders have shifted their focus on the importance of digital security to minimise the risk to their economic and social activities. This approach recognises digital security risk as a multifaceted policy area and emphasises the importance of considering this risk from an economic and social perspective (Figure 33).

Figure 33. Digital security is a multifaceted policy area



The 2015 *OECD Council Recommendation on Digital Security Risk Management for Economic and Social Prosperity* ("Security Risk Recommendation") (OECD, 2015k) reflects this new approach. It calls for the integration of digital security risk management into an organisation's overall risk management and decision-making processes. This requires that CEOs, management boards and line managers understand both the opportunities ICTs can offer in terms of innovation, productivity, and competitiveness, as well as the security risk they can bring in terms of financial and reputational damages, disruption of operations, loss of innovation, etc. It also requires that organisations include digital security risk in their existing broader enterprise risk management governance framework to ensure its continuous and systematic assessment and that appropriate decisions are made on how to accept, reduce, transfer or avoid this risk. A key aspect of such a governance framework is the co-operation between economic and social decision makers and ICT security experts.

6.2. Balancing digital security and privacy measures with economic and social priorities

While the implementation of digital security measures is necessary to reduce digital security risk – which can never be eliminated – decisions on the choice of security measures need to be informed by an assessment of the risk itself, the economic and social objectives and benefits at stake, and the cost and impact of the measures.

This assessment aims to determine the acceptable level of risk and address the economic and social trade-offs resulting from the implementation of digital security measures. It is a challenge for organisations. A lack of appreciation of these trade-offs may result in the adoption of security measures that impose an outsized cost on an organisation relative to the benefits of reduced risk exposure. Examples include the direct and indirect cost of security measures, such as opportunity costs and efficiency losses, as well as other negative effects of security measures on the activities that they aim to protect. In addition, security measures may impose social costs if they impede the global, open, interconnected and dynamic nature of information and communication

technologies, and in particular the Internet, which is essential to economic and social prosperity. An effective approach to address the trade-offs is through the adoption by organisations of a digital risk management process that ensures that their choice of digital security measures is appropriate to the context in which they operate and commensurate with the risk they face and their economic and social objectives.

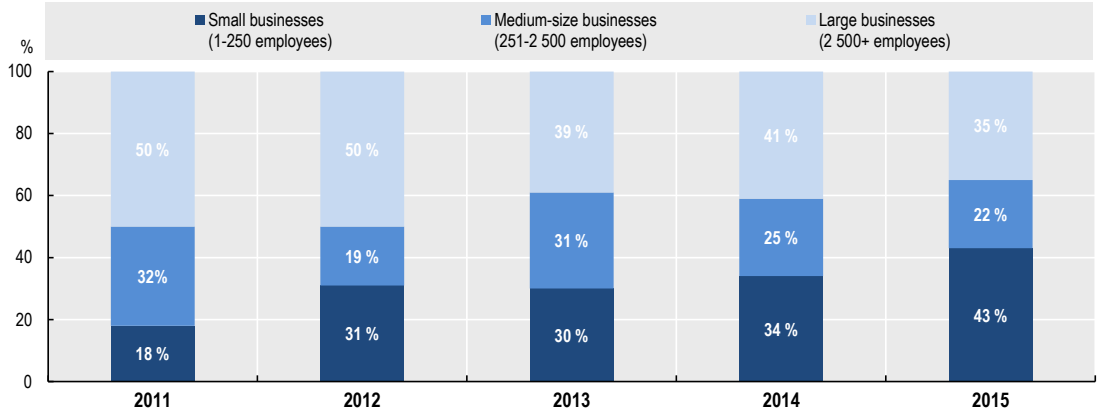
Businesses, including SMEs, can benefit greatly from digital security and privacy measures

In the firm context, every business must determine how best to deal with digital security and privacy risk to benefit from the online environment and achieve growth and scale. Good practices in digital security risk management and privacy protection can enhance the agility and resilience of a business, increase its competitiveness and provide opportunities for partnerships with other organisations. A 2013 survey of business leaders by The Economist Intelligence Unit (2013) suggests, however, that most companies are failing to create a culture of risk awareness. Only about one in four companies report an extensive awareness of digital risk across the organisation. This gap is becoming a public policy challenge, particularly as it relates to SMEs.

SMEs and early-stage start-ups are critical to economic growth. They drive competition and innovation, and contribute to job creation. In high income economies, SMEs undertake the majority of private economic activity, accounting for more than 60% of employment and 50% of GDP (OECD, 2014e). In the United States and Canada, SMEs account for the majority of GDP in most industries. Similarly, in the European Union, SMEs represent 99% of businesses. In emerging economies, SMEs contribute on average to more than 50% of employment and 40% of GDP. In low-income developing countries, SMEs contribute significantly to broadening employment opportunities, social inclusion and poverty reduction (OECD, 2015i).

According to a survey by the National Small Business Association in the United States, the average estimated cost for SMEs from digital security attacks increased from USD 8 700 to USD 20 750 between 2013 and 2014, and average theft from their bank accounts rose from USD 6 927 to USD 19 948 in the same period. So-called “fraudulent transfer schemes” are on the rise. These attacks exploit publicly available information and weaknesses in email systems to trick SMEs into transferring large sums of money into criminals' bank accounts. According to the US FBI, such schemes cost companies more than USD 1 billion globally between October 2013 and June 2015, and while companies of all sizes have lost money to such schemes, SMEs are believed to be the biggest targets (Aguilar, 2015). This finding is consistent with a 2016 report by digital security firm Symantec showing that SMEs have become the main target of “spear-phishing” attacks (based on malicious emails) among businesses (Figure 34) (Symantec, 2016).

Figure 34. Spear-phishing attacks, by size of targeted organisation



Source: Symantec (2016).

In the event that a digital security incident does befall a SME, it can result in a loss of consumer trust, damage to reputation, or a drop in revenue. All these outcomes 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. According to a 2011 study cited by the US House Small Business Subcommittee on Health and Technology, roughly 60% of small businesses close within six months of a digital security attack (Kaiser, 2011).

SMEs in general face distinct challenges in managing digital security risks. Such challenges include a lack of general ability in managing digital security, awareness, resources, and expertise (OECD, 2016h). According to Eurostat (2015), only one in four SMEs (27%) reports having a formally defined ICT security policy, as opposed to 72% of large enterprises and 51% of medium enterprises.

To address these issues, some G20 economies have included specific programmes and initiatives targeted towards SMEs in their national digital risk strategies. These programmes tend to fall into one of three broad categories: public funding or subsidies for security checks, audits and adoption of more secure technologies; information sharing; and awareness campaigns. Examples of initiatives in some G20 economies are listed in Table 3.

Table 3. Examples of SME-targeted initiatives in national digital security strategies

Country	Initiatives
Australia	• Measures to allow small businesses to have their cyber security tested by CREST Australia New Zealand accredited providers.
France	• Development of a Best Practice Guide with SME representative organisations.
Germany	• The Federal Ministry for Economic Affairs and Energy has set up a task force on "IT security in industry" with the participation of industry. • The Federal Ministry of Education and Research is funding research programmes to develop sophisticated security software tailored to SMEs.
Japan	• Awareness raising measures, including the organisation of seminars, the formulation and dissemination of cybersecurity-related guidelines. • Improvement of the structures to share cybersecurity information concerning the latest methods of digital security attacks and security audits regarding cloud services.
India	• Fiscal benefits to businesses for adoption of standard security practices and processes.
United Kingdom	• Training and capacity development through the Cyber Essentials or Cyber Essentials Plus programmes, which provide free online information security training for SMEs. • Information and threat sharing through a single point of advice for the public and SMEs. • Single reporting system for citizens and small businesses to report cybercrime. • "Cyber Streetwise" and "Get Safe Online" awareness programmes targeting SMEs and consumers. • A digital security innovation voucher scheme to help SMEs protect their systems.
United States	• Cybersecurity training to SMEs through 68 District Offices, 9 Manufacturing Extension Partnership Centers, and other regional networks across the country.

Public policy to improve digital security and privacy risk management by SMEs is still in its infancy. A key issue is to identify appropriate incentives tailored to SMEs to foster the adoption of best practices. Various avenues can be envisioned, including the development of a market for digital security and privacy risk insurance, and tax incentives. Several countries such as France and the United Kingdom have developed special schemes and guides to help SMEs. While SMEs require special attention, it is important however to keep in mind the interdependencies between firms of all sizes resulting from generalised interconnectedness. This was demonstrated by the theft of 70 million individuals' personal data during the 2013 breach of Target's systems

in the United States where criminals gained access to the large firm information system by penetrating the network of the small business that Target used for heating and air conditioning services.

6.3. Approaches to promoting digital security

G20 economies are acutely aware of the new evolving threat landscape. Over the years, most governments have adopted digital security public policy measures. Some G20 economies have created new laws aimed at protecting electronic transactions and prosecuting cybercrimes. Others have established critical information infrastructure protection policies and cybersecurity plans, and have vested responsibility for cyber security in existing agencies or directorates. Others have initiated national incident response protocols, and have established national Computer Security Incident Response Teams (CSIRTs). These are all good steps towards improving national cyber security. Too often these efforts are, however, fragmented and reactive. Governments are progressively realising that scattered policy measures have become insufficient to effectively take up the digital security challenge, and have started to adopt more holistic national digital security strategies.

These strategies aim to enhance governmental co-ordination at policy and operational levels and clarify roles and responsibilities. They generally include a whole-of-government vision, covering the responses to the following questions: How does the government understand the digital security challenge? Why is it addressing this issue? What are its overarching objectives and general approach to achieve them?

Some governments choose to limit the scope of their national digital security strategy to some aspects (e.g. economic and social prosperity) and to address other aspects (e.g. defence, cybercrime) in separate strategic documents.

Key objectives of national digital security aimed to support economic and social prosperity include:

- Creating the conditions for all stakeholders to manage digital security risk against economic and social activities and to foster trust and confidence in the digital environment.
- Taking advantage of the open digital environment for economic and social prosperity by reducing the overall level of digital security risk within and across borders without unnecessarily restricting the flow of technologies, communications and data.
- Ensuring the provision of essential services and the operation of critical infrastructures (OECD, 2008a).
- Protecting individuals from digital security threats while taking into account the need to safeguard national and international security, and to preserve human rights and fundamental values.

It is important that the strategies (i) result from a broad intra-governmental co-ordination process to ensure consistency with other national strategies such as national digital strategies (OECD, 2015e), skills strategies (OECD, 2016i), innovation strategies (OECD, 2015j), digital government strategies (OECD, 2014f), etc.; (ii) build on an open and transparent process involving all stakeholders (see below); and (iii) establish co-ordination mechanisms among all relevant governmental actors to ensure that their management of digital security risk is coherent and enhances economic and social prosperity. Often, the strategy documents provide relatively high-level strategic orientations and a detailed set of policy measures addressing the various aspects of digital security are described in separate implementation plans that are reviewed and revised more often than the strategy. A number of specific initiatives can also be contained in national strategies as further discussed in the next sections.

Improving legal frameworks

National strategies and their action plans generally include a set of initiatives of various kinds to improve public policies. They may include self-regulatory (e.g. encouraging codes of conducts), educational (e.g. awareness raising), institutional and organisational (e.g. creation of agencies and PPPs), and legislative measures.

Because of its lack of flexibility to address an extremely dynamic area, legislation is often considered as a last resort with respect to digital security policy making. Moreover, the appetite for new legislative measures often depends on a country's legal system, culture and style of government. Nevertheless, legislation is often developed or, at least, a matter of discussion in a number of areas including:

- Personal data protection (see below),
- Reporting of digital security incidents, for example personal data breaches, security incidents in critical infrastructures,
- Information sharing on threats and vulnerabilities,
- Fight against cybercrime,
- Critical information infrastructure protection, and
- Digital identity, for example establishing the legal value of digital signature and its recognition across borders, or creating a national digital identity framework (cf. OECD, 2011b).

Improving the evidence base for digital security policy making

Rigorous monitoring and evaluation is vital for policy makers to develop effective public policies. There are, however, significant barriers to improving the evidence base for digital security policy making, even in countries with a more established track record in evaluation (Leeuw and Leeuw, 2012; ENISA, 2014).

New reports are continuously published with metrics covering specific aspects of digital security. However, many do not provide sufficient details regarding their data sources or methodology, are limited in scope and in geographic diversity, and may be developed or funded by actors with vested interests. While such statistics are useful, they are often not sufficiently robust to be used with a high degree of confidence for public policy making. With some notable exceptions, these statistics are not regularly updated, providing a snapshot picture from a constantly changing angle, and coming from different sources. At the same time, the need for better evidence has increased in proportion to the elevation of security and privacy risk on governments' policy agendas. Compared to other areas of digital economy policy, such as telecommunications policy for example, digital security statistics are still in their infancy.

There is an underexploited wealth of empirical data that, if mined and made comparable, would enrich the current evidence base for policy making. Such indicators would help identify areas where policy interventions are most clearly warranted, and provide guidance on designing policy interventions and determining their effectiveness (OECD, 2012a). Collection of and development of such metrics and empirical data would also provide an important input into the evaluation of policies intended to manage digital security risk.

6.4. Fostering a culture of co-operation

An effective and enduring national digital security strategy requires dialogue and co-operation across all levels of government, business, civil society and the technical community, as well as across countries. Multi-stakeholder co-operation can facilitate governments' efforts to reach out to communities and groups such as consumers, children and elderly people, and economically vulnerable populations in order to raise awareness

about digital security risk and how to manage it. As most of the digital and critical infrastructures is owned, operated and/or used by private sector, public-private co-operation is essential.

Public-private co-operation

Overall, an ongoing public-private dialogue is key to devise public policies that foster digital security risk management across society without stifling innovation and reducing the economic and social opportunities offered by the digital environment. It is also good practice to tailor the modalities of the dialogue to specific audiences, such as SMEs that face special challenges (see below) and typically convey their collective concerns through different channels than large businesses.

Co-operation among public and private stakeholders can improve identification and remediation of vulnerabilities and threats, as well as mitigation of digital security risk. It can take place through mutually trusted initiatives and partnerships whether private or public-private, formal or informal, at domestic, regional and international levels to: (i) share knowledge, skills and successful experience and practices in relation to digital security risk management at policy and operational levels; (ii) exchange information related to digital security risk management; (iii) anticipate and plan for future challenges and opportunities (OECD, 2015k).

A number of governments have made PPPs a prominent part of their national digital risk management strategies. Such arrangements are particularly significant in the protection of critical infrastructures, reporting and dissemination of threat information, incident response (through CSIRTs), the conduct of research and development in digital security, and the development of a digital security industry. Examples of specific public-private initiatives in selected G20 economies are included in Table 4.

In general, public-private co-operation should be understood as a two-way communications channel that benefits both the government and non-governmental stakeholders. However, this is not always the case and the absence of reciprocity can become an obstacle to effective operational co-operation, in particular with respect to the exchange of information between governments and businesses on digital security threats and vulnerabilities.

Table 4. Examples of public-private initiatives for digital security

Country	Public-private initiatives
Australia	• Co-design of voluntary guidelines on good digital security practice ("Australian Internet Security Initiative"). • Joint public-private awareness initiatives and education campaigns. • Streamlining of digital security governance and structures to improve interaction between the private and public sectors. • Relocation of the Australian Cyber Security Centre to enable the government and the private sector to work more effectively together. • Sharing of real-time public-private digital threat information through joint sharing centres.
Canada	• Information on risks and impacts of cyber incidents is shared between governments and the private sector.
Italy	• Information sharing on attacks and incidents, and on risks and vulnerabilities assessment. • Creation of joint working groups. • Periodic national exercises involving relevant public stakeholders and private-sector operators. • Regular exchange of best practices and lessons learned between private and public stakeholders to facilitate reciprocal understanding and foster joint training of personnel. • Establishment of national Computer Emergency Response Team as a co-operative PPP.
Saudi Arabia	• Information-sharing capabilities through "government-private partnerships". • Establishment of a combined effort of representatives from public sector organisations with mission responsibilities for infrastructure and the owners/operators of those infrastructures.
South Africa	• Establishment of a public-private trusted forum. • Encouragement of private sector to address common security interests, collaborate with government, and foster co-operation among interdependent industries to create a common understanding of the threats and vulnerabilities.
South Korea	• Establishing a joint response system and team of private, public and military sectors.
Turkey	• Decision-making mechanisms for the security of critical infrastructures. • Co-ordination of public and private co-operative R&D for national technologies in digital security.
United Kingdom	• Establishment of a "Cyber-security Information Sharing Partnership" to exchange cyber threat information in real time, increasing situational awareness and reducing the impact on business. • Publicly funded accelerator to nurture UK digital security start-ups.
United States	• Establishment of a public-private R&D partnership to allow industry and government to work together to develop and deploy technical solutions for high-priority cybersecurity challenges and share results with the broader community. • Adoption of the 2015 Cybersecurity Act to simplify digital threat information sharing by private companies with each other and the Government. • Creation of the Critical Infrastructure Cyber Community C³ Voluntary Program, a PPP to help align critical infrastructure owners and operators adopt the National Institute of Standards and Technology's Cybersecurity Framework.
European Union	• Creation of the European Public-Private Partnership for Resilience (EP3R) to co-ordinate public and private actors in critical information infrastructure protection. • Establishment of a PPP (EUR 1.8 billion investment by 2020) to foster co-operation on early-stage research, align the demand and supply sectors for cybersecurity products and services, and develop common building blocks.

Improving international co-operation

Effective international co-operation is essential for improving current digital security risk policies. This is due to the global nature of the Internet, global adoption and spread of digital technologies, as well as transnational

conduct of cybercrimes and digital security attacks. Global interconnectedness creates interdependencies between stakeholders and calls for their co-operation on digital security risk management.

Almost all national digital security strategies call for improved international co-operation. With many countries now having set up a national co-ordination agency or mechanism, there is an opportunity for them to extend it as "an international contact point to facilitate co-operation on cybersecurity at policy and operational levels" (OECD, 2012b). Indeed, the Security Risk Recommendation calls for governments to strengthen international co-operation and mutual assistance notably by:

- Participating in relevant regional and international fora, and establishing bilateral and multilateral relationships to share experience and best practices; and promoting an approach to national digital security risk management that does not increase the risk to other countries,
- Providing, on a voluntary basis as appropriate, assistance and support to other countries, and establishing national points of contacts for addressing cross-border requests related to digital security risk management issues in a timely manner, and
- Working to improve responses to domestic and cross-border threats, including through CSIRTs co-operation, co-ordinated exercises and other tools for collaboration.

There are numerous international and regional fora and organisations through which various aspects of digital risk management might be pursued. Among them, the OECD has been a key forum for bringing together member countries and other G20 economies and organisations to discuss and co-operate around policy issues such as the protection of critical information infrastructures, privacy, cryptography policy, and electronic authentication. As efforts to foster capacity building in less developed countries are increasing, co-operation between digital security and development oriented international and regional fora could become necessary. One example is the international partnership initiated by the ITU with a set of other international and regional organisations (European Union Agency for Network and Information Security (ENISA), OECD, Organisation of American States, World Bank, United Nations Conference on Trade and Development (UNCTAD), Commonwealth Telecommunications Organisation (CTO), and Commonwealth Cybercrime Initiative (CCI) to bring together in a single guide existing guidance and recommendations from these organisations in order to help developing countries in the adoption of their national cybersecurity strategy.

6.5. Promoting good practices for effective data protection

Digital security and the protection of personal data ("data protection")[7] are closely related: digital security incidents create privacy issues when they affect the confidentiality or integrity of data directly or indirectly related to individuals (i.e. "personal data"). Several international instruments, including the *OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("Privacy Guidelines") (OECD, 2013d) include a "Security Safeguards" principle[8] and digital security risk management can help implement this principle.

Different stakeholders will be subject to different types and intensity of risks from digital security incidents affecting personal data, often called "data breaches" or "personal data breaches". For instance, when personal data is publicly disclosed following a data breach or falls into the hands of unauthorised persons, individuals face privacy breaches that can lead to financial fraud and other physical, material and moral damage. Public and private organisations may, on the other hand, face direct financial loss, reputational damage and loss of customer trust. They may also risk lawsuits and fines from data protection authorities for breaching legal privacy frameworks.

From a digital security risk management perspective, personal data breaches can be viewed as a particular type of digital security incident where two parties are exposed to the risk but one (the organisation) is in

charge of its management for the other (the individuals). In many cases, the interests of these two parties may not be sufficiently aligned: organisations can have strong incentives to exploit individuals' personal data for economic gains but be less inclined to take appropriate measures to protect privacy if they don't see a clear benefit in doing so.

Privacy and personal data protection legal frameworks, including data breach notification requirements, can be viewed as incentive mechanisms that increase the risk for organisations that do not sufficiently protect individuals' rights and interests when they process personal data. For example, why would a company inform individuals that their personal data has been breached if this information would also undermine the company's reputation? Yet knowing that a breach occurred is essential for individuals to mitigate subsequent possible negative consequences.

While personal data breaches illustrate the overlap between digital security and personal data protection, these two areas are distinct. Many risks related to privacy are unrelated to digital security risk. For example, data collected automatically from smart meters by an energy company to optimise electricity production may reveal people's behaviour inside their homes. Whether there is a violation of privacy and data protection will depend on how personal information is collected, used, disclosed and accessed. This can be illustrated by questions such as: are the individuals informed about this data collection? Do they have access to their personal data? Is the data used only for the purpose initially specified?

Nevertheless, despite these differences, public policy for privacy and data protection can benefit from lessons learned from digital security risk management. In contrast to digital security risk, which is addressed through national strategies, legislation continues to be the main response to privacy risk in many countries. While legal protection is essential, privacy in an increasingly data-driven economy would benefit from a multifaceted strategy, along the model of digital security strategies.

Privacy strategies could strengthen protection, help create the conditions for privacy protection to become a differentiator in the marketplace and provide the flexibility needed to benefit from emerging technologies. They could also encourage research and innovation with respect to "privacy by design" approaches and help focus efforts by privacy enforcement authorities and other actors. Such a strategic approach to privacy protection could facilitate whole-of-society discussions to address complex privacy challenges such as those emerging from the use of big data analytics and artificial intelligence. Co-ordinated privacy strategies at the national level would help foster co-operation among all stakeholders, support the development of international arrangements that promote interoperability among privacy frameworks and lessen uncertainty in data flows (Box 5).

BOX 5. INTERNATIONAL CO-OPERATION AND INTEROPERABILITY OF PRIVACY PROTECTION APPROACHES

The G8 Deauville Declaration outlined that we still "face considerable challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data" (G8, 2011). Likewise, the *OECD Council Recommendation on Principles for Internet Policy Making* calls for strengthening the consistency and effectiveness of privacy protection at a global level. The Communiqué which is annexed to it further recognised the objective of governments to pursue global interoperability in this area. The OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (amended in 2013) similarly recognises the value of globally interoperable privacy frameworks that ensure effective protection of privacy and support the free flow of personal information around the world.

There exist a range of approaches to interoperability among privacy frameworks. The US-EU Safe Harbour Framework, which was adopted under the EU adequacy regime and implemented in 2000, was an early example. Since then, this agreement was invalidated and a new agreement was developed to address privacy protection for data transferred between the US and the European Union – the US-EU Privacy Shield. Other initiatives have been undertaken to bring together different approaches and systems of protection, including work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region. The Council of Europe updated Convention 108 on the Automated Processing of Personal Data in 2012. Further work is needed at the policy level towards a more seamless approach to global privacy governance.

6.6. Key areas for policy action

Robust strategies to manage digital security and privacy risks are essential to establish the trust needed for economic and social activities to fully benefit from digital innovation. Some productive areas for policy actions by the G20 are outlined below.

Develop national digital security and privacy strategies

G20 economies could develop strategies, supported at the highest level of government, to create the conditions for all stakeholders to manage digital security risk to economic and social activities and to foster trust and confidence in the digital environment. Such strategies should incorporate a whole-of-society perspective while providing the flexibility needed to take advantage of digital technologies for the benefit of all. G20 economies could also initiate international arrangements that promote effective privacy and data protection across jurisdictions, including through the development of national privacy strategies that would foster interoperability among frameworks (OECD, 2016j). Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by organisations and ensure that privacy requirements are maintained. It can also enhance individuals' awareness and understanding of their rights in a global environment.

In order to optimise the economic and social benefits expected from the digital environment, leaders and decision makers could encourage a shift towards the adoption of a risk management approach so that digital security risk management becomes an integral part of an organisation's overall risk management and decision-making processes, and the resulting choice of security measures take into account the interests of others, is appropriate to and commensurate with the risks faced, and does not undermine the economic and social activity they aim to protect.

If they have not already done so, G20 economies may wish to consider adhering to the 2015 *OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity* which may offer useful guidance as governments undertake to develop or revise their national digital security strategy and set up digital security risk management frameworks. Sharing of best practices would facilitate the development of these frameworks and their implementation.

Address the special needs of SMEs by developing guidance tools and incentive mechanisms

G20 economies could take action to encourage SMEs to leverage the opportunities of the digital environment for their business and at the same time promote good practices to minimise potential adverse effects. While different types of SMEs face different challenges, all would benefit from integrating digital security risk management into their business decision making. Increasing SMEs awareness of digital risk and elevating their capacity to manage it is critical. Given that SMEs may lack expertise and face resource constraints, larger organisations, industry associations, the technical community and governments can play an important role in this area and share their knowledge, skills and expertise about best practices in managing digital risk. Useful approaches could include the development of SME-specific risk management guidance tools and incentives.

Develop better evidence to support policy making on digital security risk and privacy protection

While technical experts and policy makers generally agree that digital security risk and privacy concerns are changing in scale and require urgent action by all stakeholders, the evidence to support this conclusion remains often anecdotal and qualitative. With some notable exceptions, the available statistics are often not sufficiently robust to be used with a high degree of confidence for public policy making. While this situation is typical of an area which, without being completely new, is still at an early stage of maturity, there are also some complex challenges related to measuring digital security risk, including data breaches. For example, organisations may be reluctant to disclose quantitative information about vulnerabilities, incidents and impact to avoid further exposing their reputation or attract malicious actors.

Compared to other areas of digital economy policy, such as telecommunications policy, digital security and privacy statistics are still in their infancy. However, organisations and business around the world are facing similar digital risk challenges. There are, therefore, ample opportunities for countries and leaders in public and private sectors to learn from one another. In order for this mutual learning to take place, there is a need for agreed upon and consistent terminology and indicators that can be systematically collected and are comparable over time and across countries. These indicators would help governments and business design and evaluate policies and risk management strategies, learn from failures and successes, and promote adoption of good practice.

7. SKILLS AND THE DIGITAL ECONOMY

- To ensure that everyone can engage in and benefit from the digital economy and adapt rapidly to new and unexpected occupations and skill needs, education and training systems in G20 economies should place a stronger emphasis on promoting ICT generic skills, ICT specialist skills, and ICT-complementary skills, including foundational skills, digital literacy, higher-order critical thinking skills as well as social and emotional skills. Greater efforts are also needed to raise the skills of those adults with weak literacy, numeracy and digital skills to enable them to fully participate in the digital economy and society.
- Skills are a key factor affecting the industry specialisation of a country and its integration in international markets and GVCs. A better alignment of industrial and trade policies with skills policies is necessary for countries to preserve and enhance their comparative advantages.
- Digital technologies are creating new opportunities for skills development. Seizing these opportunities requires a process of institutional learning, where actors are given sufficient scope to experiment with new tools and systematic assessment of outcomes leads to select the most effective practices. Barriers to access these new technologies must be addressed, as well as concerns about the quality of online education and the lack of recognition for learning outcomes.
- The development of more effective strategies in G20 economies that enable all people to adapt to and excel in the digital economy, including through the use of ICTs and other technologies to upgrade skills, is essential. This implies identifying the mix of skills needed to boost quality employment and active participation in a digitalised economy as well as promoting policies and targets to promote their development and use. It also means facilitating continuous adaptation as changing task requirements on-the-job put pressure on formal education and training systems to remain up-to-date.

7.1. The policy challenge

The pervasiveness of digital technologies in daily life is fundamentally changing the way that individuals access and elaborate knowledge in G20 economies. They must process complex information, think systematically and take decisions weighing different forms of evidence. They also have to continuously update their skills to adapt to rapid technical change in the workplace. More fundamentally, to seize the new opportunities that digital technologies are opening in many areas, individuals must develop the right bundle of skills to make meaningful use of these technologies.

7.2. What skills for the digital economy?

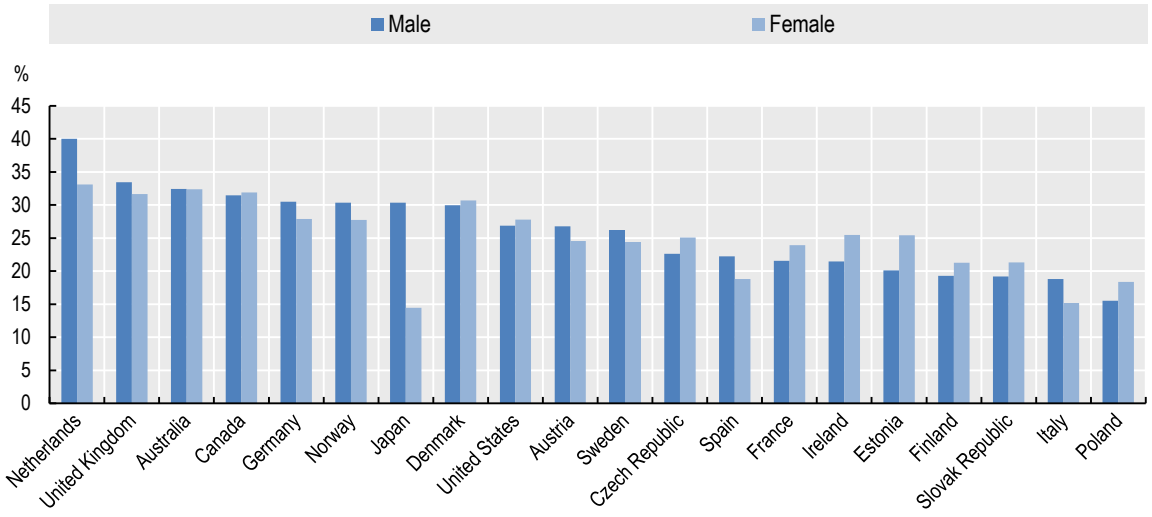
Increasing use of digital technologies at work is raising the demand for new skills along three lines. First, workers across an increasing range of occupations need to acquire generic ICT skills to be able to use such technologies in their daily work (e.g. access information online or use software). Second, the production of ICT products and services – software, web pages, e-commerce, cloud and big data – requires ICT specialist skills to programme, develop applications and manage networks. Third, the use of ICTs is changing the way work is carried out and raising the demand for ICT-complementary skills, including the capability to process complex information, communicate with co-workers and clients, solve problems, plan in advance and adjust quickly. Last but not least, the attainment of sound foundational skills constitutes a prerequisite for the development of proficient ICT generic, specific and complementary skills.

ICT generic skills

Recent research shows that the demand for ICT generic skills, as measured by the OECD Survey of Adult Skills (PIAAC), has increased in a large majority of countries (OECD, 2016k). Yet, the frequency of ICT use at work continues to differ significantly across countries (Figure 35). Furthermore, in half of the countries surveyed by PIAAC, women tend to use ICTs at work less than men.

Figure 35. Daily users of office software at work, by gender, 2012

As a percentage of all workers



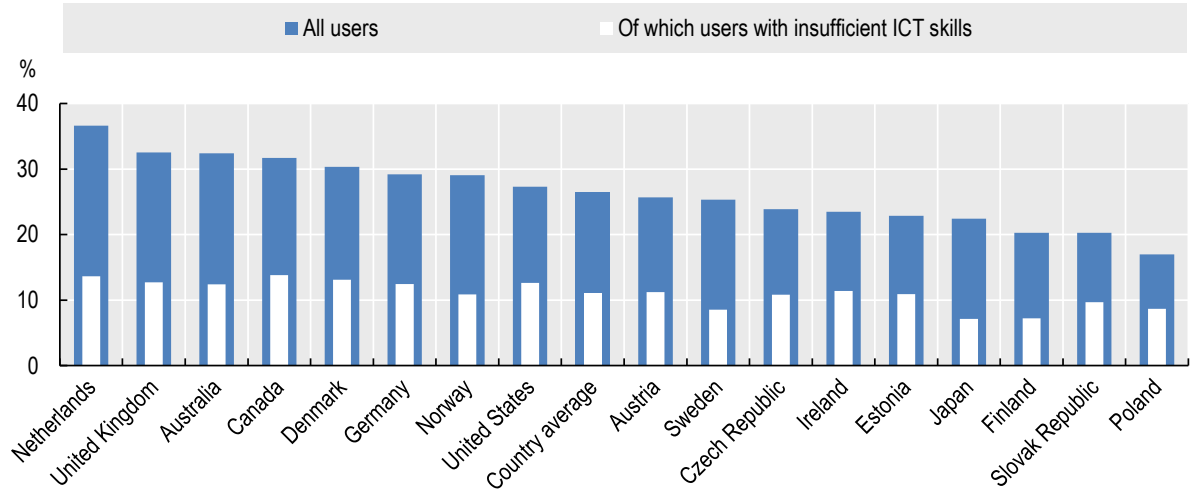
Note: Data for United Kingdom refer only to England and Northern Ireland.

Source: OECD (2016k).

The analysis also compares the demand for ICT generic skills and the supply of these skills in the workforce, as measured by the PIAAC assessment of ICT skills. Many workers use ICTs regularly without adequate ICT skills: on average, over 40% of workers using office software every day do not seem to have sufficient skills to use them effectively according to the performance assessment (Figure 36).

Figure 36. Daily users of office software at work, by ICT skills, 2008-2013

As a percentage of all workers



Note: Data for United Kingdom refer only to England and Northern Ireland.

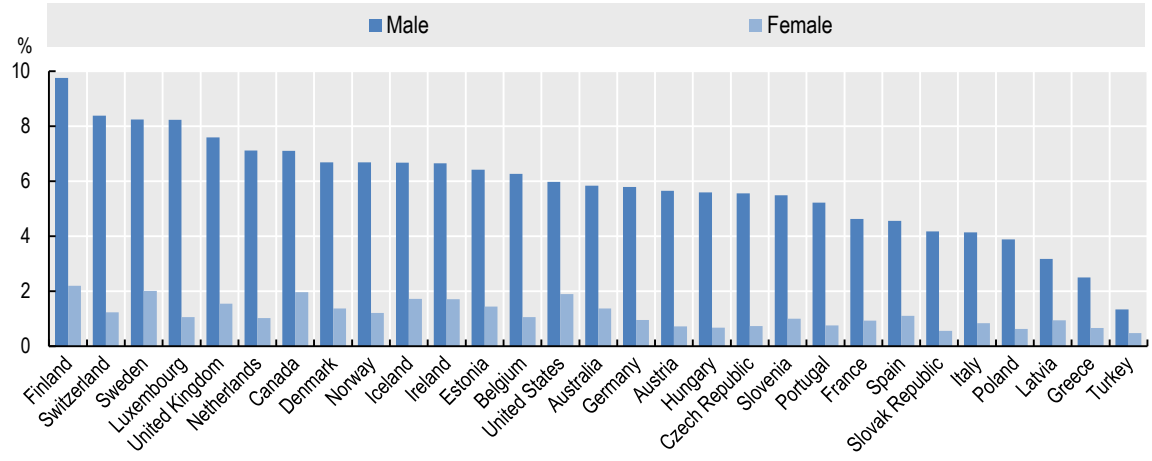
Source: OECD (2016k).

ICT specialist skills

ICT specialists have been among the most dynamic occupations in recent years and several forecasts suggest that the demand for ICT professionals will grow even faster in the near future. In 2014, ICT specialists accounted for 3.6% of all workers in OECD countries. This figure hides large differences between men and women. While 5.5% of male workers in OECD countries are ICT specialists, only 1.4% of female workers are (Figure 37).

Figure 37. ICT specialists by gender, 2014

As a percentage of all male and female workers



Source: OECD (2016k).

Some forecasts predict a significant shortage of ICT professionals (European Commission, 2014; OECD, 2014g) over the next 5 to 15 years. These forecasts rely on a scenario-based approach which, by its very nature, is hard to validate. Although imperfect, available statistics suggest less pessimistic scenarios (OECD, 2016k):

- In ICT services, wages have been growing in line with productivity growth over for 15 years while vacancy rates have remained stable or even decreased since 2007.
- The share of online vacancies for ICT specialists has also remained stable in most countries for which data are available since 2012. Median vacancy duration, i.e.: the number of days necessary to fill an online vacancy for ICT specialists was just 32 days in France, Germany and the Netherlands in 2014.
- In the European Union, only 3% only of enterprises reported hard-to-fill vacancies for ICT specialists, a proportion that has not changed over recent years. Business surveys in Australia and New Zealand as well as other international surveys report similar findings.

As available statistics are not comprehensive enough to fully address these questions, the development of better measures – based on both official statistics and online vacancies – is an important step to strengthen the evidence base in all G20 economies for policymaking in this area.

ICT-complementary skills

The diffusion of ICTs in the workplace is not only raising the demand for ICT specialist and generic skills, it is also changing the way work is carried out and raising the demand for ICT-complementary skills. These are skills that are not related to the capability to use the technology effectively but to carry out the work within the new environment shaped by ICTs, i.e.: a "technology-rich environment". For instance, higher frequency of information made available by ICTs calls for better capability to plan in advance and to adjust quickly. Organisations characterised by horizontal work enabled by ICTs call for more co-operation across teams and

stronger leadership. Wider diffusion of information among a larger number of workers increases the importance of management and co-ordination. The sales skills required in face-to-face commercial transaction are not the same as those involved in an anonymous e-commerce sale.

Researchers have identified three broad domains that are important for skills development (National Research Council, 2012; OECD, 2015l): a cognitive domain, including cognitive processes, knowledge and creativity; an intrapersonal or emotional domain, including intellectual openness, work ethics and self-confidence; and an interpersonal or social domain, including teamwork, collaboration and leadership.

OECD research also shows that higher use of ICTs at work is associated with tasks that require more interaction with co-workers and clients, more problem solving and less physical work (OECD, 2016k). As ICTs are reshaping business models and firms' organisation, the skills required to perform these tasks become more important. Changes in the task set associated with increasing use of ICTs tend to be larger for people in low-skilled occupations than for those in middle- and high-skill occupations. Therefore, the need for re-skilling is likely to be larger for those people that educational and training systems have more trouble reaching.

To ensure that individuals can engage in digital activities and adapt rapidly to new and unexpected occupations and skills needs, a stronger emphasis has to be placed on promoting strong foundational skills, digital literacies, higher-order critical thinking competencies as well as social and emotional skills.

New forms of work and skills

In an increasingly integrated global economy, digital technologies are enabling firms to segment work in new ways and to increase the use of temporary labour. With innovative online platforms, new intermediary firms are connecting individual providers with individual customers, turning some full-time, long-term jobs into an uneven flow of "on-demand" tasks.

The number of users on the two largest job-matching platforms has increased 15 times in ten years, reaching 36 million in 2015, a figure that underestimates the actual number of platform-enabled workers. If it continues, this trend could transform the traditional employer-employee relationship, with significant implications for labour market policy and social dialogue (OECD, 2016o).

For workers, greater flexibility in the choice of working time may come at the cost of lower job quality, higher income volatility, lower access to social protection and more responsibility for skills development. For firms, lower labour costs and wider access to a global pool of virtual workers may erode their human capital assets.

It is uncertain how many of the growing number of independent workers have the skills to thrive in platform service markets. Easy entry into platform services markets might attract a number of individuals who lack the entrepreneurial and self-management skills to succeed in independent work. In contrast to well-educated and high-skilled entrepreneurs, workers that need less sophisticated skills, e.g. in handyman services, driving, or click-work, might have decided to enter platform services markets motivated by short-term cash flow, but without properly accounting for the cost and risk they are taking on. Managing multiple jobs, building and maintaining online reputation, complying with potential liabilities, identifying and managing suitable health and pension schemes, covering holidays, maternity and sick leave, finding and carrying out training to upskill and build a career, to name just a few challenges, seems to go beyond traditional expectations associated with (independent) workers. If the latter do not have the skills to manage these responsibilities, they are unlikely to take advantage of perceived opportunities of platform services markets.

To meet these challenges, governments and social partners can improve their ability to detect emerging labour market trends and explore ways of developing existing labour market programmes and safety nets, in which eligibility is tied to standard employment models, so as to ensure inclusive growth and job quality in the new work organisation enabled by the digital economy.

Fostering digitally competent consumers

Initiatives to promote consumer education and awareness can assist consumers to develop the skills, knowledge and confidence needed to navigate an increasing complex digital marketplace and make informed decisions. At a general level this should include consumer awareness of the consumer protection framework that applies to their online activities, including their respective rights and obligations, at domestic and cross-border levels. Such programmes should be designed to meet the needs of different groups, taking into account factors such as age, income, and literacy (OECD, 2016l).

Although work to improve consumer digital competency is not yet widespread, one notable initiative is the European Commission's identification of a set of 14 specific digital competencies for consumers. A first set relates to actions taken before purchasing goods and services in the digital marketplace, which focus on information search, comparing information, evaluation of alternatives, dealing with commercial communication, managing digital identity, and making responsible and sustainable consumption choices.

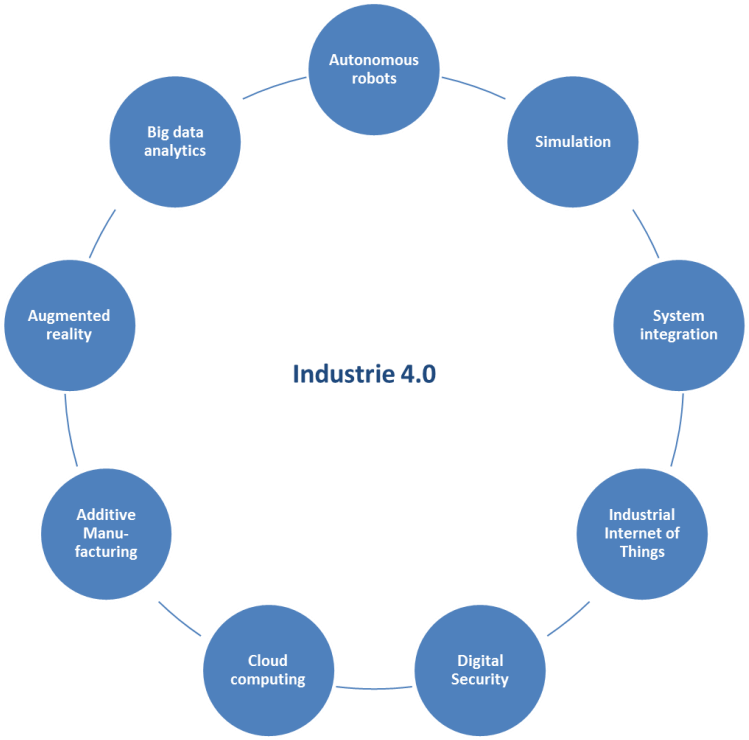
A second set is oriented around the purchasing process: making a purchase, participating in collaborative economy platforms, managing payments, understanding copyrights, licenses and contracts for digital content, protecting data and health. A final set considers the post-purchase phase: sharing information, asserting consumer rights, updating digital consumer competences (JRC, 2016). More testing and experience will be need to determine how best to improve consumer digital competency. Ultimately, dialogue between consumer policy and education ministries about the incorporation of digital consumer education into school curricula and adult education may be needed.

7.3. Skills for Industrie 4.0

The term Industrie 4.0 encompasses the digitalisation of production processes based on devices autonomously communicating with each other along the value chain. Production units become "smart factories" where computer-driven systems monitor physical processes, create a virtual copy of the physical world and make decentralised decisions.

Nine technologies appear to be the enabling factors of Industrie 4.0 (Figure 38). These technologies make it possible to gather and analyse data across machines, enabling faster, more flexible, and more efficient processes to produce higher-quality goods at reduced costs. This in turn increases manufacturing productivity, shifts economics, fosters industrial growth, modifies the profile of the workforce and ultimately changes the competitiveness of companies and regions.

Figure 38. Nine technologies that are transforming industrial production



Source: OECD, adapted from Rüsmann et al. (2015).

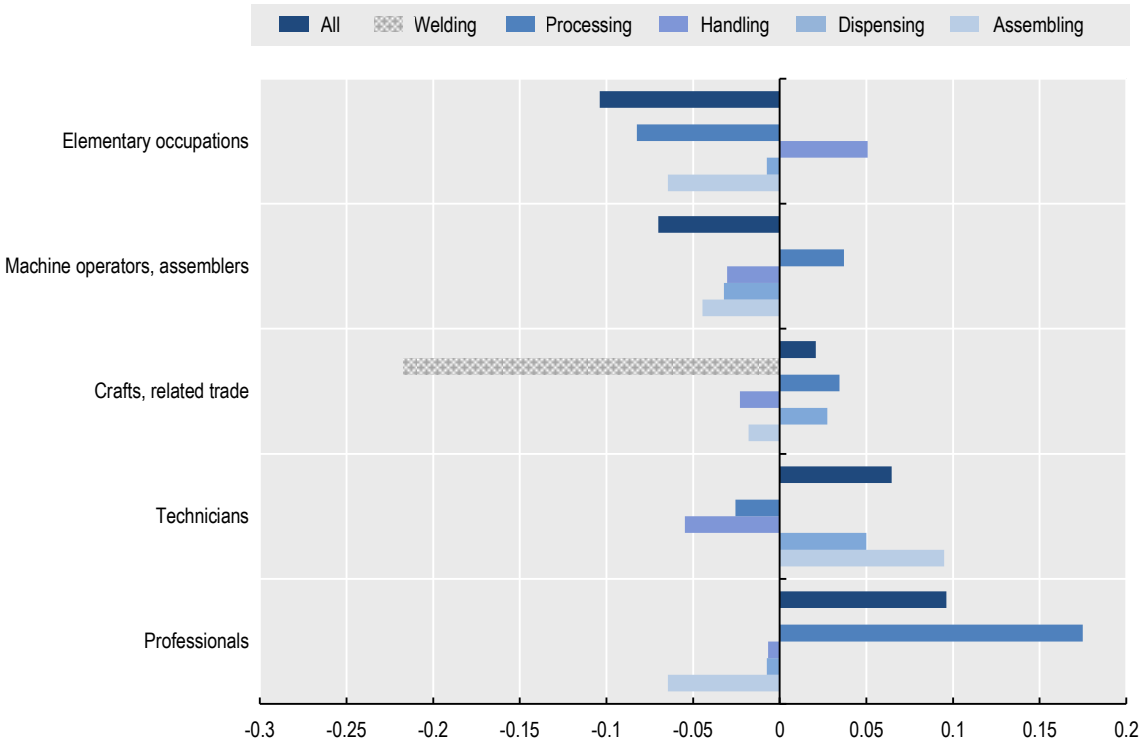
What are the skills required for Industrie 4.0?

Skills requirements for Industrie 4.0 are more interdisciplinary than those for basic digital literacy. Industrie 4.0 creates new operational and organisational structures relying on decision making, co-ordination, control and support services – a much more complex environment. There is also a need to co-ordinate between virtual and real machines and plants in production management systems. In general, this means that there are significantly higher demands placed on all members of the workforce in terms of managing complexity, higher levels of abstraction and problem solving. Employees are expected to act more on their own initiative, have excellent communication skills and be able to organise their own work (Smit et al., 2016).

Robotisation provides a useful illustration of how Industrie 4.0 is changing the demand for skills. OECD (forthcoming b) shows that robots replace certain tasks, previously carried out by humans, while creating the demand for new tasks to be carried out by workers. As a result, employment will decrease in occupations comprising tasks that can be automated and will increase in occupations where human labour is complementary to robots. The balance between substitution and complementarity effects depends on the robots' field of applications, with employment falling in some areas and growing in others (Figure 39).

Figure 39. Estimated elasticity between robots (by application) and employment (by occupation)

Proportional increase in employment associated to a 1% increase in robots



Note: Estimated elasticities based on 14 countries (Austria, Germany, Denmark, Spain, Finland, France, Croatia, Ireland, Italy, Norway, Romania, Sweden, Turkey and the United Kingdom) over 1993-2014.

Source: OECD (2016 forthcoming b).

For example, handling robots, which include metal casting, plastic moulding but also measuring, inspection and testing, appear to complement workers in elementary occupations while substituting for all other occupational groups. Welding robots tend to substitute for human workers performing the same operation, notably in the occupational group Crafts and Related Trade Workers. And assembling robots are found to increase the demand for Technicians, who are called to supervise and improve the production flows. All other occupations, however, are negatively affected by this type of robot.

In general, when robots interact with occupations lacking specialised skills or abilities, they can trigger changes in the task composition and a shift towards tasks that cannot be automated, such as those involving interpersonal skills, problem solving or decision making. In these cases, robots can substitute for low value, routine tasks and increase the value of those skills necessary to the performance of more "abstract" tasks.

The diffusion of industrial robots, accelerated by continuous improvements in technology implies that skills related to specialised but routine tasks will increasingly become obsolete, even if they require substantial years of investment in education. More important appear to be more general skills such as high level of literacy and numeracy, or even interpersonal and communication skills.

Country-specific features, e.g. industry specialisation and the prevailing degree of automation in a country may result in different effects on skills demand. In addition, similar technologies may lead to different skills needs depending on the organisational environment (Hartmann and Bovenschulte, 2013).

Results from the PwC 2016 Global Industrie 4.0 Survey show that 50% of the companies that are included in the survey see the lack of digital culture and training as a top challenge to making their operations more

digital. Therefore, the main issue for most firms today turns out to be the recruitment, tenure and training of people with the appropriate skills rather than the adoption of a particular technology (PwC, 2016).

Pilat and Nolan (2016) argue that organisational change, workplace innovation, management and skills are some of the areas where firms will need to invest to support rapid technological change, supported by complementary public investments in education, research and infrastructure. Interim results of the OECD project on the next production revolution (OECD, 2016a) also show that rapid technological change could challenge the adequacy of skills and training systems to match demand and supply for new skills although digital technology could naturally play a role in augmenting skills supply, for instance through massive open online courses (MOOCs). For some production technologies, the current supply of skills appears to be insufficient.

Benefiting from these new technological trends that are central to this new production paradigm is dependent on a broad range of policy drivers. Smit et al. (2016) show that most EU member states have not adopted national policies that specifically address the issues related to Industrie 4.0. As regards the provision of the appropriate skills, their recommendations include policies to support funding as regards education and migration.

Education systems indeed play a key role to making the most of Industrie 4.0 as they are called to seek to provide broader skill sets and job-specific capabilities, close the IT skills gap, and offer new formats for continuing education (Lorentz et al., 2015). Furthermore, the performance and positioning of firms, as well as the specialisation and competitiveness of industries and economies in GVCs are shaped by the skill composition of the workforce. There is increasing evidence (OECD, forthcoming c) that a country's comparative advantages do not depend on a specific set of skills but on the way these skills are distributed among workers, i.e. on their "skill bundles".

The distribution of skill bundles within a country affects its specialisation in certain industries and its integration in international markets and GVCs (Ohnsorge and Trefler, 2007; Bombardini, Gallipoli and Pupato, 2012). This implies that two countries with similar skill endowments may end up specialising in different industries and position themselves at different production stages along GVCs depending on the way skills are bundled in the workforce.

This evidence suggests that policies focusing only on certain types of skills may be short-sighted. In particular, STEM-related skills need to be complemented with communication and team working skills. Education and skills policies, which are sometimes regarded as remotely connected to industrial and trade policies, appear to strongly influence countries' industrial structure and specialisation in international trade. Thus, a better co-ordination and alignment of industrial and trade policies with education and skills policies seems necessary for countries to preserve and enhance their comparative advantages.

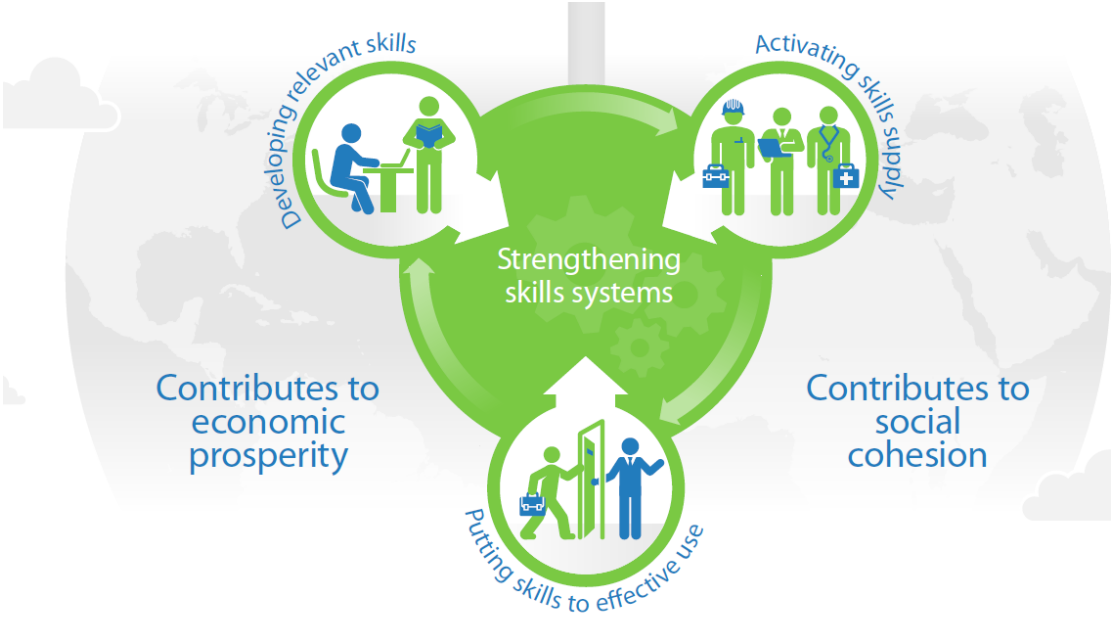
7.4. The OECD Skills Strategy: A focus on the digital economy

The changes in the demand for skills driven by the digital economy present two major challenges to skills development. First, while there is awareness that the skills profile of citizens and workers will be very different than in the past, the skills of the future are difficult to identify with certainty due fast technological change in the digital economy. The second challenge is to ensure that once changes in skills have been identified, skills development systems adjust sufficiently fast to match new skill demands.

The OECD Skills Strategy provides a framework that can help G20 economies identify the strengths and weaknesses of their national skills systems, benchmark them internationally, and develop policies that can transform better skills into better jobs, economic growth and social inclusion. The Skills Strategy is based on three pillars; developing relevant skills; activating skills supply; and putting skills to effective use. G20

economies and societies need to perform well across all three pillars if they are to realise the full benefits of skills for economic prosperity and social inclusion (Figure 40). The Skills Strategy also emphasises that getting better outcomes requires adopting a systematic and comprehensive approach to skills policies that needs to engage all relevant ministries, all levels of government and all relevant stakeholders in working together to identify and take ownership of the country's skills challenges and to develop and implement joined-up strategies and actions to address them.

Figure 40. The OECD Skills Strategy



Source: OECD (2012c).

The Skills Strategy provides a useful approach to address the opportunities and challenges for skill development in the digital economy. This approach consists of three main steps. First, identify more precisely the kind of skills required in the digital economy, through the definition of an agreed framework for digital literacy, further cross-country analysis of existing datasets and the development of new surveys. Second, examine how these changes may translate into curriculum reform, teacher training and professional development. Third, leverage ICTs to improve the access to and the quality of education and training, e.g. through online courses, new learning tools at school and adequate recognition of skills acquired through informal learning.

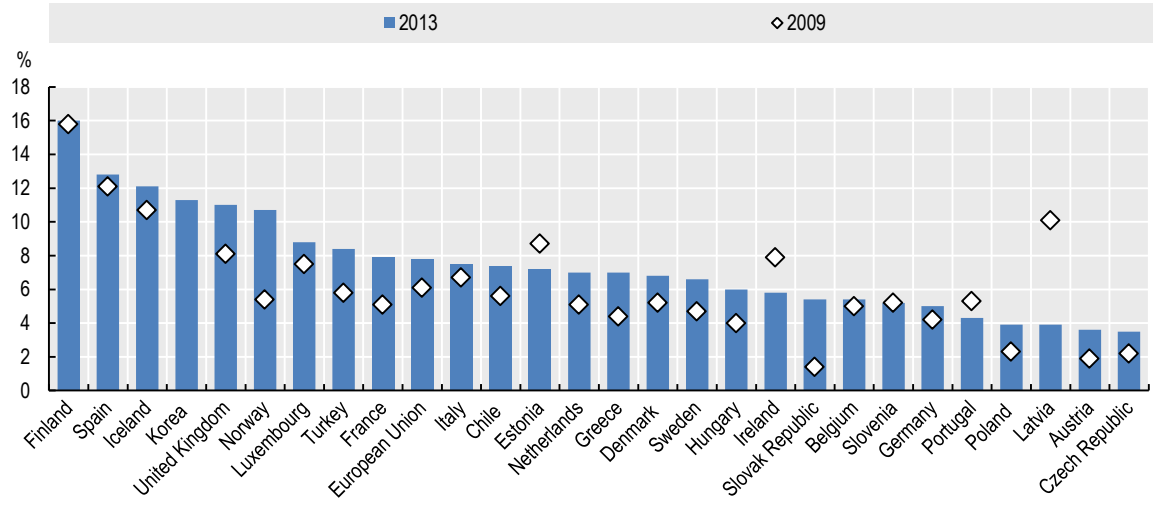
7.5. Leveraging digital technologies for better skills

The pervasiveness of digital technologies today has fed growing expectations of their benefits for education and raises questions as to the reasons why these benefits have not yet fully materialised. Paraphrasing Solow's so-called "productivity paradox", one can see computers everywhere but in learning outcomes. The debate in the educational community is vivid. Many voices claim that ICTs bring up a generational change of unprecedented nature, with far-reaching implications for education. Others argue that digital media and connectivity has far more negative effects on the education of young people than positive ones (OECD, 2012d).

The educational literature provides some insights as to why technology has failed on its promises in radically improving education, pointing to weaknesses in knowledge-management processes, teachers training and incentives mechanisms (OECD, 2010b). At the same time, a growing body of research is addressing these issues and providing evidence for the positive effects of ICTs in opening new forms of learning for the 21st century.

While raising the demand for new skills, digital technologies are also creating new opportunities for skills development. MOOCs and open educational resources modify learning methods and give access to quality resources to a larger population over more flexible hours (Figure 41). The use of digital technologies in formal education and vocational training has the potential to improve learning, although the outcomes depend on the capacity to link these tools to effective pedagogy. Big data analytics can also complement labour market information systems with a more timely and precise monitoring of changing skills demand to adapt skills development and activation policies.

Figure 41. Individuals who participated in an online course



Source: OECD (2015d).

Finally, the increase in the quantity of data that are collected on education and labour markets on a daily basis through online courses, administrative records and online job vacancies, and their exploitation through data analytics can open endless avenues for research and innovation in education and training and helps to better inform policy decisions.

Digital technologies can also help to identify emerging skills needs, evolving demands and potential skills gaps by providing real-time intelligence on the labour market. Workers, firms and policy makers can monitor changes in occupational demands and adjust their strategies accordingly with potential benefits with reference to school to work transitions and labour market reinsertions. Moreover, digital technologies can help public employment services facilitate the exchange of information about employment opportunities and produce efficiency gains by serving larger audiences at similar or lower cost.

In spite of their potential, these initiatives have, thus far, remained a niche. Barriers to their adoption include limits on learners and teachers/trainers' capacity to take advantage of digital technologies; concerns about the quality of online education; and the lack of recognition for learning outcomes. Policies to overcome these barriers and to ensure consistency and quality, especially in an international marketplace, are key to grasping the learning opportunities created by these tools.

7.6. Key areas for policy action

While there are challenges to ensuring that all working age adults in G20 economies have the skills they need to compete in a world that is increasingly digital and data-driven, it is a challenge that governments must meet. While the future is uncertain, governments can nonetheless help their populations to adjust and adapt through concerted policy action.

Develop strategies that enable all working age adults to adapt to and excel in the digital economy

The development of strategies that enable all workers to adapt to and excel in the digital economy, including through the use of ICTs and other technologies to upgrade skills, is essential. This implies identifying the mix of skills needed to boost quality employment and active participation in a digitalised economy as well as promoting policies and targets to promote their development and use. It also means facilitating continuous adaptation as changing task requirements on-the-job put pressure on formal education and training systems to remain up-to-date. At the same time, given that the skills gap tends to be larger for people in low-skill occupations than for those in middle- and high-skill occupations, it is especially important to ensure that adults with weak literacy, numeracy and digital skills can easily take up opportunities to improve their skills so that they too can participate fully in society and share in the benefits that ICTs and other technologies can bring to all of society.

8. DIGITALISATION, SMES, START-UPS AND DYNAMISM[9]

- Important differences in ICT adoption and usage exist between large and smaller firms, with SMEs facing several barriers to adopting ICTs and digital technologies in their operational activities, in particular in having the resources to acquire the necessary complementary knowledge-based assets, such as organisational and human capital. There are also important differences across manufacturing and services sectors.
- While recent years have shown a growing trend towards buying ICTs as a service, SMEs lag in their adoption of cloud computing and other sophisticated digital technologies. It is essential to help promote adoption of these digital technologies among SMEs because they can help overcome some of the traditional barriers to investing in digital technologies, including the often high, upfront sunk costs of these investments, and allow them to switch more rapidly from one technology to another to avoid being locked in. Comprehensive national digital strategies that take into account SMEs, policies that facilitate access to finance, and SME engagement with competency centres and/or technology diffusion extension services can be helpful in this regard.
- A number of key indicators such as firm entry and churning rates suggest that business dynamism in many G20 economies and OECD countries has declined over time, especially following the crisis. Based on entry rates, declining business dynamism appears particularly strong in ICT-producing and ICT-using sectors, raising concerns about innovation. At the same time, when analysing patterns in ICT use, there appears to be a considerable gap in technology adoption between plant size and age, with plants that are both younger and smaller less likely to use data management software than those that are larger and older.
- Boosting business dynamism and promoting the growth of start-ups and innovative SMEs, as well as supporting start-ups and SMEs in leveraging digital technologies, are important areas for policy action. Policies that can help include facilitating access to finance, building on the *G20/OECD High-level Principles on SME Financing*. Pro-competitive product market regulations and employment protection legislation that is not overly stringent can also foster firm dynamism and the adoption of certain digital technologies. Policies that facilitate the mobility of workers as well as training and skills development are important to help smaller firms compete with larger, established incumbents.

8.1. The policy challenge

The ability of SMEs to swiftly adopt new technologies, to learn by doing, innovate, and optimise their production, is constrained by their small scale, limiting their ability to reap the benefits of the digital economy. It is essential to foster use of more sophisticated digital technologies among SMEs, especially cloud computing, which allows smaller firms to overcome some of the barriers associated with the high-fixed costs of ICT investment. The overall success of SMEs in embracing digitalisation in G20 economies also depends on a sufficiently dynamic business environment, where innovative digital start-ups can grow and reach scale, and where the least productive firms are eventually closed down or restructured. Recent analysis suggests that young and small firms are often much more affected by poorly designed regulatory frameworks than large and incumbent firms, limiting their growth and reducing overall business dynamism. Policy action to boost the growth prospects of start-ups and SMEs is thus essential.

8.2. Digitalisation and SMEs

The use of digital technologies is now almost universal in many G20 economies, but less so for SMEs (see Chapter 1 on access). As discussed already there, SMEs have many potential benefits that they can draw from digital technologies, for example:

- **Better access to skills and talent**: SMEs and entrepreneurs face significant challenges in finding and affording qualified workers, but better job recruitment sites, outsourcing and online task hiring can make it easier to find people with the appropriate skills.
- **Greater access to markets**: The Internet allows firms to access markets all over the world at relatively low cost, enabling them to reach scale. Some SMEs even manage to internationalise their activities thanks to better access to digital technologies, including the Internet and mobile telecommunications. There is even some evidence on the emergence of so-called "micro-multinationals", i.e. small and young firms that are born global.
- **More extensive access to financing**: The Internet is an increasingly important source of financing for firms. Various types of online crowdfunding have emerged over the past few years and offer new opportunities for entrepreneurs and SMEs to obtain funding. Moreover, digital intangible assets (e.g. IP) can sometimes also be used as collateral by firms, facilitating their access to finance.
- **Better collaboration and communication**: The Internet also provides extensive opportunities for SMEs to collaborate with others in ways that weren't possible before due to a lack of time, resources, or connections. This includes collaboration among SMEs and entrepreneurs via solutions such as incubators, research clusters and online tools. It also facilitates SMEs' participation in global value chains.
- **Greater access to technology and applications**: Through cloud services, the Internet also provides SMEs with access to a wide range of technologies and applications, including big data analytics, helping firms to solve problems at a much lower costs than before.
- **More extensive product development**: Crowdsourcing via the Internet provides a way for SMEs to design and develop products, and work around traditional barriers to expensive research and development.
- **Reductions in red tape**: More indirectly, the administrative burden generated by governments for starting and running companies can be significant, but online government portals for information on business creation and registration can help lower the burden on SMEs.

Despite these potential benefits, SMEs lag in the uptake of ICTs relative to larger firms. This is because SMEs face a range of barriers in adopting ICTs and other digital technologies in their operational activities. SMEs tend to have limited financial resources, which makes adopting new technologies, including ICTs, difficult given these tools are often expensive. Another important barrier is related to human and organisational capital since investments in new technologies often require investments in complementary knowledge-based assets. SMEs do not often have the skilled people to operate new digital technologies in their teams, the resources to train these workers, or have the management that can help them make the most of the new technologies.

However, even if ICTs (and data) are made available, the modalities of their provision can be as crucial as the provision itself. Evidence shows that in particular the lack of appropriate (open) standards and fears of vendor lock-in, often due to proprietary solutions, can be strong barriers to adoption. This is particularly true for SMEs, which often lack the negotiating power and the know-how about advanced ICTs such as cloud computing, data analytics, and the IoT (see OECD, 2015e, 2016m).

For many digital technologies, a lack of trust in the digital economy has also been raised as a potential barrier to ICT adoption (OECD, 2008b, 2015a, 2016d). This is to a large extent due to the increasing digital security

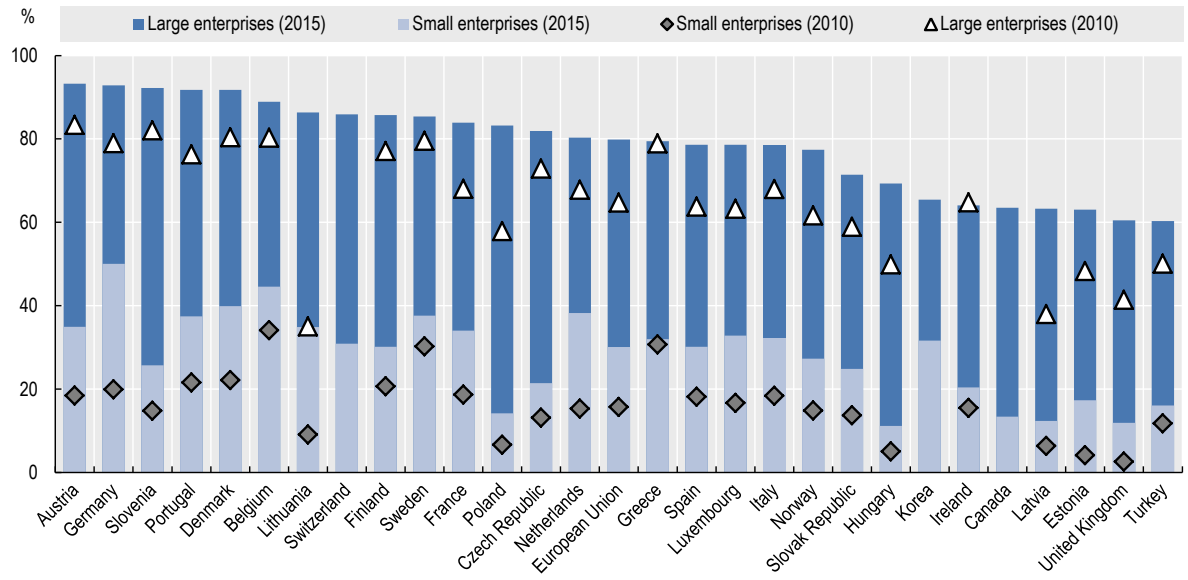
risks perceived by potential adopters, which is partly also the result of the increasing sophistication of digital security threats. In addition, increasing concerns have been raised with respect to whether privacy and IPRs are sufficiently protected (and enforced) in the digital economy. There are also additional risk factors associated with emerging practices in the use of personal data and intellectual property that risk deteriorating trust in the digital economy, and thus reducing incentives to ICT adoption. For instance, discrimination enabled by data analytics, for example, may result in greater efficiencies and innovation, but may also limit individuals' freedom (OECD, 2015f).

SMEs also often face a deficit of knowledge and awareness of the chances and new business opportunities offered by digitised business and work, which then leads to a poor ability to change and competitive disadvantages. A 2014 survey among 1 000 SMEs in Germany revealed that for 70% of enterprises with annual revenue below EUR 500 million, the digitalisation of processes was still seen irrelevant. What is making the situation worse is that many of the currently available ICT products and information do not necessarily take the specific needs of SMEs into account. A study funded by the German Federal Ministry of Economic Affairs and Energy (2015), for instance, confirms that current research and projects on Industrie 4.0 are too often not presenting their results in a format and language that is appropriate to SMEs and skilled crafts.

For some digital technologies (e.g. broadband) small firms are just as likely to use these technologies as larger firms; however, significant adoption gaps exist for most digital technologies (see also Chapter 1 on access). Large adoption gaps across small and large firms exist also for more complex software applications, such as ERP software. Large firms are much more likely to use ERPs than small firms: on average respectively 78% and 27% although there is some heterogeneity across countries (Figure 42). For example, small firms in Germany have the highest propensity to use ERPs (50%). However, even here there is a substantial adoption gap with the largest German firms (with 93% adoption rate). These disparities likely reflect that larger establishments, with access to greater information flows, may yield greater benefits from complex digital technologies like ERP. This gap also reflects – as mentioned above – that large firms are more able to afford the high sunk costs of the ICT and complementary investments in human and organisational capital.

Figure 42. Use of ERP software by firm size, 2010 and 2015

As a percentage of enterprises in each employment size class



Notes: Size classes are defined as: small (from 10 to 49 persons employed) and large (250 and above). For Canada, large enterprises have 300 or more employees. For Iceland and Sweden the data refers to 2014. For Canada and Korea the data refers to 2013 and for Switzerland the data refers to 2011.

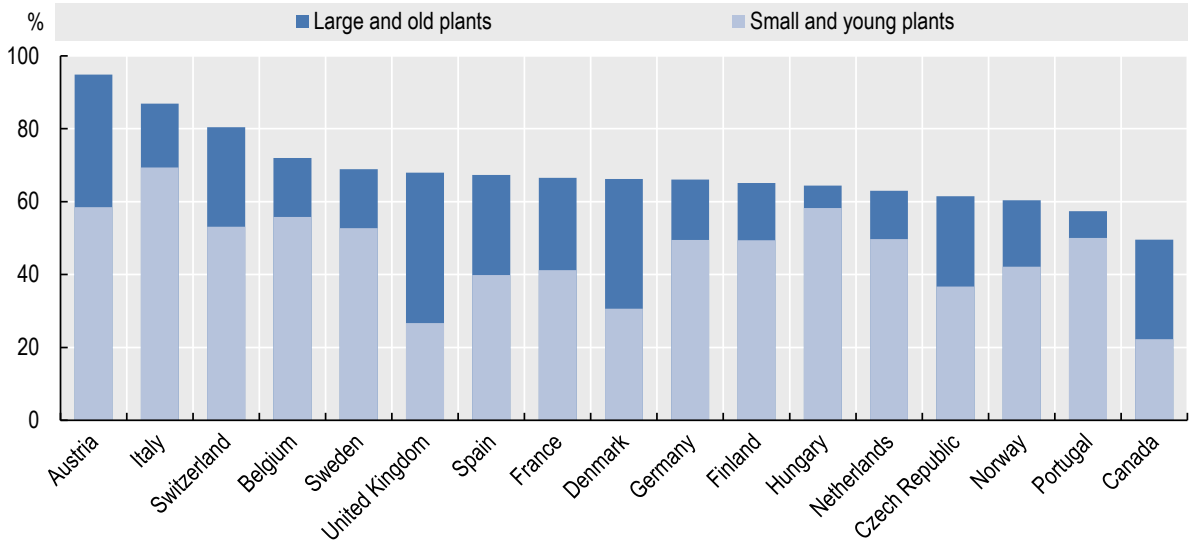
Source: OECD (2015e).

These adoption gaps between large firms and SMEs appear to persist over time. Both small and large firms have increasingly adopted ERP software: On average, 78% of large firms used ERPs in 2015 compared with 64% in 2010, and 33% of small firms used ERPs in 2015 compared to only 16% in 2010. However, even though ERPs have diffused to more small and large firms, the disparity across firm sizes in 2015 remains at similar levels to 2010. On average, large firms remain around 50% more likely to have adopted ERPs than small firms in 2015, a similar adoption gap as in 2010.

The available data also point to systematic differences in the adoption of other complex digital technologies across firms;[10] small and young plants (one to ten years old) are, for example, less likely to use data management software than older and larger establishments (see Figure 43). Although there is considerable cross-country variation, a common finding is that plants that are both younger and smaller are less likely to use data management software than those that are larger and older. On average, 67% of larger-older plants use data management technology, whereas only 41% of smaller-younger plants do so. Similarly, on average 41% of establishments that are larger-older use innovation software as opposed to roughly 11% for small-young plants.

Figure 43. Use of data management software by size and age, 2012

As a percentage of plants in each employment size and age class



Notes: Size classes are defined based on plant employment as: small (from 1 to 100 persons employed) and large (250 and above). Age classes as defined based on plant age as: young (1-10 years) and old (25+ years). Small and young plants comprise a large proportion of new plants of multi-plant firms.

Source: Authors' calculations based on data from CiTDB.

In contrast to the "traditional" investment in emerging ICTs, recent years have witnessed a growing trend towards buying ICTs as a service (Marcolin, Le Mouel and Squicciarini, forthcoming). This externalisation of the costs of ICT investment by purchasing services that are functionally equivalent to ICT investment may help SMEs to overcome the barriers discussed above. Indeed, one reason why firms are beginning to move away from making investments in ICTs is that it enables firms to escape the often high, upfront sunk costs of these investments. Another reason – important for large as well as smaller firms – is that the fast advances in ICTs result in a continual churning of technology use; buying ICT services allows companies, and SMEs in particular, to switch more rapidly from one technology to another as they are not locked in by the large investment of specific ICTs which may become rapidly obsolete because of the arrival of newer – and better – technologies.

However, as shown in Part 1 on the degree of digitalisation, SMEs also lag larger firms in the use of cloud computing, the main vehicle for buying ICT services. In the United Kingdom, for instance, 21% of all smaller enterprises (10 to 49 employees) are using cloud computing services, compared to 54% of all larger enterprises. One important barrier here may be the security concerns that SMEs raise as regards their involvement in cloud services. It is essential to foster cloud computing use among SMEs to help smaller firms rapidly scale up and it provides supercomputing resources in a flexible manner via a pay-as-you-go model, without the need to make heavy upfront investments.

8.3. Digitalisation, start-ups and dynamism

The digital economy is also an important source of entrepreneurship and business dynamism, enabling new firms to emerge and grow. The Internet lowers barriers to entrepreneurship and makes it easier to start, grow and manage a business. It also supports "lean start-ups" that leverage the Internet to lower fixed costs and outsource many aspects of the business to stay agile and responsive to the market. The Internet also affects the broader business environment by lowering transaction costs, increasing price transparency and improving competition. It is now easier for businesses to communicate with suppliers, customers, and employees using Internet-based tools. Improved communication is also leading to the emergence of new and transformed business models.

Recent evidence shows that despite the new opportunities linked to digitalisation, there has been a general decrease in business dynamism across countries. This decline in business dynamism markedly accelerated during the crisis, and the recovery since has only been partial, with broadly similar trends observed for manufacturing and services. More specifically, entry rates appear to have steadily declined over the period, while churning rates and growth dispersion – more stable before the crisis – have dropped considerably since 2009, especially in non-financial business services (Blanchenay et al., forthcoming).

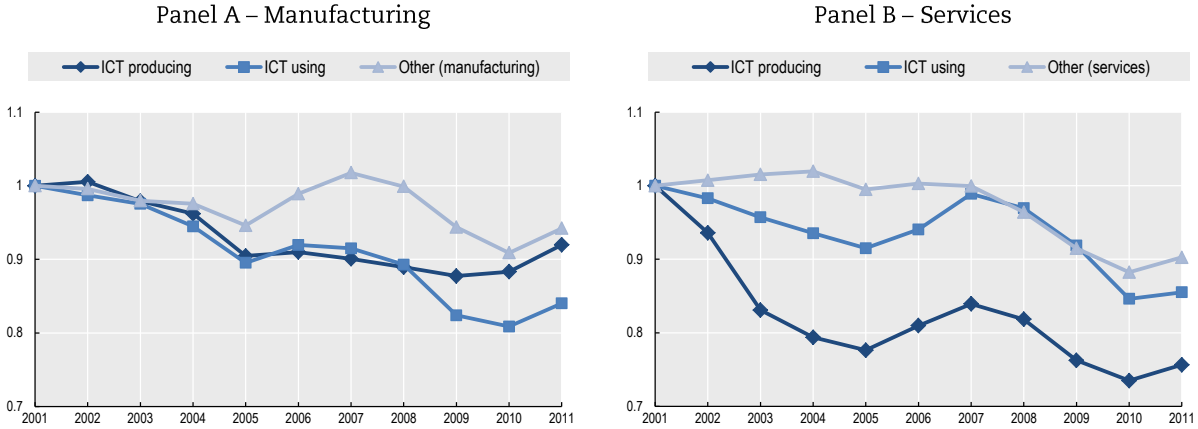
BOX 6. CLASSIFICATION OF ICT-PRODUCING AND -USING SECTORS

ICT-producing sectors are defined following the ISIC rev.4 definition in Annex I of OECD (2007), at the A38 two-digit level to allow matching with DynEmp data. ICT producers are defined as "IT and other information services" and "Telecommunications" from the services sector and "Computer, electronic and optical products" from the manufacturing sector. Other producing industries included in the OECD (2007) definition at the four-digit level (such as "Wholesale of computers, computer peripheral equipment and software") are not included, since these represent a minority of activity when aggregated to the A38 level (in this example, "Wholesale and retail trade, repair of motor vehicles and motorcycles"). ICT intensive-using sectors are defined as non-producing sectors from the DynEmp manufacturing (services) sample located in the top quartile of ICT intensity, where intensity is measured by the compensation to ICT as a share of value-added, using EUKLEMS UK data for the year 2000, following the methodology of Michaels, Natraj and Van Reenen (2014). For some A38 service industries, we use the categories of ICT-intensive users following Van Ark, Inklaar and McGuckin (2003). Consequently, ICT users are defined as "Publishing, audio-visual and broadcasting activities", "Legal and accounting activities" and "Scientific research and development" from the services sector and "Electrical equipment", "Machinery and equipment" and "Chemicals and chemical products" from the manufacturing sector.

This decline in dynamism across countries is particularly marked in ICT-producing and ICT-using sectors. Figure 44 compares entry rates across countries for three broad groups of sectors: ICT-producing, ICT-using, and other sectors (see Box 6 for details on the definitions), separately focusing on manufacturing (Panel A) and non-financial business services (Panel B).

Figure 44 (Panel B) illustrates a strong decline in entry rates for ICT-producing services sectors between 2001 and 2011, with some recovery immediately before the crisis. Milder declines in entry rates occur in ICT-producing manufacturing sectors, with the decline in dynamism concentrated in the early 2000s (Panel A). This is mirrored in the ICT-using sectors, which also exhibit a pronounced decline in dynamism over the same period, especially for manufacturing. However, the remaining sectors of the economy are characterised by a more modest decrease in entry rates, occurring mostly after the crisis. Qualitatively similar patterns also hold true when focusing only on small entrants.[11]

Figure 44. Business dynamism in ICT-producing, ICT-using and other sectors



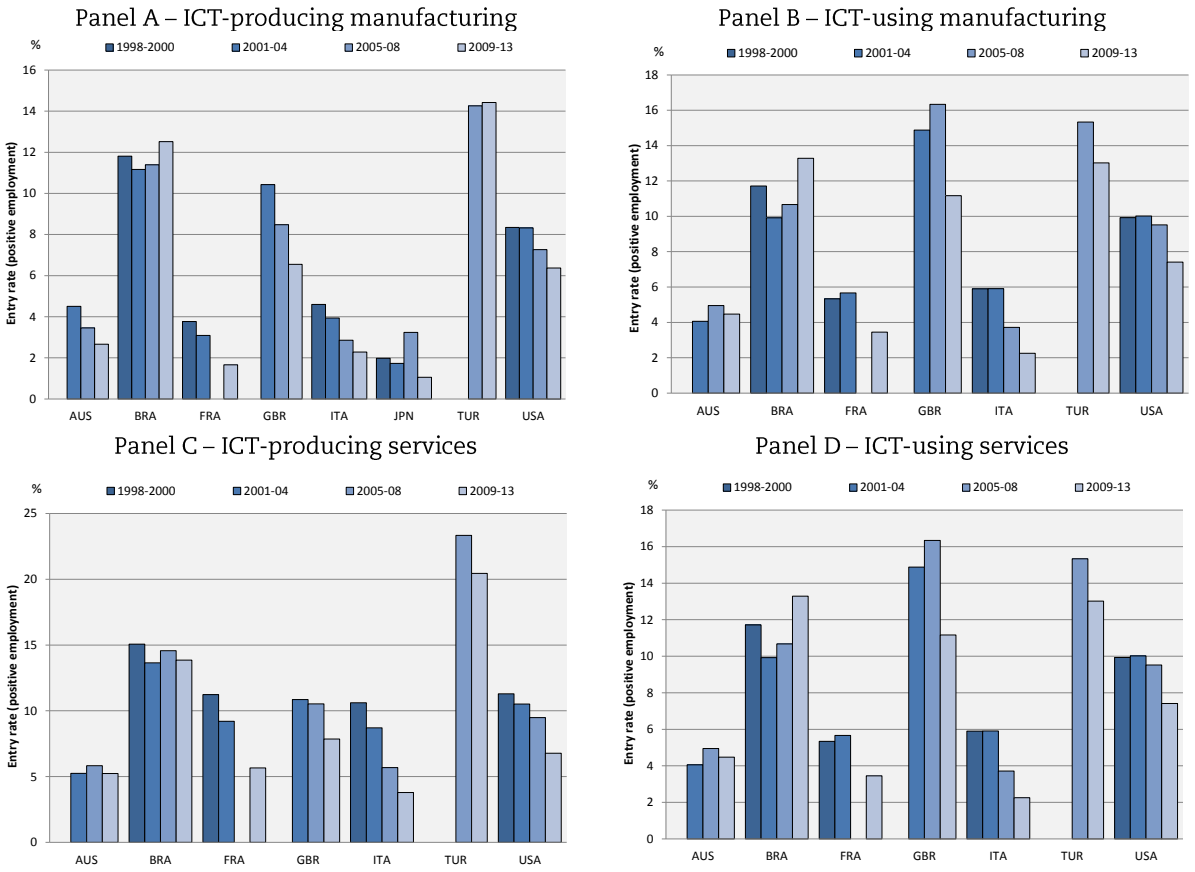
Notes: The graphs illustrate entry rates (number of entrants with positive employment over the total number of units with positive employment) in manufacturing (Panel A) and non-financial business services (Panel B). Three groups of manufacturing and non-financial business services sectors are distinguished (ICT-using, ICT-producing, other sectors). See Box 6 for details of classification of ICT producers and users. Figures report three-year moving averages, conditional on the availability of data. A coverage table is available in Blanchenay et al. (forthcoming). Data for Japan are limited to the manufacturing sector. The time period under consideration ranges between 2001 and 2011. The first available year is set as index year. Owing to methodological differences, figures may deviate from officially published national statistics. Data for some countries are still preliminary.

Source: *OECD DynEmp v.2 database*, http://oe.cd/dynemp.

Declining business dynamism in ICT sectors is evident across the vast majority of countries, with some heterogeneity. Figure 45 shows the business entry rates for ICT-producing and using sectors across the different countries in the sample), separately focusing on manufacturing (Panels A and B) and non-financial business services (Panels C and D). Almost all countries experienced pronounced falling entry rates in ICT-producing sectors during the period, more evidently in services. While there is slightly more cross-country heterogeneity when focusing on ICT-using sectors, the large majority of countries also exhibit declining dynamism in these sectors.

There are several potential mechanisms by which digital technologies influence business dynamism that may provide insights into the declining dynamism found across countries over time. The nature of new digital technologies may favour large firms at the expense of dynamism – reducing the entry and growth potential of new firms. Digital technologies may also trigger dynamics that benefit a minority of leading frontier firms (Calvino, Criscuolo and Menon, 2016; Brynjolfsson et al., 2008). For example, advances in digital technologies have enabled large multinationals to co-ordinate and profit from complex and fragmented production networks (OECD and World Bank, 2015). In some sectors, such as ICT-providing services and other ICT-using services, the significantly decreased marginal cost of both production (provision) and transport (communication) of digital goods (services) have been associated with easier scalability (Brynjolfsson and McAfee, 2011).

Figure 45. Cross-country heterogeneity in ICT-producing and ICT-using sectors: business entry rates

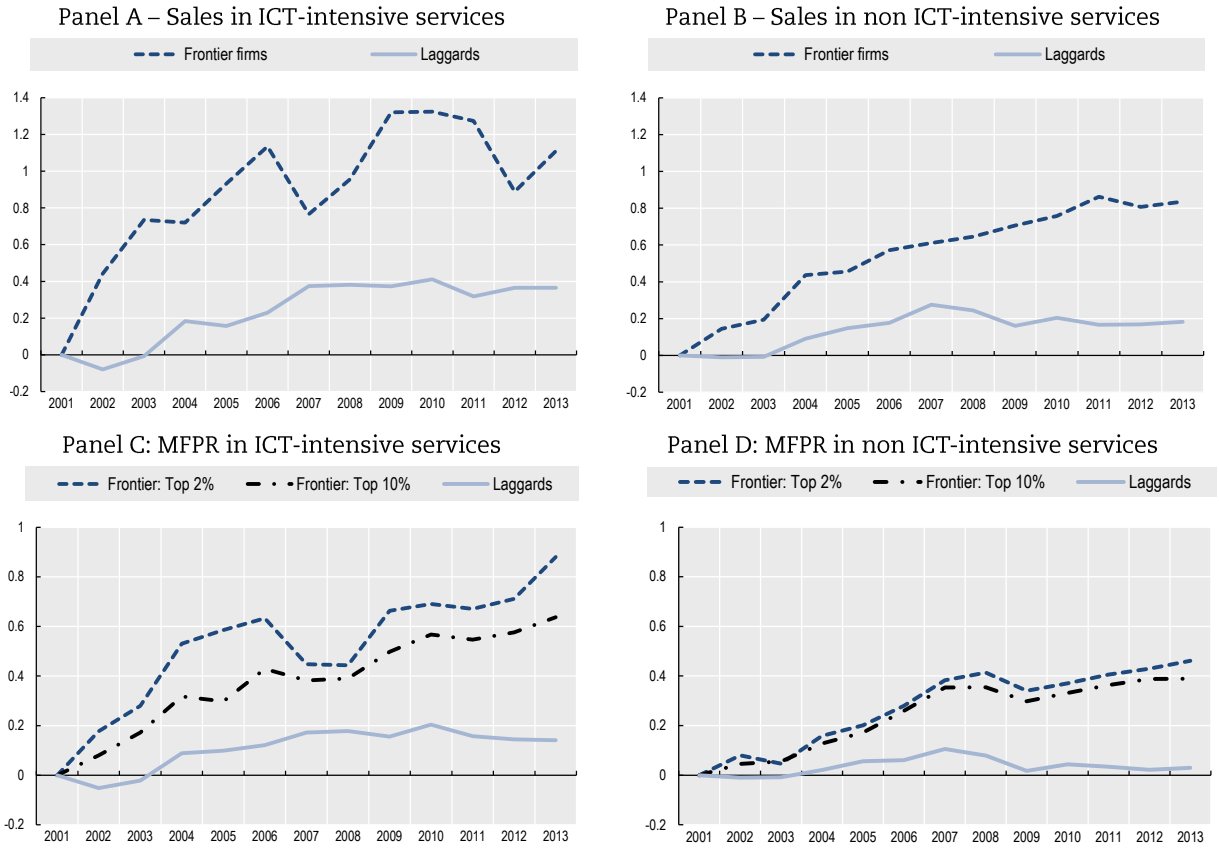


Notes: The graphs illustrate entry rates (calculated as number of entrants with positive employment over total number of units with positive employment) over time in a particular group of sectors. See Box 6 for details of classification of ICT producers and users. Country-specific values are derived as weighted sectoral averages, using the number of units with positive employment in the country-sector-year as a weight. Figures report average country-specific values in the periods 1998-2000; 2001-04; 2005-08; 2009-13, conditional on the availability of data. A coverage table is available in Blanchenay et al. (forthcoming). Only G20 economies are presented, conditional on the availability of data. The period between 2005 and 2008 has been excluded for France due to a redesign of the business register in 2008. Figures for Japan are limited to the manufacturing sector. Owing to methodological differences, figures may deviate from officially published national statistics. Data for some countries are still preliminary.

Source: *OECD DynEmp v.2 database*, http://oe.cd/dynemp.

In some cases, such as social media and online platforms, this has been strengthened by the presence of strong network externalities. These trends have led to a "winner-take-all" dynamics, where the strongest providers take most of the market and even the second best firms take a significantly smaller share of the market (see Andrews, Criscuolo and Gal (2016) for empirical evidence). In particular, Andrews, Criscuolo and Gal (2016) show that divergence in multifactor productivity is accompanied by divergence in sales between frontier and laggard firms, particularly in ICT-intensive services, and that within the global frontier a small cadre of elite firms (top 2%) became more productive relative to other frontier firms, especially in ICT-intensive services (see Figure 46).

Figure 46. Evidence of winner-take-all dynamics



Notes: In Panels A and B, the global frontier group of firms is defined by the top 5% of companies with the highest multi-factor productivity (MFPR) levels within each two-digit industry, while Panels C and D employ two definitions of the global frontier based on the top 2%, and 10% of the MFPR distribution to emphasise a growing dispersion at the top of the productivity distribution. Laggards capture all the other firms. Unweighted averages across two-digit industries are shown for sales and MFPR, separately for services and ICT services, normalised to 0 in the starting year. Time period is 2001-13. Services refer to non-financial business services. ICT-intensive services refer to the information and communication sector (industry code J in NACE Rev. 2) and postal and courier activities (53). See Andrews, Criscuolo and Gal (2016) for further details.

Source: Andrews, Criscuolo and Gal (2016), based on the recent update of the OECD-Orbis productivity database (Gal, 2013).

However, there are several other mechanisms that might explain potential links between digitalisation and declining dynamism. The increasing complexity of new technologies – which may require more investment in complementary knowledge – may have slowed technology diffusion to smaller and younger firms (Andrews, Criscuolo and Gal, 2016). Trends towards early acquisition of start-ups by large technology companies may also limit the incentives for young firms to make long-term scale investments through ICTs and complementary human capital (Decker et al., 2016a). ICTs could present new business models for the expansion of young firms without growing employment substantially, for instance, through enabling purchases of outsourced services along with the use of new types of machinery and robotics (Brynjolfsson and McAfee, 2011; Abramovsky and Griffith, 2006).

8.4. Key areas for policy action

The discussion in this chapter, combined with that in previous chapters on access (Chapter 1), financing (Chapter 3), standards (Chapter 4), security (Chapter 6) and skills (Chapter 7), points to a wide-ranging policy agenda to help SMEs seize the benefits from digitalisation.

Foster SMEs' access to and effective use of digital technologies

It is essential to foster use of more sophisticated digital technologies among SMEs, especially cloud computing, which allows smaller firms to overcome some of the barriers associated with the high-fixed costs of ICT investment. Use of these technologies helps smaller firms rapidly scale up and it provides supercomputing resources in a flexible manner via a pay-as-you-go model, as set out in Chapter 1 on access.

This requires comprehensive national digital strategies; enhancing competition in telecommunication markets and improving Internet access for disadvantaged groups, SMEs and regions. Policies that facilitate access to finance can be useful in this regard, building on the *G20/OECD High-level Principles on SME Financing*, as discussed in Chapter 3 on financing. Such policies will not only facilitate the access of SMEs to the technology itself, but also help them in making the necessary complementary investments, e.g. in process and product innovation, in ICT services or in skills. SME engagement with competency centres and/or technology diffusion extension services can also be helpful.

As noted in Chapter 6, digital security is an economic and social risk that governments and decision makers should address as such rather than treating it just as a technical issue. National digital security strategies can in particular help address the specific needs of SMEs by providing them with practical guidance and the appropriate incentives to adopting good practices. There is, for example, increasing interest in tailored standards and certification schemes developed by or in co-operation with business, and in leveraging digital risk insurance.

Promote firm dynamism and the growth of innovative SMEs

The overall success of SMEs in G20 economies in embracing digitalisation also depends on a sufficiently dynamic business environment, where innovative digital start-ups can grow and reach scale, and where the least productive firms are eventually closed down or restructured. Removing burdensome product market regulations and ensuring that employment protection legislation is not overly stringent helps promote firm dynamism and the adoption of digital technologies by firms. Sound regulatory frameworks (also discussed in Chapter 10 on legal frameworks) that enable digitalisation are essential. This implies ensuring that policies do not unduly favour incumbent firms over new business models.

Recent analysis suggests that young and small firms are often much more affected by poorly designed regulatory frameworks than large and incumbent firms, limiting their growth and reducing overall business dynamism. Calvino, Criscuolo and Menon (2016), for example, finds that the effects of less favourable access to finance, strict bankruptcy regulations, and weak contract enforcement and civil justice efficiency, more strongly affect the growth dynamics of entrants than incumbents. The negative effect of these policy failures on start-up performance is particularly strong in volatile sectors, many of which are ICT producers and intensive users of digital technology.

In addition to these broader policies, there are also good reasons for G20 governments to apply SME-specific policies that enable these firms to effectively leverage digital technologies and helping them expand and grow. Recent research has lighted the growing importance of complementary investments, e.g. in new business processes, may require a renewed emphasis on programmes such as technical extension services that facilitate the diffusion of the necessary knowledge to SMEs. Historically, such programmes have played a major role in diffusing new agricultural technologies. Moreover, extension programmes in manufacturing, some with a broader focus than technology, have been extensively evaluated and can be helpful in complementing broader framework policies.

9. CONSUMER RIGHTS IN THE DIGITAL ERA

- Despite the steady increase business-to-consumer e-commerce, there remains considerable untapped potential. Well-tailored consumer protections and competitive markets are essential to build the trust needed to further develop these markets for the benefit of consumers and businesses alike. More effective implementation of consumer rights is essential for e-commerce to reach its full potential. Policy frameworks in the OECD and UN offer an excellent starting place, but likewise require a greater implementation commitment by governments.
- Cross-border and cross-sectoral enforcement co-operation is but one area for further work. In an increasingly data-centric environment, approaches like data portability offer promise but require further study to ensure that they work for both consumers and businesses. At the same time, G20 economies could usefully explore the issue of platforms and consumer trust with a view to assessing if concerted G20 action could help strengthen consumer trust.
- Consumer choices in this information-intensive environment are impaired by challenges relating to complexity and uncertainty, sometimes compounded by misleading or fraudulent business practices. The expanding reach of platforms – including peer platforms – poses special challenges to consumer trust, while at the same time opening up new opportunities.

9.1. The policy challenge

Thirty-plus years of regulatory reform, coupled with the mainstreaming of the commercial Internet and mobile technology, have repositioned consumers – and their 60% share of GDP – as pivotal. More than ever, active, empowered consumers drive innovation, productivity and competition. As the G20 seeks to address issues of inclusive growth, equity and fairness, the consumer trust agenda is moving to the frontlines, especially with the arrival of hundreds of millions of new middle-class consumers from emerging countries.

9.2. The consumer protection landscape in the context of e-commerce

Continued improvements in consumer access to broadband Internet, particularly through mobile devices, have opened up global opportunities for business-to-consumer (B2C) e-commerce. More than 7 billion mobile subscriptions worldwide were registered in 2015, up from less than 1 billion in 2000 (ITU, 2015). The progressive lowering of trade barriers, the expansion and deepening of global supply chains and, perhaps most importantly, the entry of consumers from emerging markets offer more opportunities for a truly global, consumer-driven e-commerce marketplace.

In the United States, for example, the share of e-commerce as a percentage of overall retail has nearly tripled over the last ten years (United States Department of Commerce, 2016). But it's no longer just the most developed economies that are leading this change. In 2014, the initial public offering of the Alibaba Group – a Chinese e-commerce firm – raised USD 25 billion, the largest in history of the New York Stock Exchange. As of 2013, China was the largest B2C market in the world both by number of buyers and overall revenues (UNCTAD, 2015). In Indonesia, social media is a key driver of e-commerce, where almost 9 in 10 online users have a social media account (UNCTAD, 2015). Another key driver is the use of mobile devices: Indian companies Snapdeal and Flipcart are estimated to take as much as 70% of orders via mobile phones (Meeker, 2015).

Although B2C e-commerce is growing rapidly, it is still a small share of overall retail sales. This is in part because the growth of e-commerce markets for goods, services and information is closely linked to consumer

trust. The trust challenges include not only digital manifestations of risks consumers face offline (such as deceptive commercial practices), but also Internet-specific risks, such as online identity theft and cross-border Internet fraud. And it can be difficult for consumers used to "brick and mortar" shopping to develop the types of geographical, temporal, tactile and social cues for online transactions that they use to navigate transactions and develop trust in the offline environment. According to a 2014 consumer survey, the top two concerns reported by EU Internet shoppers are the misuse of personal data and security of online payments (European Commission, 2015a). In a 2015 US Census Bureau survey, 45% of online households reported that privacy and security concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet (US NTIA, 2016).

The untapped potential of e-commerce is particularly evident in the cross-border context. Only limited data is available, but what there is shows variability among countries. Some reports suggest that more than one-half of e-commerce transactions involving consumers in India and Singapore were cross-border, with cross-border transactions likewise the majority in Colombia, Paraguay and Venezuela. By contrast, in Canada only 20% of online sales value was attributed to customers outside the country in 2013 (UNCTAD, 2015). European numbers are even smaller. Although nearly one out of two EU consumers has shopped online domestically, only 16% have purchased from a seller in another EU country. The situation may be even more difficult when European consumers look outside, with on 38% reporting that the feel confident shopping outside the European Union, as compared with a 60% rate for domestic purchases online (European Commission, 2015c).

One element affecting consumer trust in a global context is the growing range of unsafe products that are available via e-commerce. A key challenge is the share of unsafe products bought online from overseas, with goods banned in one country due to safety concerns being accessible to buyers from another country without knowledge of the ban. Although consumers now have greater tools to help monitor such conduct in markets, the role of well-equipped consumer authorities remains essential to enhance consumer trust in the digital marketplace.

Another important issue involves the varying levels of protection across payment mechanisms. Payment protection may vary from country to country, depending on the payment methods used. In most countries, consumers making a payment with a credit/debit card benefit from the protections attached to such cards. But redress is often unavailable when consumers use pre-paid cards or are being charged on their mobile phone bill. Minimum levels of consumer protection for mobile and online payments are needed, regardless of the payment mechanism used.

Indeed, the opportunities inherent in e-commerce are tempered by the reality that in many parts of the world consumers benefit from fewer regulatory safeguards and good business practices. One study of global consumer protection laws described the coverage of such laws online as "patchy" (UNCTAD, 2015) and the disparity poses particular challenges in the cross-border context. This reality was reflected in the efforts to strengthen consumer protection work in UNCTAD (see below) as well as at a regional level, for example in the ASEAN context.

Raising the level of protection can help enhance consumer trust and capacity to participate in domestic and cross-border trade in a safe and informed manner, helping reduce differences between the well-informed and the less-well-informed, the protected and the unprotected, and, ultimately, the haves and the have-nots. Well-tailored consumer protections are essential to build the trust needed to further develop these markets to the benefit of consumers and businesses alike.

9.3. *Strengthening consumer trust in emerging platform markets*

Digital platforms play a key role in facilitating and structuring the daily activities and interactions of individuals, and therefore lie at the heart of the digital ecosystem. Consumers use digital platforms such as Netflix and

YouTube to watch media content; Uber and Citymapper to plan and book transport; Facebook and Twitter to dialogue and socialise; Alibaba, eBay, Flipkart and Snapdeal to shop, Airbnb and Booking.com to arrange accommodation, and Google and Baidu to retrieve information. This increased societal reliance on platforms has attracted the attention of regulators and policy makers interested in examining the extent and nature of the power exercised by digital platforms and what policies are needed to safeguard the interests of consumers.

The term "platform" has been defined in a multitude of different ways. A report commissioned by the Dutch government usefully classified platforms into four broad categories rather than provide a definitive definition of this term. According to this report, platforms can be divided into: (i) resellers and distributors; (i) marketplaces; (iii) social networks; and (iv) platform of platforms. Within these categories, the report suggests that these platforms differ with regard to their features, including their underlying revenue model; whether they give rise to network effects; and their data and content usage (TNO, 2015).

For the purposes of this chapter, platforms are considered to have two key characteristics. First, platforms are two- (or multi-) sided. Platforms are intermediaries: they connect two or more distinct groups, for instance buyers and sellers, or content providers and individuals. Sometimes this involves the provision of different products to the different groups (e.g. search services for consumers and advertising for firms). This two-sided nature has the potential to lead to direct network effects, where increased use or involvement by one group leads to benefits for other members of that same group. For example, all telephone users benefit from increases in the number of telephone users. Two-sided platforms may also benefit from indirect network effects, where more use by one group leads to benefits for a complementary and distinct group (e.g. more users of a search engine will lead to benefits for advertisers). The other key element is the digital character, which has been essential to the ability of platforms to achieve rapid scale and impact.

The primary benefit of platforms for consumers is that they spur competition among providers of goods, content and services. They do this by correcting and reducing market failures, such as transaction costs and information asymmetries. They also encourage broader market participation from a consumer and provider perspective. This competition, in turn, can lead to direct consumer benefits by pushing down consumer prices, enhancing quality and innovation and increasing choice.

Trust in peer platform markets

Peer platforms are an emerging area with special challenges related to trust. Peer-to-peer transactions have long played a role in commerce, but online platforms enable them on a much greater scale. Early examples include platforms for the sale of goods (e.g. online auction sites). Newer models include the rental of short-term accommodation and transport or mobility services. Using real-time geo-locational data accessed through mobile apps, mobility services rent private cars, rides and parking spaces. Other areas being transformed by these platforms involve small jobs, meal services and financial services. These business models are often described as the "sharing" economy or "collaborative consumption", but those terms do not well capture the commercial exchange dimension that is commonplace in these markets.

These business models open up economic opportunities for the individuals supplying the goods or services ("peer providers") and for the platforms making the connections ("peer platforms"). Consumers can encounter issues of trust in their use of peer platforms in many different contexts: trust into the reliability and qualifications of the peer provider; trust in the asset or service; and trust in the guarantees and safeguards offered by the peer platform.

Peer platform markets provide an excellent lens to explore the operation of trust in online consumer markets. The challenges of building trust in "traditional" B2C e-commerce is exacerbated in peer platforms, where the supplier of goods and services (peer provider) is a non-professional who has not made a significant investment

in the goods or products offered and does not have an established brand or other hallmarks of reliability. These factors may be compounded where there is uncertainty about the extent to which regulations established to protect consumers apply to the transaction. As a result, platforms have developed a number of practical, innovative mechanisms to address concerns and inhibitors to consumer engagement. The most common trust mechanisms developed by these platforms are outlined below:

- **Review and reputation systems**: A central element in helping consumers to make informed choices are review and reputation systems, which can also help regulate behaviour through monitoring, feedback-systems and the exercise of peer pressure.
- **Guarantees or insurance**: In response to negative experiences with accidents, but also theft and fraud, a number of peer platforms have introduced guarantees.
- **Verified identities**: Some peer platforms take steps to verify the identity of peers, which can be particularly helpful in resolving disputes.
- **Pre-screening**: Some platforms offer pre-screening of peer providers, through verification of external databases (e.g. motor vehicle records or criminal background checks).
- **Secure payment systems**: Many peer platforms offer secure payment services, often in co-operation with established external payment systems.
- **Education, checklists and forms**: Many platforms invest in educating users, including with respect to possible legal or other obligations that may apply to traders, drivers, or hosts (OECD, 2016n).

Although the success of peer platform markets is suggestive that the trust mechanisms above are having a positive impact, more experience and evidence is needed for policy makers to assess what additional steps are required to build trust on peer platforms. With respect to reputation and rating mechanisms, there are, for example, questions about the accuracy and objectivity of some reviews, as well as the selection or presentation of reviews by peer platforms. Ratings may be false, biased or reflect socially desirable behaviour or strategic manipulation. More generally, many of these trust mechanisms effectively place the burden of monitoring on consumers, which may come at a particular cost for less-able consumers.

Other trust issues concern the role of data. Peer platforms markets rely extensively on the collection and use of personal data about the peer consumers and peer providers and their interactions. Like other e-commerce and online businesses, peer platforms have to navigate the complex challenge of appropriate governance for the collection and use of this data and provide reasonable security safeguards to avoid the data security breaches and other privacy or data protection problems that have become commonplace. But there is an additional challenge for peer platform markets, which is the responsibility that is also placed on the peers for protecting the data they obtain about each other in the course of their transactions. Relying on these non-professional actors to take appropriate steps to avoid compromise of consumer data may present an even greater risk to consumer trust. At a minimum, raising the level of awareness of these risks would be important.

Addressing information asymmetries and the role of disclosures

Platforms act as intermediaries between different groups in the digital environment. Some operate as “market makers” and play a pivotal role in the digital ecosystem as a result of factors such as their size, business model and connection capacity. For instance, in the European Union nearly half of all Internet traffic goes through only 1% of websites that are actively trading in EU member states (European Commission, 2015b). From a consumer perspective, platforms play a crucial role as entry points for access to goods, services and digital content products by directing individuals towards content and services across the web. This intermediary role therefore leaves platforms in a position of power over consumers, even while opening up opportunities for greater consumer choice and competition, and better tailored goods and services.

Platforms are often criticised for their opaque operations. Profiling and personalisation may, for instance, be hard for users to detect (although this is not unique to platforms). Users may have no knowledge of the selection criteria on which the processes of implicit personalisation are based and they are not provided with any tools to change them or "turn them off". Many services offered by digital platforms, such as search engine services, are deemed to be "credence" goods, whose effectiveness is difficult for a consumer to ascertain. They may be characterised by high levels of information asymmetry such that even after the product or service is consumed it is difficult for the customer to evaluate it. For instance, it is difficult for users of search engine services to evaluate the quality of the search results they obtain, or to know whether these results are "neutral" or are designed to engender a particular reaction.

This could prove problematic in practice as platforms will determine what goods, services and information will be available on their platform and this may have implications for freedom of expression. When platforms decide to exclude a particular application from their store, the user will have limited knowledge of when and why this occurs. Although general policies such as 'objectionable content' guidelines may be available to users, they are not given an insight into how they are applied or the opportunity to contest such decisions. In other words, it is the platform that shapes our digital experiences and determines what we can and cannot see or purchase. This is significant as more of our daily activities are conducted online.

Some suggest that much of the concern regarding platform influence lies in their control over access to individuals and the way in which the relationship between platforms and users is shaped, rather than their control over access to information (Helberger, Kleinen-von Königslöw and van der Noll, 2015). Users, for instance, will not know how limited the news they are obtaining is if they are unaware that their news feed is personalised. This concern may be exacerbated if a digital platform not only registers transactions and perceptions but seeks to create them.

Another example is the use of "dynamic pricing" based on individual profiles. A study conducted by the UK Office of Fair Trading (OFT) on online targeted advertising and pricing indicates that certain misleading pricing techniques could "result in consumers making purchasing decisions they would not have made were prices more clearly advertised, or spending more than they needed to" (CMA, 2015). Another practice, known as "drip pricing", enables businesses to use their power over the online purchasing process to add extra, hidden charges in ways that triggers behavioural biases such as anchoring and endowment effects to prevent consumers from making optimal choices. Consumer protection enforcement agencies in Australia, Canada and the United Kingdom have taken enforcement actions against such practices (OECD, forthcoming d) although these examples are not specific to portals.

A traditional rationale justifying consumer policy market intervention is the need to remedy information asymmetries. One of the general principles of the revised UN Guidelines for Consumer Protection is to meet the need for "access by consumers to adequate information to enable them to make informed choices according to individual wishes and needs" (UNGA, 2015). Effective, well-targeted information can assist consumer decision making by making it easier for them to compare products, increasing transparency and accountability, reducing search costs, helping to prevent disputes and protecting consumers from deceptive practices. Information that is not well-designed, on the other hand, can be useless or even counterproductive.

Behavioural research has shown that how information is presented or framed can have a dramatic effect on how consumers respond to that information. In order for disclosures to be effective they must be carefully designed. A key challenge in this respect is complexity. Research suggests that consumers do not often read privacy notices or the terms and conditions presented to them, and that presenting effective information disclosures is challenging (OECD, 2011c).

9.4. *Promoting effective consumer rights and privacy*

The importance of consumer trust to the development of online markets has been long-recognised. In a 1998 Declaration, the OECD called for the development of consumer protection guidelines to enhance trust in e-commerce and the development of the global marketplace, which led to the original *OECD E-commerce Guidelines* (1999). At the time, e-commerce was a new frontier. It created many new opportunities for consumers, including wider access to goods and services at competitive prices, but also brought challenges.

Newly updated international standards for consumer protection reflect the most recent thinking about how best to frame the protection of consumers online and build trust. The revised *UN Guidelines for Consumer Protection* – adopted by the UN General Assembly in December 2015 – sets out the main characteristics of effective consumer protection legislation, enforcement institutions and redress systems. The UN Guidelines include a specific section covering e-commerce that highlights some of the key considerations for ensuring that consumers are as protected in their online activities as in other types of commerce (UNGA, 2015). G20 economies have been active in the UN work. India has set up a task force to ensure the effective implementation of the new UN Guidelines. Brazil has pending legislation to address e-commerce and privacy. For developing countries, UNCTAD's new Intergovernmental Group of Experts on Consumer Protection Law and Policy has a mandate that includes capacity building and technical assistance that may be of particular relevance.

Even more recent is the revised *OECD Recommendation on Consumer Protection in E-commerce* (OECD E-Commerce Recommendation) (March 2016), adhered to by 12 G20 economies, which sets out the core characteristics of a framework for effectively protecting and empowering consumers in the online marketplace. It addresses challenges relating to information disclosure, misleading and unfair commercial practices, confirmation and payment, fraud and identity theft, and dispute resolution and redress. Updated provisions cover digital content, privacy and security, consumer reviews and ratings, non-monetary transactions, new payment mechanisms, and the use of mobile devices to conclude transactions (OECD, 2016l).

Taken together, the OECD and UN frameworks outline the essential components for developing an overarching set of protections for consumers online. Implementing them in certain areas, however, can pose particular challenges, for example in platform markets which challenge traditional assumptions about how businesses and consumers interact (see Section 9.2). Likewise, the growing importance of consumer data to e-commerce brings additional challenges, pointing to the promise of policy approaches like data portability and enforcement co-operation.

One particular issue of concern for consumers involves privacy. Recognition of the importance protecting consumer privacy has grown immensely in recent years. For example, the revised *UN Consumer Protection Guidelines* now include a provision on the protection of privacy: *Businesses should protect consumers' privacy through a combination of appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data*.

The data generated by consumer online activity has enabled the provision of "free" services in exchange for these data, a development reflected in the addition of "non-monetary transactions" to the scope of the OECD E-commerce Recommendation. The data are also used to tailor services to consumers' preferences but also to build individual profiles. This may exacerbate information asymmetries, risks of discrimination and other privacy harms. Although many countries provide legislative or constitution protection for privacy and other consumer rights, the effective implementation of those rights is challenging in an era of data abundance and in which data flows and business interactions are characterised by a high level of complexity. This section reviews two approaches to approving the implementation of rights in this area. For a more complete approach, the first international framework to address privacy and the protection of personal data was the *OECD Privacy Guidelines* of 1980, which were recently updated (OECD, 2013d).

Fostering greater consumer control over their personal data: The role of data portability

The potential and pitfalls of digitised data generation and processing are well-documented. One policy response has been to consider the question of whether individuals should have the opportunity to obtain access to their own information to use it for personal purposes. This opportunity has been called "data portability" although this term is used to describe consumer rights that vary significantly in terms of their nature and scope.

Various rationales are advanced to support data portability. A common starting place is the notion that data portability can empower individuals, thus leading to better functioning and competitive markets, and ultimately growth and consumer welfare benefits. Data portability can be seen through a data protection lens and can also be considered as a means to achieve the free flow of data. While this initiative extends beyond personal data to encompass all varieties of data, the right to data portability will contribute to the attainment of this objective. Several approaches to data portability are outlined below (Box 7), which emphasise the potential that data portability has to increase competition between providers of goods and services.

Data portability is expected to increase competition between providers of digital goods and services (such as social networking services) and in other analogue markets (for instance, utilities markets). Data portability may enhance competition by (i) reducing information asymmetries between individuals and the providers of goods and services; (ii) limiting switching costs for individuals; and (iii) potentially reducing barriers to market entry.

While there is generally little dispute about the potential benefits of data portability, the attainment of the data portability goals outlined above will pose policy and implementation challenges. These include concerns regarding data security, implementation costs, and the differentiated impact these initiatives may have on consumers. Data security is perhaps the most significant impediment to data portability initiatives, given the very real tension between data access and security (see Chapter 6 on digital security). Verification of identification is a challenge for content and service providers. Some service providers will process personal data about an individual but may not have any significant prior contact with an individual, or they may only hold indirect identifiers for that individual.

A second common challenge for these initiatives relates to implementation costs. If the right to data portability requires companies to adjust their technical capacity to provide access to data in an accessible format this will also increase business costs. There are potential impacts on innovation as well. Data portability might, for instance, deter entry to the market if new entrants are concerned that they are unable to retain users and guarantee a return on their investments as a result of portability provisions. At present, the business plans of many digital providers are based in part on the expectation that they will not need to share their customer data, in particular with competitors.

A third concern is that data portability might have negative implications for equality and diversity. Although savvy consumers might take advantage of data portability opportunities, less confident or less active consumers are less likely to do so. A related concern regarding data portability is that it may conflict with other rights and interests. One example of this is the potential conflict between one individual's right to data protection (exercised through data portability) and another individual's right to privacy. It is easy to imagine a situation where personal data, such as a photograph of two friends, is ported from one social network service to another in a way that violates the second individual's privacy rights.

BOX 7. EXAMPLES OF DATA PORTABILITY INITIATIVES

"My Data" initiatives in the United States

In 2010, the Obama administration launched a series of "My Data" initiatives to facilitate access by consumers to their own personal data in particular sectors. Some of these initiatives relate to data held by public bodies, but others encourage private enterprises to give consumers access to their data. For example, the "Green Button" initiative allows consumers to access their electric utility data and this opportunity is now offered to over 60 million homes and businesses in the United States. The "Blue Button" initiative is a hybrid initiative (applicable to public and private-sector healthcare providers) that seeks to expand patients' access to their medical records. This initiative had, as of March 2016, enabled an estimated 150 million Americans to access their health records from private-sector healthcare stakeholders (including health professionals and retail pharmacy chains).

The UK "Midata" initiative

The UK government introduced its "midata" (then "mydata'") initiative as part of a broader consumer empowerment strategy in 2011. Midata seeks to give consumers access to the electronic information that companies hold about their transactions in a machine-readable and portable format. This transaction data includes, for instance, information that is collected regarding an individual's browsing history and purchases. The midata initiative focuses on three sectors: energy supply; the mobile phone sector; and the financial sector (current accounts and credit cards). Currently voluntary, the Secretary of State may introduce regulations to make midata compulsory if the government is unsatisfied with the progress made.

The EU GDPR "right to data portability"

The European Union's new general data protection regulation (GDPR) sets out a "right to data portability" in its Article 20. This Article provides that individuals shall have the right to receive the personal data that they have "provided to" a data controller "in a structured, commonly used and machine-readable format" and the right to transfer that personal data from one controller to another without hindrance. Furthermore, where it is technically feasible, the individual has the right to have the personal data transferred directly from one controller to another. While personal data is defined in the GPDR as "any information relating to an identified or an identifiable individual", there are a number of limitations to this right. The right to personal data portability only applies where the individual has either consented to the personal data processing or where the information is processed pursuant to a contract. The right also only applies to digitised information processing (when the information processing is automated). The GDPR explicitly states that the right should not adversely affect the rights and freedoms of others. Failure to comply with the right is, however, subject to significant sanctions: at its most serious, a breach of this right to data portability may entail a fine of EUR 20 million or 4% of worldwide annual turnover.

The right to data portability in the Philippines

Under the regulations implementing the Data Privacy Act of 2012 when a data subject's personal data is processed by electronic means and in a structured and commonly used format, he or she shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of a data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means.

Fostering greater cross-border and cross-disciplinary co-operation among enforcement authorities

Cross-border commerce has long generated a need for the agencies charged with enforcing consumer protection laws to work with their counterparts in other countries. An informal network created in the 1990s to facilitate such co-operation, the International Consumer Protection and Enforcement Network (ICPEN), now boasts members from 60 countries, 14 of which are part of the G20. The Internet and other communications technologies dramatically expanded the opportunities for business-to-consumer interactions across borders, with a corresponding need for deeper and more routine cross-border enforcement co-operation. Considerable efforts have gone into addressing the policy challenges of making such co-operation more effective, both in the OECD and UNCTAD. Challenges remain, however, both in expanding the number of countries participating in such co-operation and ensuring that enforcement bodies have the appropriate authority and resources, including the ability to share information with their foreign counterparts in cross-border cases.

A common feature of the concerns discussed in this chapter is the central role of consumer data. Because of the role of data, many of the enforcement challenges discussed fall within the intersection of legal frameworks for consumer protection, data protection, and competition law. The links between consumer protection and privacy (and security) have long been clear, but with personal data now at the core of e-commerce business models, and increasing digital security threats, the need for joined-up approaches in managing risks arising out of consumer data has become essential. The need for co-ordination may spill over as well into sector-specific regulatory frameworks (e.g. communications or financial services or media law).

Traditionally, regulators and professionals charged with overseeing these issues come from different types of agencies and communities but there is increasing overlap in the substantive and organisational challenges they face. There is a need to breaking down the traditional “silo” approach and promoting more co-ordinated governance mechanisms across these different areas. If even modest projections are correct, the growth of the IoT applications and big data analytics will elevate further the role of consumer data in the digital economy. This will most likely raise new issues and different dimensions of existing challenges across consumer protection, privacy and related areas. Ultimately, silo approaches will increase complexity rather than facilitate solutions for maximising the benefits of these new developments while minimising the potential risks.

9.5. *Key areas for policy action*

Shifts in the functioning of businesses and markets are providing huge opportunities for empowering consumers as the Internet expands access to goods and services at competitive prices, bringing with it greater transparency to inform consumer decision making. At the same time, consumer choices in this information-intensive environment are impaired by challenges relating to complexity and uncertainty, sometimes compounded by misleading or fraudulent business practices. And improvements in business transparency do not often extend to the role that consumer data now plays in shaping a consumer's buying experiences and opportunities. Some productive areas for policy action by the G20 that could help enhance consumer rights, build consumer trust, and help deliver on the promise of e-commerce are outlined below.

Effectively protect digital consumers

Establishing a vibrant and dynamic e-commerce marketplace requires broadband infrastructure, hosting and payment facilities and specialised software. But it also requires a willingness on the part of consumers to overcome doubts about transacting at a distance where goods cannot be examined in advance, fears about the risks of entering payment details online, and doubts about whether there can be remedies or redress or if something goes wrong.

The newly agreed *UN Guidelines on Consumer Protection* offer an important starting place for addressing the trust concerns for the protection of consumer in the digital economy. In a number of areas, however, more

specific provisions may be needed, and the OECD E-commerce Recommendation provides a more comprehensive approach that serves as a useful complement to the UN instrument. G20 economies that have not already adhered to the OECD E-commerce Recommendation may wish to consider doing so. As always, effective implementation is a challenge, and there may be a role for the G20 in forging a commitment to do so.

Address the enforcement challenges posed by the cross-border context and greater co-ordination across regulatory silos

Greater co-operation across borders and across regulatory silos would provide a more consistent regulatory environment for consumers and businesses alike. The OECD E-commerce Recommendation calls for improving the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities across borders, through notification, information sharing, investigative assistance and joint actions. A particular focus should be improving the ability of consumer protection enforcement authorities to share information, subject to appropriate safeguards for confidential business information or personal data.

In today's complex, data-intensive e-commerce environment, cross-disciplinary co-operation is also needed. The same practices may violate consumer protection and privacy laws, involving enforcement authorities from both areas. The situation may be even more complex in certain sectors like financial or health services, which have their own regulatory enforcement bodies. A G20 call for greater co-operation and co-ordination among the various types of enforcement authorities which may have responsibilities in consumer data matters would be useful.

Give greater attention to the role of platforms and the challenge of building consumer trust

Platforms offer a multitude of potential benefits to stakeholders in the digital economy, including consumers. Nevertheless, concerns have been expressed about their potential impact on consumer rights and interests. Platforms with “power” have been singled out for special attention in this regard. However, efforts to flesh out the potential and challenges of “platform power” are at any early stage.

Key questions remain to be answered regarding this power and the information asymmetries it creates, along with the appropriate role of regulation. While acknowledging the concerns raised by platforms, it is also important to ensure that policy intervention does not stifle innovation or prevent the consumer benefits from platforms. Given the cross-border nature of digital platforms, G20 economies could usefully explore the issue of platforms and consumer trust with a view to assessing if concerted G20 action could help strengthen consumer trust.

Identify good practice approaches to making data portability work for consumers and businesses

The increasing centrality of consumer data to e-commerce and online activity suggests that innovative thinking is needed to expand consumers’ abilities to access and reuse their data. Data portability is expected to increase competition between providers of digital goods and services and boost the ability of consumers to make more productive use of their personal data. But if not implemented effectively, potential new market entrants may be deterred by the technical implementation costs as well as loss of potential revenue.

There is an evidence gap in this area and governmental study and support is needed. Likewise, additional study is needed to identify which types of portability mechanisms and practices will drive the consumer uptake needed for their success. A forward-looking G20 digital agenda could include data portability as an important area for further exploration with the aim of identifying good practice approaches to making data portability work for consumers and businesses.

10. DIGITALISATION AND LEGAL FRAMEWORKS

- Digitalisation is changing the world faster than many laws have evolved, resulting in some poor fits between laws and digitalised economies and societies. To capitalise fully on the advantages of digitalisation while managing the challenges it can bring, countries should develop mechanisms to periodically review their legal frameworks and, where appropriate, update them to ensure that they are well-suited to the increasingly digitalised world. Designing and implementing a whole-of-government approach to digitalisation is crucial in this regard.
- One important legal area that is being affected by digitalisation is competition. The effects are mixed, with much more competition in most markets but a tendency towards winner-take-all outcomes in others. Competition policy may need to undergo some adjustments in the digitalised context, such as a shift towards looking at data as the most vital competitive asset in some markets, different approaches to market definition and market power, and a greater focus on international co-operation and co-ordination among competition authorities. The G20 may wish to develop tools for assessing the particular complexities of competition in the digital era.
- Online platforms create new markets and opportunities, but also raise a range of economic and social challenges. In this context, labour, consumer protection, tax, and privacy laws are highly relevant. Governments should consider updating laws to address factors that unnecessarily make working through online platforms less attractive, the lack of clarity in certain regulations, tax issues that emerge with the proliferation of small revenues earned via platforms, and consumer and privacy protection of online market participants. More broadly, G20 economies could undertake analysis of the opportunities and challenges raised by online platforms and how different policies may help address them.

10.1. The policy challenge

Legal frameworks tend to evolve more slowly than digitalisation does. This divergence has led to the situation today, in which 20th century laws commonly guide 21st century, digitalised economies and societies. Because of that, concerns have arisen that businesses and consumers are losing opportunities and are facing inadequate protections and greater uncertainty. Accordingly, legal frameworks need to be reviewed and, where appropriate, updated to ensure that they are well-suited to the increasingly digitalised world.

10.2. Digitalisation and competition

While many legal areas are relevant to digitalisation, a particularly important one for digital innovation and growth is competition. Digitalisation promotes greater competition in a large variety of product and service markets, both domestically and internationally. Digitalisation has eroded geographic market boundaries by facilitating the entry and growth of Internet-based suppliers and retailers (e.g. Amazon, Rakuten, Alibaba) that do not need to have a physical presence in all markets where they sell, which has in turn has helped expand GVCs. Digitalisation has also enabled new types of products and services that compete with existing ones (e.g. services that stream television content over the Internet versus cable and satellite TV providers, online-only publications versus traditional print media, etc). In some cases, these new products and services have greatly reduced prices (e.g. financial and brokerage services) and improved services (e.g. movie rentals). Occasionally, digitalisation has helped to make possible new products and services that disrupt well-established markets (e.g. film cameras replaced by digital cameras, digital cameras supplanted by smartphones, compact discs superseded by digital downloads and streaming).

Network effects and scale without mass

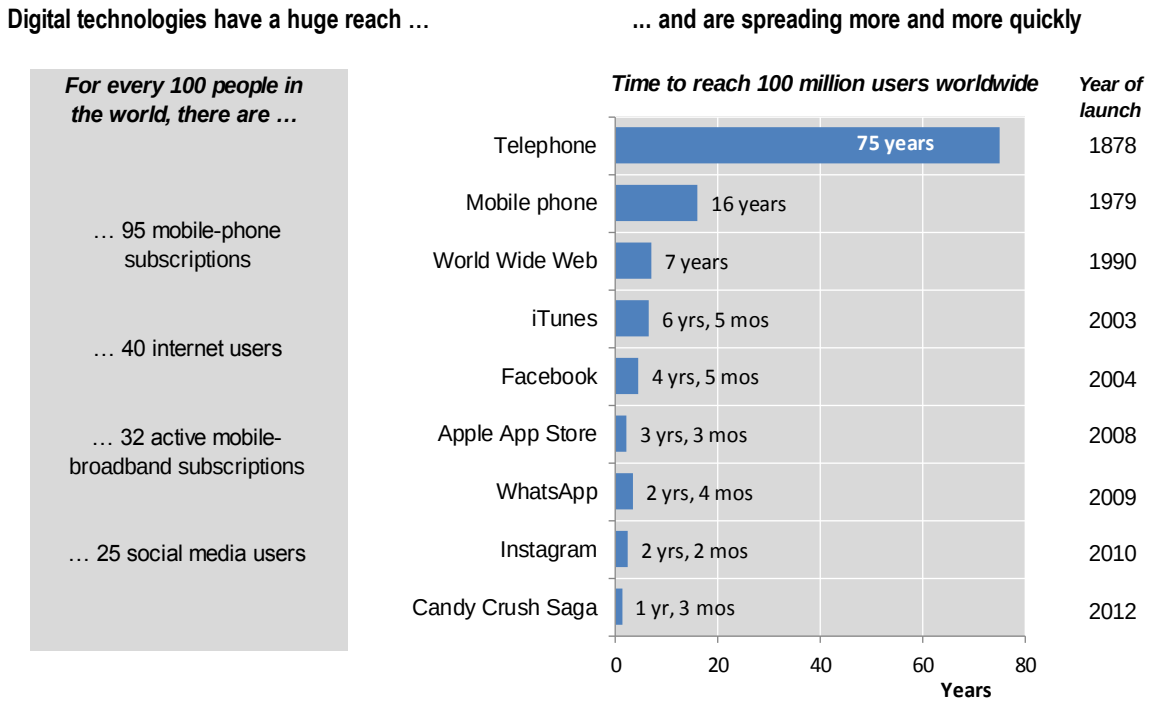
But even as digitalisation leads to greater competition in many markets, it has also demonstrated a potential to tilt others towards greater concentration, market power and even dominance. That is especially true in online platform markets, where network effects and the possibility to achieve "scale without mass" can drive winner-take-all or winner-take-most outcomes. Examples include markets such as social networks, Internet search and advertising, and mobile phone operating systems.

While network effects – the phenomenon that some products, such as the telephone, become more useful as the number of users increases – are widely understood, scale without mass refers to a feature of many digital markets that allows companies to add new users at virtually no cost. These firms do not have to invest in building new plants or doubling raw materials orders if their customers double. This is because they are not producing physical products, so they have no manufacturing plants per se and their raw material takes the form of digital bits, not atoms. Bits are far less expensive to scale up quickly than atoms because bits can be reproduced and distributed at almost no cost, so firms in digital markets can expand their customer bases vastly and rapidly while their physical capital expands at a far slower rate.

While network effects – the phenomenon that some products, such as the telephone, become more useful as the number of users increases – are widely understood, scale without mass refers to the ability to add new users at virtually no cost. Scale without mass benefits purely digital firms such as social networks quite powerfully because they are not producing physical products, so they have no manufacturing plants per se and their raw material takes the form of digital bits, not atoms. Bits are far less expensive to scale up quickly than atoms because bits can be reproduced and distributed at almost no cost, so firms in digital markets can expand their customer bases vastly and rapidly while their physical capital expands at a far slower rate. Scale without mass can also benefit a range of other firms, albeit to a lesser extent, that do business online even if their services or goods are delivered offline.

When a firm operating in a digital market is very successful, scale without mass in combination with network effects can lead to hypergrowth that is all but impossible for even very innovative companies to achieve in physical product markets. Facebook, for example, reached 100 million users just 4.5 years after its launch. Its wholly-owned mobile app, WhatsApp, reached that mark within 3.5 years. In comparison, it took 16 years for mobile phones to gain 100 million users, while wired telephones needed 75 years to reach that mark (Figure 47).

Figure 47. Digitalisation and hypergrowth



Source: OECD, based on BCG (2015).

Although the factors that can create hypergrowth in digital markets (network effects and scale without mass) may bring considerable consumer welfare benefits in the form of affordable and innovative new services, those same factors may also stifle competition by entrenching the market positions of the powerful firms they helped to create. Specifically, a first-to-market firm that benefits from network effects and scale without mass can sometimes become so strong so fast that it quickly leaves subsequent entrants far behind and facing a more challenging set of obstacles to their growth. The entrants' path is more difficult because, unlike the first firm, they are trying to enter a market that already has a large and growing incumbent that is benefiting from scale economies and network effects.

Customer lock-in as a barrier to competition

Furthermore, some incumbents in digital markets benefit from high switching costs, which can lock customers in and make it even harder for entrants to gain a foothold in a market. The more consumers use online services, the more they grow accustomed to them and are reluctant to switch away from them. In addition, the more data customers provide to the service and the harder or more costly it is to transfer that data to a competing service, the less likely the customer is to switch, even if prices rise, quality declines, or the service provides less privacy. And when their data is not tied only to a particular type of service, but to a whole ecosystem of which that individual service is but one part, customers are even less willing to switch. This may happen, for example, with respect to cloud service providers. Thus, network effects, scale without mass, and lock-in effects may combine to reduce competition in digital markets.

Nevertheless, if an entrant has a substantially superior product or service, the advantages of network effects and scale without mass may move from the incumbent to the new entrant and overwhelm any lock-in effect that had previously protected the market leader. When that happens, the incumbent can be dethroned even faster than it had once ascended. Google displacing Yahoo in Internet search and Facebook toppling MySpace are two examples of this phenomenon.

Thus, although the hypergrowth that digitalisation enables in some markets can lead to less competition, it is also sometimes the case that digital firms acquire and lose market power more rapidly than in traditional markets, rising and falling in Schumpeterian fashion. That is to say, digital markets may see a succession of powerful firms periodically displacing their predecessors. This is not competition in the classical static sense, with a large number of rivals simultaneously vying with each other mainly on the basis of price. Instead, it is competition based on innovation, which occurs over time.

Other effects on competition

Other than network effects and steep economies of scale, potentially harmful effects on competition brought by digitalisation include the greater ease of creating and distributing pirated copyright-protected goods and counterfeit trademarked goods. Piracy can reduce incentives to invest in bringing more products and services to the market. Furthermore, by raising digital security challenges, digitalisation may contribute to corporate espionage, which can also reduce incentives to invest and compete (see Chapter 6 on digital security).

Some of the largest effects of digitalisation on competition are likely still to come. 3D printing, for example, has the potential to profoundly transform production and distribution in ways that would destroy some industries while creating new ones. The Alibaba of the future may not sell and ship an enormous variety of physical goods, but rather an enormous variety of downloadable code that enables consumers to print products in or near their homes. In principle, depending on factors such as how widely 3D printing proliferates, this could reduce prices because transportation costs may be greatly reduced. But it is also an open question whether network effects will arise in the 3D printing software market and lead to a winner-take-all or winner-take-most outcome, opening the possibility of non-competitive pricing. In addition, the rise of 3D printing has the potential to make economies of scale virtually irrelevant in many traditional markets, as production will take place in a distributed fashion rather than in a concentrated one.

Adapting competition policy to the digital era

As digitalisation continues to affect competition, it may lead to some adjustments in competition policy, as well. One possible modification is that as digitalisation shifts production from atoms to bits, competition policy's focus could widen beyond goods, services, and revenue to include data as well. That is to say, it could recognise that the rise of digital businesses that offer "free" services in exchange for customer data, for example, implies that data is the key resource in certain digital economy markets. Therefore, data could be considered to be the primary competitive asset in some competition enforcement matters, whether they involve merger control, unilateral conduct, or co-ordinated behaviour.

This would lead investigators and courts to ask questions such as whether two companies that propose to merge would have so much data to mine that no competitors would be able to match them (and whether existing laws could do anything about it if they would). Moreover, a relevant question might be whether privacy should be a consideration in merger reviews when two companies that have substantial amounts of personal data propose to join. Would the merging companies have so much market power that users would have no alternative but to submit to unfavourable privacy terms? In other words, should authorities worry just as much about privacy effects as they do about price effects?

Because digital firms can scale up so quickly, it has been proposed in some G20 economies that competition authorities should speed up their work to remain relevant in digital markets. However, these proposals are founded on the idea that the main purpose of competition law enforcement is to fix problems in the specific market where the conduct is occurring. They miss the point that the larger value of such enforcement (except, perhaps, in merger control matters) is in setting precedents and thereby deterring anticompetitive conduct in many other markets, both presently and in the future.

One approach is to accept the fact that competition policy will not always be able to rescue particular markets in the digital economy from anticompetitive conduct before it leads to dominance. But by continuing to conduct proper investigations with careful analysis, competition authorities can maximise the likelihood of doing the most overall good. Thus, even if taking the time to conduct a thorough investigation results in a given market being monopolised in the meantime by a firm that engaged in anticompetitive conduct, as long as the remedies are appropriate the defendant will learn that its strategy was ultimately a poor choice – and many other firms will learn that lesson, too. At the same time, by taking the time to do their best work, competition authorities will have reduced the risk of false positives and false negatives alike, along with their attendant chilling effects on legitimate competitive conduct.

An additional modification that may be needed is to adjust the way in which relevant markets are defined. Defining the relevant market is a necessary step in virtually all competition law cases. Traditional markets are defined using something called a small but significant non-transitory increase in price (SSNIP) test, that helps to locate the market's boundaries in both geographic and product space. But when products are free and markets are two-sided, as in many online platform markets, the SSNIP test does not perform well. One possible alternative, discussed in OECD (2013e), is a small but significant non-transitory decrease in quality (SSNDQ) test. But at this point that is more of a theoretical possibility than a developed technique.

Similarly, the definition of market power may need to be modified. When digital markets are two-sided, two or more user groups benefit from the use of an online platform. Often, two-sided markets involve one market in which the service is free in a pecuniary sense (customer data is usually the value that the provider receives in exchange) while the other side involves a paid service (typically advertising). Commonly defined as the power to control prices or exclude competition, market power's pricing component loses relevance in two-sided platform markets with nominally free services on one side, and in markets where the key competitive factor is control over data rather than control over price. This is the case, for example, with Internet search and advertising, social media and advertising, and email and advertising. Market power analysis (and competition analysis generally) in two-sided markets can be extremely challenging because conduct that is harmless or even pro-competitive on one side of the market can damage competition on the other side, requiring a balancing of effects that is very difficult to carry out objectively and rigorously. Competition policy is also not particularly adept yet at dealing with cases that involve nominally free products. Incorporating the concept that data has value and that it can be a currency with which services are "bought" is new territory in competition policy.

Another possibility is that firms' increased use of big data analytics, together with Internet-driven connectivity, may result in reactive algorithmic pricing that is adept at reaching and enforcing outcomes identical to what collusion would achieve. In other words, the digitalised world may feature computers that are as good as, or are even better than, humans at creating and maintaining cartels. That raises the question of whether today's competition laws could do anything about it, given that they require an actual agreement to collude, or at least a "meeting of the minds" with a reciprocal intention to restrict competition, to trigger illegality. Can computers "agree" to collude, or come to a meeting of their "minds"? Furthermore, simply to be able to detect computerised collusion, competition agencies may themselves have to figure out how to use big data analytics.

Finally, digitalisation raises the stakes for international co-operation and co-ordination in competition policy. Thanks to greater connectivity and bandwidth, more and more businesses are "born global". Business practices in the digital economy therefore have a greater tendency to cause effects across jurisdictions. This creates a risk of jurisdictional disputes, different legal standards being applied simultaneously to the same practice, incoherence in the application of competition law, arbitrage or "forum shopping" by companies looking for the most lenient environment for their business practices, and a decline in the effectiveness of remedies.

10.3. Other legal areas highly relevant for digitalisation

Of course, competition laws are not the only types of laws that are highly relevant to digitalisation. As digital technologies have advanced over the past decades, and as individuals, firms and governments have come to rely on them more and more heavily, a growing portion of legislation has a bearing on digitalisation, including laws that are specifically intended to spur it. Some legal areas, such as freedom of expression, access to information, privacy, and personal data protection, have gained relevance and heightened attention with the rise of digitalisation. The subject areas in which legislation has emerged that are most relevant to fostering digitalisation vary from country to country, depending on the jurisdiction's political and legal systems, its history, economic structure, social norms, etc. However, areas in which such legislation is common among many countries include:

- **Telecommunications** (e.g. spectrum licensing, universal access/services),
- **Privacy** (e.g. personal data protection, transborder data flows),
- **Security** (e.g. critical information infrastructures, cybercrime),
- **Digital identity** (e.g. e-signatures, e-authentication),
- **Intellectual property** (e.g. intermediary liability, digital content products),
- **E-government** (e.g. public sector information, public procurement),
- **Consumer protection** (e.g. electronic and mobile commerce and payments),
- **Environment** (e.g. electric and electronic equipment recycling), and
- **Safety** (e.g. online product safety, protection of children online).

The transformative and sometimes disruptive effects of digitalisation in more recent years have led many governments to review legal frameworks in an even broader range of areas. Areas that have gained particular attention include:

- **Trade** (e.g. telecom and computer services, trade facilitation),
- **Labour** (e.g. regulated professions, independent work),
- **Tax** (e.g. corporate profit shifting, small earnings), and
- **Sector-specific legislation** (e.g. health, energy, transportation).

While some issues raised by digitalisation clearly need a legal response and legal certainty is crucial for many aspects of digitalisation, it is less clear how other issues should be addressed. In today's environment of rapid digital innovation and given the wide application of digital technologies in the economy and society, a comprehensive legal framework for digitalisation would likely become obsolete rather quickly. Providing an experimental space for legislation and considering industry self-regulation are two options for finding ways to strike a sustainable balance between laissez-faire digitalisation and heavy-handed legal intervention. In addition, high-level principles can serve as a guide for policy makers, business and society to orient and prioritise decisions throughout the process of digitalisation.

Seizing the advantages while meeting the challenges of online platforms for labour, consumers and taxation

Most of the policy areas mentioned above present both opportunities and challenges for lawmakers who are aiming to develop sound legal frameworks for digitalisation. This point can be illustrated with a brief, but closer, look at labour, consumer protection, and tax policies in the context of online platforms. Online platforms create labour markets with low entry barriers, in particular for individuals who value flexible work

and income opportunities. Becoming a driver for Uber or a host on Airbnb is easier for most than becoming a taxi driver or a hotel owner. Beyond driving and hosting, there are many other services that individuals can offer in online platform markets and provide independently, without being in a traditional employment relationship. In addition to low entry and exit costs in platform service markets, the possibility to self-determine the time – and in some cases the place – of work, can be beneficial for unemployed, physically handicapped, elderly people, child carers, or anyone who has difficulties to participate in the labour market, including women in countries where women are not allowed to work.

In many countries, however, independent work involves greater risk than permanent employment, and not all independent workers are compensated for that risk. Health and pension insurance, paid holiday and paid sick leave, as well as other benefits are in most countries attached to permanent employment and are co-financed by employers. Independent workers, including those in online platform markets, have to finance such safety nets and benefits themselves. While some liberal professionals who work independently, such as doctors, lawyers or entrepreneurs, tend to be compensated for the risk they take and can afford private insurance, the OECD found that, on average, non-standard workers tend to suffer wage penalties as compared to permanent employees and thus might not be in a position to cover the additional cost of safety nets and benefits that are common to permanent employment (OECD, 2016o; see also OECD, 2015m).

Another area in need of attention is the common lack of clarity in rules applying to participants (both sellers and consumers) in online platform markets. Rules in many sectors – e.g. obligations attached to a hotel licence – were written for companies. It is not always clear whether individual service providers should comply with the same rules. Similarly, consumers in peer platform markets face uncertainty about how much protection laws provide them, since responsibilities and liabilities for platforms and for unincorporated individuals with respect to consumers, including their privacy, are often not clearly defined. The uncertainty for individual providers and peer consumers in platform markets as to what rules are applicable to them might discourage many to participate in such markets.

Taxation is another area in which online platforms present both opportunities and challenges. Ensuring that the many small providers in platform markets comply with tax laws can be more difficult than ensuring that a much smaller number of large firms comply. For example, many countries may have difficulties making sure that individuals declare small incomes they earn in online platform markets. The challenge becomes even greater when individuals earn several small incomes on different platforms. At the same time, online platforms could offer new possibilities for ensuring tax compliance in their markets. If platforms would co-operate with public authorities, e.g. by exchanging data on the revenue of individuals trading on their platform, tax collection could be facilitated and enforced more easily than in traditional markets that are not digitally monitored.

10.4. Fostering innovation in the digital economy through legal frameworks

Across all legal areas that affect digitalisation, a risk of continuing to use 20th century laws and regulations in the 21st century is that, having been designed for the pre-digitalised world, they could inadvertently shield incumbents from new competition that digitalisation could bring, thereby thwarting innovation. That, in turn, could translate into poorer growth in productivity, jobs, and well-being.

However, reforming policies that unintentionally block, deter, or retard entry by disruptive firms can be a challenging task because those policies usually serve other, legitimate objectives. Making matters more difficult, incumbent firms sometimes respond to potential (or actual) disruption by lobbying for existing regulations to be applied to a new entrant even when those regulations are not well-suited to the disruptive innovation. Rightly or wrongly, incumbents may claim that the disruptor will have an “unfair” advantage unless the regulations are applied to it. Furthermore, incumbents may lobby for new regulations that are simply a pretext for blocking entry.

Examples have arisen concerning peer platform markets for services such as ride and home sharing. Uber, for instance, has been fined, banned, or targeted with new regulations in Canada, France, and Germany, among other countries. The pro-Uber arguments in these cases tend to be that taxi regulations were designed for a business model that Uber has made obsolete: a limited number of taxi drivers, licensed to operate by local governments, charging inflexible rates set by a regulator. Uber's opponents tend to argue that the regulations are necessary because their purpose is to ensure that taxis and their drivers are safe and trustworthy, while price controls ensure that prices are "fair".

Several competition agencies, including those in Canada, France, Germany, Italy, and the United States, have reviewed these arguments and spoken up in favour of easing regulatory restrictions on Uber. They have issued official letters and reports urging reviews of taxi regulations to identify which ones are truly necessary, as well as reforms to permit app-based ride services to continue operating.

Heimler (2015) has pointed out that many disruptive digital businesses which have gone on to become major global enterprises originated in the United States (e.g. Google, Apple, Facebook, Amazon, Uber, Airbnb). He argues that this is a reflection of the less restrictive regulatory environment in the United States. If he is right, then the success of those businesses provides a vivid illustration of what is at stake for countries that continue to enact and enforce regulations that protect incumbents and discourage digital innovation.

Furthermore, recent work by the OECD (2016p) has shown that a poor legal and regulatory environment – e.g. poor contract enforcement and lengthy bankruptcy procedures – affects start-up firms much more than incumbents, and particularly so in high-growth and volatile sectors such as ICT and business services. This finding may suggest that delaying reforms in these areas may be particularly detrimental for start-ups employing innovative business models and technologies, rather than for established firms.

Other parts of the legal framework can unintentionally impede innovation, too. Intellectual property laws are an example, which is counterintuitive because the purpose of such laws is actually to promote innovation and creativity. But incumbents sometimes manipulate IP laws to block legitimate competition, such as by tying up a potentially disruptive entrant with an infringement lawsuit that has little or no merit. The entrant may not be able to fund a legal defence, particularly if it is an SME, or it may decide that doing so is simply too risky. It might then concede its disruptive advantage in a cross-licensing agreement, sell out to the incumbent, or withdraw from the market altogether.

Finally, policy makers may inadvertently impede innovation by addressing issues arising from digitalisation with new regulations that affect large and small firms disproportionately – to the detriment of the small ones. For example, digitalisation has made cross-border requests or demands for digital content takedowns, domain name seizures, and government access to personal data held by private companies fairly common. These requests can come from many different jurisdictions, each one with different laws and legal procedures. But whereas very large firms can afford to process them with care, resolving jurisdictional and substantive issues attentively, start-ups and SMEs may not be able to do so.

10.5. Regulatory experimentation in the digital economy

Adjusting legal and regulatory frameworks to fit the digitalised world takes time. In fact, it is necessarily a continuous process because frameworks have to keep evolving as digitalisation continues to reshape economies and societies. It will not always be immediately clear which adjustments should be made. Therefore, governments have an interest in maintaining enough flexibility in policies affecting the digital economy to allow for some experimentation with legal and regulatory frameworks.

One way to experiment is to set aside zones, virtual or physical, in which new regulatory approaches to digitalisation issues can be tested. Several countries have designed such experimental zones. For instance,

South Korea has opened numerous "creative economy and innovation centres" around the country. These are integrated facilities that focus on regional specialties to enhance South Korea's creative economy. The centres support individuals and entities with creative ideas for commercialisation, facilitate innovation, nurture specialised regional businesses, provide a business platform for start-ups and SMEs to innovate and grow in collaboration with large corporations, and create or match jobs for young people using the network of each innovation centre. To achieve those ends, South Korea carried out a number of regulatory reforms to lay the legal basis for the centres, such as revising the Regulation of the Establishment and Operation of the Public-Private Joint Committee for Creative Economy and the Framework Act on Science and Technology (OECD, 2016q).

In Germany, an industrial data space initiative was launched in 2014 by leaders from the business, political, and research communities. It consists of a research component, funded by the German Federal Ministry of Education and Research, and a non-profit user association. The objective of the research component is to develop and pilot a blueprint for various implementations of the industrial data space. The main function of the user association is to determine and analyse the needs of user companies that would be met by the data space. It also participates in the development of the blueprint and promotes its standardisation. The standards and governance models that apply within the industrial data space are designed to make it easier for users to securely exchange and link data in their business ecosystems. The overall aim is to spur the creation and use of smart services and innovative business processes while preserving the data owners' control over their own data (Otto et al., 2016).

10.6. Key areas for policy action

The challenges described above suggest two areas in particular that are ripe for policy action.

Design and implement a whole-of-government approach to digitalisation

Policymaking in the digitalised world requires a coherent, whole-of-government approach. Governments should use and co-ordinate the full array of their policy levers to keep digital markets performing well. To do that, they need comprehensive information about how the rapid rise of the digital economy has affected various law and policy areas such as competition, taxation, trade, the transfer of data across borders, transportation, investment, labour markets, institutions, etc., although the speed and scale of digitalisation varies. For example, we already know that digitalisation is significantly impacting labour markets as well as tax authorities, but other policy areas are just beginning to be affected. We also know that many of the legal frameworks that are currently in place may not be well-suited to the legal issues that online platforms are raising.

There is still much to be learned about digitalisation's effects across the spectrum of law and policy areas. The G20 could therefore call on the OECD and other relevant international organisations to develop a whole-of-economy analysis of the implications of the digitalisation of the economy. This could be a valuable catalyst for political momentum around the digitalisation issue. In particular, a framework for analysing digitalisation at the country level, building and expanding on the assessment of digitalisation (Part 1 on digitalisation indicators), could be useful. Such a framework currently does not exist, and insights from a range of policy communities could help provide a whole-of-government view of digitalisation and how laws and policies may need to adapt. The identification of a G20 "pilot" country to test such a framework could be helpful in this regard.

Develop tools and approaches for assessing competition in the digital era

With respect to sectoral regulation, governments can take steps to ensure that they do not inadvertently impede competition in digital markets with policies that protect incumbents. First, countries should review

regulations in markets where digital businesses have entered, updating provisions with the aim of eliminating measures that are no longer needed, adding ones that are needed but missing, revising ones that no longer achieve their stated aims or that unnecessarily restrict competition, and ensuring that all competing firms, whether incumbents or entrants, are subject to the same regulatory constraints.

To make regulatory reviews easier and more effective, the OECD has designed a generally applicable Competition Assessment Toolkit that helps governments to ensure that their laws and regulations do not unnecessarily stifle competition and assists them in developing less restrictive approaches that still achieve government policy objectives.[12] Building on this toolkit, the G20 could call on the OECD to augment this toolkit in light of digitalisation so that it is a state-of-the-art resource for governments wishing to make their regulations of the digitalised economy as pro-competitive (or at least as competition-neutral) as possible. Other steps include encouraging competition authorities to engage in competition advocacy before regulatory bodies and lawmakers, and to take direct enforcement actions to remedy laws and regulations that unnecessarily block or deter competition whenever such actions would not be thwarted by immunity to competition laws.

High-level principles could also be developed to guide G20 economies in the development, review and implementation of competition policy in light of digitalisation. As noted above, some adjustments to traditional competition analysis concepts like market definition and market power may be needed for certain markets, so having a set of guiding principles would be helpful. In addition, such principles could also guide overall approaches in some cases. For example, concerning competition policy in online platform markets, governments should focus on keeping markets open and therefore susceptible to entry and disruption so that they remain dynamic and innovative, not on shorter term concerns. In other words, if these markets inevitably create winner-take-all or winner-take-most outcomes anyway, then trying to ensure that they are perfectly competitive in a classic (static) sense is probably not a good use of time and resources. A better idea would be to focus on ensuring that neither incumbents nor regulators interfere with the ability of new firms to enter, disrupt and grow, so that there is the potential for the rise and fall of leading firms. That will help to motivate the market leaders to stay competitive and innovative.

Part 3

POLICY RECOMMENDATIONS FOR THE G20

KEY POLICY RECOMMENDATIONS FOR THE G20

The ongoing digitalisation of our economies and societies will only expand and deepen. Digitalisation does not only contribute to productivity and efficiency, but also to broader socio-economic development. It is an accelerator of development and the G20 must be ready to make the most of it. This report provides the basis for constructing an innovative, ambitious, and pro-active G20 digital agenda. Among all the policy recommendations identified in the report, the following set of 11 recommendations represents the core actions that should be considered. Working together to take these actions forward, the G20 could build a brighter common future, using the multi-stakeholder model that has served the international community so well, and progressing towards the attainment of the SDGs. Only by taking a pro-active, 21st-century approach to the digital economy will the G20 maximise the enormous potential the digital economy holds for our economies and well-being.

1. Call for national digital strategies to close the access and usage gaps and ensure that the Internet is for all

Adoption and use of digital technologies vary among G20 economies by demographic categories, industries and firm size, raising concerns about the inclusiveness of the digital transformation. Barriers typically include some combination of a lack of high-quality and affordable infrastructure; a lack of trust in digital technologies and activities; a shortage of the skills needed to succeed in the digital economy; a more reactive than proactive approach to the openness of the Internet; services trade barriers; high costs and poor access to financing for smaller firms; barriers to the reallocation of resources across firms and sectors; and a lack of interoperability of standards. The growing number of digital agendas or strategies established by developed and emerging economies shows the relevance of a whole-of-government approach to address these supply and demand issues in a coherent manner. Calling for national digital strategies that are robust, but flexible enough to adapt to the changes in technologies and social norms, is the first step to closing the access and usage gaps and helping improve economic performance and well-being across the G20 economies.

The G20 could start by sharing national experiences and good practices in developing, implementing and evaluating national digital strategies and fix a target date for all economies to establish or update their own, taking into account more specific goals as set out below as well as other international targets such, as the SDGs and the Connect 2020 Agenda.

2. Boost investment in digital infrastructures and their key enablers

It is essential that the G20 continually invest in the development of digital infrastructures to meet existing and future demand and help bridge digital divides. They provide the foundation for many new services, applications and business models. They are also crucial in underpinning and enabling the digital innovations that are transforming production, including in the context of Industrie 4.0, now and in the future. An important area for policy action involves establishing national broadband plans with well-defined targets and reviewing them regularly. These plans should ideally assess and address the key barriers to the deployment of high-speed networks and services, including the nature of the infrastructure market itself (monopolies, duopolies), geography, administrative barriers, regulatory uncertainty, high capital expenditure, access to spectrum, and in some countries, a lack of basic infrastructure (e.g. electricity) particularly in rural areas.

Given that high-quality digital infrastructures benefit all users on the network, the G20 could agree to share experiences and practices in addressing the policy challenges associated with ensuring competition and investment, and establish a set of joint, agreed upon, and measurable targets to raise broadband penetration and ensure that the important technical enablers, such as access to Internet exchange points, spectrum, and take-up of IPv6, are in place, by a certain date.

3. *Improve framework policies to foster the financing of digital infrastructures (including data) and innovative new business models*

In parallel, G20 economies need to address financing hurdles to further investments in digital infrastructures (including data) and new business models to ensure that the digital transformation is vibrant, innovative and inclusive. Enhancing access to and use of data – itself an important 21st-century infrastructure – is increasingly important to help generate social and economic value. Framework policies are an important lever to affect the financing of digital infrastructures and new business models. Promoting effective and predictable insolvency regimes to ensure creditor rights can strengthen the confidence of a broad range of investors. In addition, taxation, product market regulation, employment protection legislation, and policy-induced barriers to exit (e.g. excessively strict bankruptcy laws) can hinder the financing opportunities for companies, especially SMEs and start-ups. Reducing such barriers boosts competition, encourages inefficient firms to exit, and channels resources to firms that are best able to make use of the resources, ensuring firm dynamism, innovation and productivity growth.

The G20 could agree to map best practices to create a more entrepreneurial culture (e.g. incubators, accelerators, business angel networks and matchmaking services) and facilitate connections among domestic and international initiatives to foster innovative new business models and tap into new sources of financing. To better target policies in support of financing fixed and mobile broadband networks, the G20 could bolster the evidence base by agreeing to collect internationally comparable statistics on the use of digital infrastructures, particularly global data traffic flows.

4. *Encourage the development of standards and standards-based interoperability to support the IoT and Industrie 4.0*

Open, voluntary standards, grounded in bottom-up and market-led approaches, are an important tool especially when dealing with fast-developing technologies and shifts in markets. Appropriate standards and guidelines are also needed to maintain current levels of safety, ensure trust based on enhanced levels of digital security and privacy, improve energy and resource efficiency, and address emerging social and organisational challenges brought on by the digital transformation. Standards-based interoperability is critical for the development of Industrie 4.0 and the IoT. Inclusive standards development can benefit from collaboration and co-operation among the many players that make up the standards ecosystem. Advanced international governance frameworks – building upon both existing public- and private-sector-led processes – and new multi-stakeholder initiatives for the benefit of all, as well as improved or new policy and implementation tools, are necessary to effectively address the complexity of today's interlinked issues in successful Industrie 4.0 development and deployment.

G20 leaders could support the adoption of best practices and policies that enable all relevant actors, including SMEs, to more effectively work together to help foster an interoperable environment in support of the IoT and Industrie 4.0. Given the breadth of standards related to Industrie 4.0 and the IoT, it may be useful to start such a dialogue in a few focused areas (e.g. smart cities and smart mobility).

5. *Ensure competition in the ICT sector and across the economy*

Digitalisation is raising important questions about competition in all G20 economies. The convergence of fixed-line communications, wireless communications and broadcasting over the Internet has created a need for countries to review their regulatory frameworks and public policy objectives to ensure that all market participants have incentives to continue to innovate, compete and invest in the ICT sector. Competition policy may also need to undergo some adjustments, such as a shift towards recognising data and its analysis as a competitive asset in some markets, exploring different approaches to market definition and market power, and undertaking greater international co-operation and co-ordination among competition authorities.

Developing tools for assessing the particular complexities of competition in the digital era would be very valuable.

To promote competition in the ICT sector and the broader economy, the G20 could consider developing a set of high-level principles to guide G20 economies in the development, review and implementation of competition policy, including in a converged environment. Alternatively, the G20 could consider calling on the OECD to supplement the OECD Competition Assessment Toolkit in light of digitalisation. G20 input to augmenting the toolkit would foster mutually-reinforcing competition policy regimes across the G20, which would maximise the potential for growth and innovation.

6. Call for national privacy and security risk management strategies and improve interoperability among frameworks

Trust is fundamental to the functioning of the digital economy; without it, individuals, firms and governments won't use digital technologies, and an important source of potential growth and social progress will be left unexploited. However, the current patchwork approach to privacy and data protection and to digital security across the G20 creates frictions in a data-driven global economy. Greater co-operation in developing coherent strategies for digital security and privacy, and implementing privacy and security risk management frameworks for prosperity, are essential. Issues around access to, use and ownership of data, including personal data, as well as safety, are particularly relevant as artificial intelligence and the IoT, and with it billions of interconnected devices, become a reality. The development of national privacy strategies responds to the specific need to adopt a whole-of-society approach to ensuring privacy and data protection while providing the flexibility needed to take advantage of digital technologies for the benefit of all.

The G20 is uniquely placed to highlight the need to consider digital privacy and security risk from an economic and social perspective and to initiate action to enhance coherence and interoperability among varying approaches and frameworks. Targets could include fostering international arrangements that promote effective privacy and data protection across jurisdictions, including through the development of model privacy strategies. Likewise, they could include fostering digital security risk management strategies. Such strategies should take advantage of the open digital environment by reducing security risk to an acceptable level without unnecessarily restricting the flow of technologies, communications and data. Given the implications for free flows of data and open markets, dialogue with a range of stakeholders, including the trade community, would be important.

7. Craft more effective strategies that enable all people to adapt to and excel in the digital economy

The development of strategies that enable all people – including women and girls – to adapt to and excel in the digital economy, including through the use of ICTs and other technologies to upgrade skills, is essential. This implies identifying the mix of skills needed to boost quality employment and active participation in a digitalised economy as well as promoting policies and targets to promote their development and use. These skills include ICT generic skills, ICT specialist skills, and ICT-complementary skills, including foundational skills, digital literacy, higher-order critical thinking skills as well as social and emotional skills, among others. It also means facilitating continuous adaptation as changing task requirements on-the-job put pressure on formal education and training systems to remain up-to-date. At the same time, given that the skills gap tends to be larger for people in low-skilled occupations than for those in middle- and high-skill occupations, it is important to ensure that the opportunities of ICTs and other technologies benefit all of society. Life-long learning skills and new forms of delivering training will be essential for navigating the digital transformation and the structural changes it will induce.

The G20 has a range of tools to help foster the development of the skills needed to succeed in the digital economy, including the high-level principles in the *G20 Skills Strategy*, which builds on the *OECD Skills*

Strategy, as well as the *G20 Initiative to Promote Quality Apprenticeships*. G20 economies can usefully take stock of these tools and agree to co-operate on a range of capacity-building programmes to better address the skills challenges brought about by digitalisation.

8. Support SMEs in reaping the benefits of digitalisation and addressing the challenges

The digital economy presents opportunities for SMEs, but also challenges. For example, SMEs lag in their adoption of cloud computing and other sophisticated digital technologies, despite the cost advantages that they may offer. It is essential to help promote adoption of these digital technologies among SMEs because they can help overcome some of the traditional barriers to investing in digital technologies, including the often high, upfront sunk costs of these investments, and allow them to switch more rapidly from one technology to another to avoid being locked in. Access to finance is another particularly important barrier for SMEs, who may not always have access to the necessary financing to make investments in digital technologies and the necessary complementary investments in skills, process innovation and digital services, although new sources of finance, including Internet-based financing such as crowdsourcing, can help mitigate this problem.

Building on the *G20/OECD High-level Principles on SME Financing*, G20 economies can facilitate access to finance and help boost business dynamism and young, innovative start-ups. To do so, the development of a joint G20 action plan that identifies the policies that can support SMEs in adopting digital technologies and their effective use could be helpful.

9. Promote consumer protection in the digital era

Consumer choices in this information-intensive environment are impaired by challenges relating to complexity and uncertainty, sometimes compounded by misleading or fraudulent business practices. The expanding reach of platforms – including peer platforms – poses special challenges to consumer trust, while at the same time opening up new opportunities. Well-tailored consumer protections and competitive markets are essential to build the trust needed to further develop e-commerce markets for the benefit of consumers and businesses alike. More effective implementation of consumer rights is essential for e-commerce to reach its full potential. Policy frameworks in the OECD and UN offer an excellent starting place, but likewise require a greater implementation commitment by governments. Cross-border and cross-sectoral enforcement co-operation is but one area for further work. In an increasingly data-centric environment, approaches like data portability offer promise but require further study to ensure that they work for both consumers and businesses.

The G20 can help promote consumer protection across borders by sharing international experiences and good practices with data portability measures and this, in turn, could be useful in determining good practices in this new area. At the same time, G20 economies could usefully explore the issue of platforms and consumer trust with a view to assessing if concerted G20 action could help strengthen consumer trust. To the extent that G20 members have not adhered to the *OECD Recommendation on Consumer Protection in E-commerce*, they could consider doing so.

10. Adapt legal frameworks to the realities of an increasingly digital and data-driven global economy and improve measurement

Digitalisation affects all corners of the economy and society, and it requires governments to reach across traditional policy silos and across different levels of government and develop a whole-of-government approach to policy making. This means more co-ordination when making decisions and conducting actions across government ministries and levels of government as well as actively involving all key stakeholders, including the business community, trade unions, civil society and Internet technical community, in the policy making process. To do so, comprehensive information about how the rapid rise of the digital economy has affected various legal and regulatory frameworks and policy areas such as competition, taxation, trade, the transfer of

data across borders, transportation, investment, labour markets, institutions, etc. is essential. For example, digitalisation is significantly impacting labour markets as well as tax policies, while other policy areas are just beginning to be affected.

The G20 can help elaborate a whole-of-economy approach to the policy implications of the digitalisation of the economy. A common framework for analysing digitalisation at the country level, building and expanding on a quantitative assessment of digitalisation, could be useful in this regard. Insights from a range of policy communities and from all stakeholders could help provide a whole-of-government view of digitalisation and how legal frameworks and other policies may need to adapt. Another specific action G20 economies could take is to agree to make a "digital impact assessment" a requirement for any new policy changes.

11. Co-ordinate and co-operate to better measure digitalisation across G20 economies

Sound measurement is the foundation on which good, evidence-based policy advice is based. Designing better policies for a digital economy and society requires further efforts to improve measurement and evidence, including on the spread of digital technologies themselves. Digitalisation also raises challenges for the measurement of growth and productivity. G20 economies can usefully work together to further develop cross-country comparable metrics in areas such as e-commerce and business use of sophisticated digital technologies (e.g. cloud computing and big data analytics, among others). New areas, such as trust and the IoT, are the next frontier. All countries need to work together to fill the data gaps and in doing so enabling better benchmarking, evidence building, policy development, and the identification and prioritisation of reforms, taking into account each G20 economy's level of development.

G20 economies can help build on the *G20 Data Gaps Initiative* by developing and agreeing to a set of specific actions to take to develop better cross-country comparable metrics on the digital economy. Priority areas could include e-commerce and more robust metrics on firm use of digital technologies, which can be accomplished by further implementing model surveys, among other means. Emerging areas, such as trust and the IoT, could also be explored.

REFERENCES

Abramovsky, L. and R. Griffith (2006), "Outsourcing and Offshoring of Business Services: How Important Is ICT?", *Journal of the European Economic Association,* Vol. 4, No. 2-3, pp. 594-601.

Acemoglu, D.et al. (2013), "Innovation, Reallocation and Growth", *NBER Working Papers*, No. 18993.

Aguilar, L. (2015), "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses", Public Statement, US Securities and Exchange Commission, www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html, accessed 30 November 2016.

Ahmad, N. and P. Schreyer (2016), "Measuring GDP in a Digitalised Economy", *OECD Statistics Working Papers*, 2016/07, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwqd81d09r-en.

Allianz (2015), "Allianz Risk Barometer 2015: Businesses exposed to increasing number of disruptive scenarios", Press Release, Allianz, www.agcs.allianz.com/about-us/news/press-riskbarometer2015/, accessed 30 November 2016.

Andrews, D., C. Criscuolo and P. Gal (2016), "The global productivity slowdown, technology divergence and public policy: A firm level perspective", *Hutchins Center Working Paper*, No. 24, Hutchins Center on Fiscal and Monetary Policy, The Brookings Institution, Washington, DC.

Arntz, M., T. Gregory and U. Zierahn (2016), "The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis", *OECD Social, Employment and Migration Working Papers*, No. 189, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlz99h56dvq7-en.

Atkinson, R. D. and A. S. McKay (2007), "Digital prosperity: understanding the economic benefits of the information technology revolution", https://ssrn.com/abstract=1004516.

Autor, D. H. (2015), "Why Are There Still So Many Jobs? The History and Future of Workplace Automation", *Journal of Economic Perspectives*, Vol. 29, No. 3, pp. 3-30.

Bakhshi, H., A. Bravo-Biosca, and J. Mateos-Garcia (2014), "Inside the datavores: Estimating the effect of data and online analytics on firm performance", Nesta, March, www.nesta.org.uk/sites/default/files/inside_the_datavores_technical_report.pdf.

Barua, A., D. Mani, R. Mukherjee (2013), "Impacts of effective data on business innovation and growth", Chapter Two of a three-part study, University of Texas at Austin, www.businesswire.com/news/home/20100927005388/en/Sybase-University-Texas-Study-Reveals-Incremental-Improvement, accessed 20 May 2015.

BCG (The Boston Consulting Group) (2015), "The Digital Imperative", BCG Perspectives, www.bcgperspectives.com/content/articles/digital_economy_technology_strategy_digital_imperative/?utm_source=2015April&utm_medium=Email&utm_campaign=Ealert, accessed 30 November 2016.

BCG (2012), "The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity", BCG, www.bcg.com/documents/file100409.pdf.

Bessen, J. (2015), *Learning by Doing: The Real Connection between Innovation, Wages, and Wealth*, Yale University Press, New Haven.

Blanchenay, P. et al. (forthcoming), "Cross-country Evidence on Business Dynamics Over the Last Decade: from Boom to Gloom?", *OECD Science, Technology and Industry Working Paper*, OECD Publishing, Paris.

Blind, K. and B. Kahin (forthcoming), "Standards and the Global Economy," in Jorge L. Contreras, ed., *Cambridge Handbook of Technical Standardization Law*, Cambridge University Press, Cambridge.

Bloom, N. et al. (2014), "The New Empirical Economics of Management", *NBER Working Papers*, No. 20 102.

Bloom, N., R. Sadun and J. Van Reenen (2016), "Management as a Technology", *NBER Working Papers*, No. 22 327.

Bloom, N., R. Sadun and J. Van Reenen (2012), "The Organization of Firms Across Countries," *Quarterly Journal of Economics*, 127: 1 663-705.

Bombardini, M., G. Gallipoli and G. Pupato (2012), "Skill Dispersion and Trade Flows", *American Economic Review,* Vol. 102, No. 5, pp. 2 327-48.

Bordonada, J., Lucia-Palacios, L. and Y. Polo-Redondo (2012), "The influence of organizational factors on e-business use: analysis of firm size", *Marketing, Intelligence and Planning*, Vol. 30, No. 2, pp. 212-229.

Bottazzi, G., A. Secchi and F. Tamagni (2014), "Financial constraints and firm dynamics", *Small Business Economics,* Vol. 42, No. 1, pp. 99-116.

Bresnahan, T. F. (1999), "Computerization and Wage Dispersion: An Analytic Reinterpretation", *Economic Journal*, June, 109:456, pp. 390-415.

Brynjolfsson, E. (1996), "The Contribution of Information Technology to Consumer Welfare", *Information Systems Research*, Vol. 7, No. 3, pp. 281-3.

Brynjolfsson, E. (1993), "The Productivity Para- dox of Information Technology", Communications of the ACM, Vol. 35, No. 12, pp. 66-77.

Brynjolfsson, E. and L. Hitt. (2000), "Computing Productivity: Are Computers Pulling Their Weight?", Mimeo, MIT and Wharton.

Brynjolfsson, E. and L. Hitt. (1997), "Breaking Boundaries", Informationweek, September, No. 22, pp. 54-61.

Brynjolfsson, E. and L. Hitt. (1996), "Paradox Lost? Firm-level Evidence on the Returns to Information Systems Spending", *Management Science*, Vol. 42, No. 4, pp. 541-58.

Brynjolfsson, E. and L. Hitt. (1995), "Information Technology as a Factor of Production: The Role of Differences Among Firms", *Economics of Innovation and New Technology*, Vol. 3, No. 4, pp. 183.

Brynjolfsson, E., L.M. Hitt and H.H. Kim (2011), "Strength in Numbers: How Does Data-Driven Decision making Affect Firm Performance?", Social Science Research Network (SSRN), 22 April, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.

Brynjolfsson, E. and A. McAfee (2011), *Race Against the Machine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy,* Digital Frontier Press, Lexington, Massachusetts.

Brynjolfsson, E.et al. (2008), "Scale Without Mass: Business Process Replication and Industry Dynamics, Harvard Business School Technology & Operations Mgt.", *Unit Research Paper*, No. 07-016.

Cabral, L. M. and J. Mata (2003), "On the evolution of the firm size distribution: Facts and theory", *The American Economic Review,* Vol. 93, No. 4, pp. 1 075-1 090.

Calvino, F., C. Criscuolo and C. Menon (2016), "No Country for Young Firms?: Start-up Dynamics and National Policies", *OECD Science, Technology and Industry Policy Papers*, No. 29, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jm22p40c8mw-en.

Chevrolet (2016), Chevrolet Lowers 4G LTE Data Pricing Up to 50 Percent, Chevrolet Media Pressroom, http://media.chevrolet.com/media/us/en/chevrolet/home.detail.html/content/Pages/news/us/en/2016/jun/0629-onstarData.html (accessed on 21 October).

CIDR (2016), *CIDR Report,* CIDR, *www.cidr-report.org/as2.0/*, accessed 1 December 2016.

Cisco (2016), "Visual Networking Index", Cisco, www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html, accessed 1 December 2016.

Citigroup-Oxford Martin School (2015), "Technology at Work: The Future of Innovation and Employment", www.oxfordmartin.ox.ac.uk/publications/view/1883, accessed 30 November 2016.

Clark, D. et al. (2014), "Measurement and Analysis of Internet Interconnection and Congestion", Center for Applied Internet Data Analysis, www.caida.org/publications/papers/2014/measurement_analysis_internet_interconnection/, accessed 1 December 2016.

CMA (United Kingdom Consumer Market Authority) (2015), "The commercial use of consumer data: Report on the CMA's call for information", CMA 38, June.

Colecchia, A. and P. Schreyer (2002), "The Contribution of Information and Communication Technologies to Economic Growth in Nine OECD Countries", *OECD Economic Studies*, Vol. 2002/1, pp. 153-171, OECD Publishing, Paris, http://dx.doi.org/10.1787/eco_studies-v2002-art5-en.

Computing Community Consortium/Computing Research Association (CCC/CRA) (2009), "From Internet to Robotics: A Roadmap for US Robotics", http://www.us-robotics.us/reports/CCC%20Report.pdf, accessed 6 December 2016.

Consoli, D. (2012), "Literature analysis on determinant factors and the impact of ICT in SMEs", *Social and Behavioural Sciences*, Vol. 62, pp. 93-97.

Daugherty, P. et al. (2015), *Driving Unconventional Growth through the Industrial Internet of Things*, Accenture Technology, https://www.accenture.com/us-en/labs-insight-industrial-internet-of-things.

Daveri, F. (2002), "The New Economy in Europe 1992-2001", Discussion Paper No. 70, WIDER, United Nation University.

Decker, R. et al. (2016a), "Declining Business Dynamism: What We Know and the Way Forward", *American Economic Review*, 106(5), pp. 203-07.

Deloitte (2015), "Connected Health – How Digital Economy is Transforming Health and Social Care", Deloitte Centre for Health Solutions, www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf.

DeNardis, L. (2011), "Opening Standards: The Global Politics of Interoperability", Massachusetts Institute of Technology, Cambridge, Massachusetts.

ENISA (European Union Agency for Network and Information Security) (2014), "An evaluation framework for national cyber security strategies", ENISA, http://dx.doi.org/10.2824/3903.

European Commission (2016), 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.

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

European Commission (2015b), "A Digital Single Market Strategy for Europe – Analysis and Evidence", https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-analysis-and-evidence-swd2015-100-final.

European Commission (2015c), "Consumer Conditions Scoreboard, Consumers at Home in the Single Market", 2015 Edition, http://ec.europa.eu/consumers/consumer_evidence/consumer_scoreboards/11_edition/docs/ccs2015scoreboard_en.pdf.

European Commission (2014), *European Vacancy Monitor*, Issue No. 12, February, http://ec.europa.eu/social/BlobServlet?docId=11426&langId=en.

Eurostat (2015), "ICT security in enterprises", http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises.

Evans, P. C. and M. Anninziata (2012), "Industrial Internet: Pushing the Boundaries of Minds and Machines", General Electrics, www.ge.com/docs/chapters/Industrial_Internet.pdf.

Frey, C. B. and M. A. Osborne (2013), "The Future of Employment: How Susceptible are Jobs to Computerisation?", Oxford Martin School Working Paper.

G20/OECD (2016), G20/OECD High-level Principles on SME Finance, https://www.oecd.org/finance/G20-OECD-High-Level-%20Principles-on-SME-Financing.pdf, accessed 6 December 2016.

Gal, P. (2013), "Measuring Total Factor Productivity at the Firm Level using OECD-ORBIS", *OECD Economics Department Working Papers*, No. 1 049, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k46dsb25ls6-en.

German Federal Ministry of Economic Affairs and Energy (2015), "Erschließen der Potenziale der Anwendung von 'Industrie 4.0' im Mittelstand", BMWi, www.bmwi.de/DE/Mediathek/publikationen,did=716886.html, accessed 1December 2016.

Google (2016), "Google IPv6 Statistics", Google, www.google.com/intl/en/ipv6/statistics.html, accessed 1 December 2016.

Goos, M., J. Konings and M. Vandeweyer (2015), "Employment Growth in Europe: The Roles of Innovation, Local Job Multipliers and Institutions", *Utrecht School of Economics Discussion Paper Series*, Vol. 15, No. 10.

Gordon, R. J. (2004), "Five puzzles in the Behavior of Productivity, Investment, and Innovation", Working Paper No. w10 660, National Bureau of Economic Research, www.nber.org/papers/w10660.pdf.

Hartmann, E. and M. Bovenschulte (2013), "Skills Needs Analysis for 'Industry 4.0' based on Roadmaps for Smart Systems", in SKOLKOVO Moscow School of Management & International Labour Organization (ed.), *Using Technology Foresights for Identifying Future Skills Needs*, Global Workshop Proceedings, Moscow, pp. 24-36.

Helberger, N., K. Kleinen-von Königslöw and R. van der Noll (2015), "Regulating the new information intermediaries as gatekeepers of information diversity", *Info*, Vol. 17, No. 6, pp. 50-71, https://ssrn.com/abstract=2728718.

Hepp, P. et al. (2004), "Technology in Schools: Education, ICT and the Knowledge Society", World Bank, http://siteresources.worldbank.org/EDUCATION/Resources/278200-1099079877269/547664-1099079947580/ICT_report_oct04a.pdf.

Hornuf, L. and A. Schwienbacher (2014), "The Emergence of Crowdinvesting in Europe", Munch Discussion Paper No. 2 014-43.

Hufbauer, G., B. Kotschwar and J. Wilson (2001), "Trade Policy, Standards, and Development in Central America", World Bank Policy Research Working Paper Series, https://ssrn.com/abstract=927867.

Internet Society (2015a), "The Internet of Things: An Overview", www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf.

Internet Society (2015b), "Collaborative Security: An Approach to Tackling Internet Security Issues", www.internetsociety.org/collaborativesecurity, accessed 2 December 2016.

ITU (International Telecommunication Union) (2015), *ITC Facts and Figures 2015*, www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

Jhurree, V. (2005), "Technology Integration in Education in Developing Countries: Guidelines to Policy Makers", *International Education Journal*, Vol.6 No. 4, pp. 467-483, http://ehlt.flinders.edu.au/education/iej/articles/v6n4/jhurree/paper.pdf.

JRC (Joint Research Centre) (2016), "The Digital Competence Framework for Consumers", JRC, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/jrc103155.pdf.

Jorgenson, D. W. (2003), "Information Technology and the G7 Economies", *World Economics*, Vol. 4, No. 4, pp. 139-169.

Jorgenson, D. W. (2001), "IT and the U.S. Economy", *American Economic Review*, March 2001, Vol. 91, No. 1, pp. 1-32.

Jorgenson, D. W. and K. J. Stiroh (2000), "US Economic Growth at the Industry Level", *The American Economic Review*, Vol. 90, No. 2, pp. 161-167.

Kaiser, M. (2011), "Prepared testimony of the National Cyber Security Alliance on the State of Cybersecurity and Small Business before the Committee on House Small Business Subcommittee on Healthcare and Technology", United States House of Representatives, 1 December, http://smallbusiness.house.gov/uploadedfiles/kaiser_testimony.pdf.

Karachalios, K. and K. McCabe (2016), "Dual Use of Standardization Strategies: Promoting Regional Integration and/or Global Markets", Working Paper, East-West Center Workshop on Mega-Regionalism – New Challenges for Trade and Innovation, http://ssrn.com/abstract=2745492, accessed 2 December 2016.

Kerr, W. and R. Nanda (2009), "Financing constraints and entrepreneurship", NBER Working Paper No. 15 498, National Bureau of Economic Research.

Koske, I. et al. (2015), "The 2013 Update of the OECD Product Market Regulation Indicators: Policy Insights for OECD and non-OECD Countries", *OECD Economics Department Working Papers*, No. 1 200, OECD Publishing, Paris, http://dx.doi.org/10.1787/5js3f5d3n2vl-en.

Leeuw, F.L. and B. Leeuw (2012), "Cyber society and digital policies: Challenges to evaluation?", *Evaluation*, Vol. 18, No. 1, pp. 111-127.

Lorentz, M. et al. (2015), "Man and Machine in Industry 4.0: How Will Technology Transform the industrial Workforce Through 2025?", The Boston Consulting Group, www.bcgperspectives.com/content/articles/technology-business-transformation-engineered-products-infrastructure-man-machine-industry-4/, accessed 1 December 2016.

Loshin, D. (2002), "Knowledge Integrity: Data Ownership", 8 June, http://datawarehouse.com/article/?articleid=3052.

Loveman, Gary W. (1994), "An Assessment of the Productivity Impact of Information Technologies," in Allen, Thomas J. and Scott Morton, Michael S. (ed.), *Information Technology and the Corporation of the 1990s*, Research Studies, Oxford University Press, pp. 84-110.

Marcolin, L., M. Le Mouel and M. Squicciarini (forthcoming), "Investment in Knowledge-Based Capital and Backward Linkages in Global Value Chains", *OECD Science, Technology and Industry Working Papers*, OECD Publishing, Paris.

MarketsandMarkets (2015), "Global Wi-Fi Market – Global Forecast to 2020", www.marketsandmarkets.com/Market-Reports/global-wi-fi-market-994.html?gclid=COD4rNjxzNACFY9XDQodvl4IIA, accessed 2 December 2016.

McKinsey Global Institute (2015), "The Internet of Things: Mapping the Value Beyond the Hype", www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world, accessed 2 December 2016.

Meeker, M. (2015), "Internet Trends", www.kpcb.com/blog/2015-internet-trends.

Michaels, G., A. Natraj and J. Van Reenen (2014), "Has ICT polarised skill demand? Evidence from eleven countries over twenty-five years", *Review of Economics and Statistics*, Vol. 96, No. 1, pp. 60-77.

Moretti, E. (2010), "Local Multipliers", *American Economic Review*, Papers and Proceedings, No. 100, pp. 1-7.

Murdock, P. et al. (2016), "Semantic Interoperability for the Web of Things", http://dx.doi.org/10.13140/RG.2.2.25758.13122, accessed 2 December 2016.

National Research Council (2012), *Education for life and work: developing transferable knowledge and skills in the 21st century,* National Academies Press, Washington, DC, https://doi.org/10.17226/13398.

OECD (forthcoming a), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris.

OECD (forthcoming b), "Determinants and Impact of Automation: An Analysis of Robots' Adoption in OECD Countries", *OECD Science, Technology and Industry Working Papers*, OECD Publishing, Paris.

OECD (forthcoming c), "Having the Right Mix: The Role of Skill Bundles for Comparative Advantage and Industry Performance in GVCs", *OECD Science, Technology and Industry Working Papers*, OECD Publishing, Paris.

OECD (forthcoming d), "Use of Behavioural Insights in Consumer Policy", OECD, Paris.

OECD (forthcoming e), *Financing SMEs and entrepreneurs 2017. An OECD Scoreboard*, OECD Publishing, Paris.

OECD (forthcoming f), "Benchmarking policies for stronger SME performance, Working Party on SMEs and Entrepreneurship", OECD, Paris.

OECD (2016a), "Enabling the Next Production Revolution; The Future of Manufacturing and Services", Interim Report, Meeting of the OECD Council at Ministerial Level, 1-2 June 2016, Paris, www.oecd.org/mcm/documents/Enabling-the-next-production-revolution-the-future-of-manufacturing-and-services-interim-report.pdf.

OECD (2016b), *The Productivity-Inclusiveness Nexus*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264258303-en.

OECD (2016c), "Managing Digital Security and Privacy Risk", *OECD Digital Economy Papers*, No. 254, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwt49ccklt-en.

OECD (2016d), "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 (2016e), *Innovating Education and Educating for Innovation: The Power of Digital Technologies and Skills*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264265097-en.

OECD (2016f), "Economic and Social Benefits of Internet Openness", *Digital Economy Papers*, No. 257, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwqf2r97g5-en.

OECD (2016g), "Maximising the Economic and Social Value of Data: Understanding the Benefits and Challenges of Enhanced Data Access", internal document, OECD, Paris.

OECD (2016h), "Managing Digital Security and Privacy Risk", *OECD Digital Economy Papers,* No. 254, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwt49ccklt-en

OECD (2016i), "National Skills Strategies", OECD, Paris, www.oecd.org/skills/nationalskillsstrategies/buildingeffectiveskillsstrategiesatnationalandlocallevels.htm, accessed 30 November 2016.

OECD (2016j), "Cancun Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity", OECD, Paris, www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf.

OECD (2016k), "Skills for a Digital World", 2016 Ministerial Meeting on the Digital Economy Background Report, *OECD Digital Economy Papers*, No. 250, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwz83z3wnw-en.

OECD (2016l), *Recommendation of the Council on Consumer Protection for E-commerce*, OECD, Paris, www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf.

OECD (2016m), "The Internet of Things Seizing the Benefits and Addressing the Challenges", *OECD Digital Economy Papers*, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwvzz8td0n-en.

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

OECD (2016o), "New Forms of Work in the Digital Economy", *OECD Digital Economy Papers*, No. 260, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwnklt820x-en.

OECD (2016p), "No Country for Young Firms?", Policy Note, OECD Directorate for Science, Technology and Innovation, June, https://www.oecd.org/sti/ind/Policy-Note-No-Country-For-Young-Firms.pdf.

OECD (2016q), "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 (2016r), *Financing SMEs and entrepreneurs 2016. An OECD Scoreboard*, OECD Publishing, Paris.

OECD (2015a), *The Future of Productivity*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264248533-en.

OECD (2015b), "ICTs and Jobs: Complements or Substitutes? The Effects of ICT Investment on Labour Market Demand by Skills and by Industry in Selected Countries", *OECD Digital Economy Working Papers*, No. 259, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwnklzplhg-en.

OECD (2015c), "ICTS, Jobs and Skills. New Evidence from the OECD PIAAC Survey", internal document, OECD, Paris.

OECD (2015d), *OECD Science, Technology and Industry Scoreboard 2015*, OECD Publishing, Paris, http://dx.doi.org/10.1787/sti_scoreboard-2015-en.

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

OECD (2015f), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264229358-en.

OECD (2015g), *The Innovation Imperative, Contributing to Productivity, Growth and Well-Being*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264239814-en.

OECD (2015h), "Crowdfunding for SMEs", Chapter 4 in *New Approaches to SME and Entrepreneurship Financing*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264240957-en.

OECD (2015i), "G20/OECD High-Level Principles on SME Financing", G20/OECD, www.oecd.org/finance/G20-OECD-High-Level-%20Principles-on-SME-Financing.pdf.

OECD (2015j), "OECD Innovation Strategy 2015. An Agenda for Policy Action", OECD, Paris, www.oecd.org/sti/OECD-Innovation-Strategy-2015-CMIN2015-7.pdf.

OECD (2015k), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264245471-en.

OECD (2015l), *Skills for social progress: the power of social and emotional skills*, *OECD skills studies*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264226159-en.

OECD (2015m), *In It Together: Why Less Inequality Benefits All*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264235120-en.

OECD (2015n), *New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments*, OECD Publishing, Paris.

OECD (2014a), "Trends Shaping Education 2014; Spotlight 5", OECD, Paris, www.oecd.org/edu/ceri/Spotlight%205-%20Infinite%20Connections.pdf.

OECD (2014b), *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264221796-en.

OECD (2014c), "Services Trade Restrictiveness Index: Policy Brief", OECD, Paris.

OECD (2014d), "Connected televisions: Convergence and emerging business models", *OECD Digital Economy Papers*, No. 231, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jzb36wjqkvg-en.

OECD (2014e), "Small businesses, job creation and growth: Facts, obstacles and best practices", OECD, Paris, www.oecd.org/cfe/smes/2090740.pdf.

OECD (2014f), "Recommendation of the Council on Digital Government Strategies", OECD, Paris, www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf.

OECD (2014g), *Forecasting Future Needs for Advanced ICT Competence in Norway*, internal document, OECD, Paris.

OECD (2013a), *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264193307-en.

OECD (2013b), *OECD Skills Outlook 2013: First Results from the Survey of Adult Skills*, OECD Paris, Paris, http://dx.doi.org/10.1787/9789264204256-en.

OECD (2013c), "New data for understanding the human condition: International perspectives", OECD Global Science Forum Report on Data and Research Infrastructure for the Social Sciences, February, OECD, Paris, www.oecd.org/sti/sci-tech/new-data-for-understanding-the-human-condition.pdf.

OECD (2013d), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OECD (2013e), "The Role and Measurement of Quality in Competition Analysis," Background Note for OECD Policy Roundtables, www.oecd.org/daf/competition/Quality-in-competition-analysis-2013.pdf.

OECD (2012a), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", *OECD Digital Economy Papers*, No. 214, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k4dq3rkb19n-en.

OECD (2012b), "Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, Paris, 10.1787/5k8zq92vdgtl-en.

OECD (2012c), *Literacy, Numeracy and Problem Solving in Technology-Rich Environments: Framework for the OECD Survey of Adult Skills*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264128859-en.

OECD (2012d), *Connected Minds: Technology and Today's Learners, Educational Research and Innovation*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264111011-en.

OECD (2011a), *Divided We Stand: Why Inequality Keeps Rising*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264119536-en.

OECD (2011b), "Digital Identity Management: Enabling Innovation and Trust in the Internet Economy", OECD, Paris, www.oecd.org/sti/ieconomy/49338380.pdf.

OECD (2011c), "The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines", Chapter 4 in *The OECD Privacy Framework*, OECD, Paris, www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD (2010a), *SMEs, Entrepreneurship and Innovation*, OECD, Paris, DOI: http://dx.doi.org/10.1787/9789264080355-en.

OECD (2010b), *Inspired by Technology, Driven by Pedagogy: A Systemic Approach to Technology-Based School Innovations*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264094437-en.

OECD (2009), *Top Barriers and Drivers to SME Internationalisation*, Report by the OECD Working Party on SMEs and Entrepreneurship, OECD, Paris, www.oecd.org/cfe/smes/43357832.pdf.

OECD (2008a), *Recommendation of the Council on the Protection of Critical Information Infrastructures*, OECD, Paris, www.oecd.org/sti/40825404.pdf.

OECD (2008b), *Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information*, OECD, Paris, www.oecd.org/internet/ieconomy/40826024.pdf.

OECD (2007), "Information Economy – Sector Definition Based on the International Standard Industry Classification (ISIC 4)", OECD, Paris, www.oecd.org/sti/sci-tech/38217340.pdf.

OECD (2006), *The SME Financing Gap*, OECD Publishing, Paris.

OECD (2004), *The Economic Impacts of ICT – Measurement, Evidence and Implications*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264026780-en.

OECD and World Bank (2015), "Inclusive global value chains: Policy options in trade and complementary areas for GVC integration by small and medium enterprises and low-income developing countries", OECD and World Bank Group Publishing.

Ohnsorge, F. and D. Trefler (2007), "Sorting It Out: International Trade with Heterogeneous Workers", *Journal of Political Economy*, No. 115, Vol. 5, pp. 868-92.

Oliner, Stephen D., and Daniel E. Sichel (2000), "The Resurgence of Growth in the Late 1990s: Is Information Technology the Story?", *Journal of Economic Perspectives*, Vol. 14, No. 4, pp. 3-22.

Orrick (2012), "The big data report", Orrick, www.cbinsights.com/big-data-report-orrick, accessed 2 December 2016.

Otto, B. et al. (2016), "Industrial Data Space: Digital Sovereignty over Data", White Paper, Frauenhofer, www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf.

Packet Clearing House (2016), *Internet Exchange Directory,* Packet Clearing House, www.pch.net/ixp/dir, accessed 16 November 2016.

Pantea, S. and B. Martens (2014), "The Value of the Internet for Consumers", JRC Technical Reports, European Commission, http://dx.doi.org/10.2139/ssrn.2446962.

Pilat, D. (2005), "The ICT Productivity Paradox: Insights from Micro Data", *OECD Economic Studies*, Vol. 2004 No. 1, pp. 37-65, OECD Publishing, Paris, http://dx.doi.org/10.1787/eco_studies-v2004-art3-en.

Pilat, D. and A. Nolan (2016), "Benefiting from the next production revolution", in Patrick Love (ed.), *Debate the Issues: New Approaches to Economic Challenges*, OECD Publishing, Paris, pp. 117-121, http://dx.doi.org/10.1787/9789264264687-22-en.

Platform Industry 4.0 (2016), "The fourth industrial revolution: Towards intelligent and flexible production", Federal Ministry of Education and Research, www.plattform-i40.de/I40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html, accessed 25 November 2016.

PwC (2016),"Global Industry 4.0 Survey: Building the digital enterprise", PwC, www.pwc.com/gx/en/industries/industrial-manufacturing/publications/assets/pwc-building-digital-enterprise.pdf.

Rigby, M. (2015), "Future-proofing UK manufacturing: Current investment trends and future opportunities in robotic automation", Barclays, www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/research/automation-report.pdf.

Rüsmann, M. et al. (2015), "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries", The Boston Consulting Group. www.bcgperspectives.com/content/articles/engineered_products_project_business_industry_40_future_productivity_growth_manufacturing_industries/, accessed 1 December 2016.

Sabatini, J. (2016), "SF begins crunching numbers on citywide internet access", 24 October, *www.sfexaminer.com/sf-begins-crunching-numbers-citywide-internet-access/*, accessed 1 December 2016.

Schoechle, T. (2009), "Standardization and Digital Enclosure: The Privatization of Standards, Knowledge and Policy in the Age of Global Information Technology", Information Science Reference (an imprint of IGI Global), Hershey, Pennsylvania.

Schreyer, P. (2000), "The Contribution of Information and Communication Technology to Output Growth: A Study of the G7 Countries", *OECD Science, Technology and Industry Working Papers*, 2000/02, OECD Publishing, Paris, http://dx.doi.org/10.1787/151634666253.

Smit, J. et al. (2016), *Industry 4.0*, European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, February.

Strassmann, P. A. (1985), "Information Payoff: The Transformation of Work in the Electronic Age", Free Press, New York, NY.

Sullivan, G. P. et al. (2010), "Operations & Maintenance Best Practices: A Guide to Achieving Operational Efficiency, Release 3.0," *Pacific Northwest National Laboratory*, US Department of Energy, August.

Symantec (2016), "Internet Security Threat Report", Vol. 21, April 2016, www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

The Economist Intelligence Unit (2013), "Information Risk. Managing digital assets in a new technology landscape", www.eiuperspectives.economist.com/technology-innovation/information-risk, accessed 30 November 2016.

TNO (2015), "Digital platforms: an analytical framework for identifying and evaluating policy options", https://english.eu2016.nl/documents/publications/2016/04/18/digital-platforms.

Tompson, P. et al. (2011), "SME Characteristics and the Use of the Internet to Expand the Scale and Geographic Scope of Sales: Evidence from the United Kingdom", in Sharma, S. K. (ed.) , *E-Adoption and Socio-Economic Impacts. Emerging Infrastructural Effects*, IGI Global, Hershey, Pennsylvania.

Turk, M. (2016), "Is Big Data Still a Thing? (The 2016 Big Data Landscape)", http://mattturck.com/2016/02/01/big-data-landscape, accessed 2 December 2016.

Tüzemen, D. and J. Willis (2013), "The Vanishing Middle: Job Polarization and Workers' Response to the Decline in Middle-Skill Jobs", Kansas City Federal Reserve Bank, www.kansascityfed.org/publicat/econrev/pdf/13q1tuzemen-willis.pdf.

UNCTAD (2016), "UNCATD B2C E-commerce Index 2016", UNCTAD, http://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d07_en.pdf.

UNCTAD (2015), "Information Economy Report 2015", UNCTAD, http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf.

UNGA (United Nations General Assembly) (2015), "United Nations Guidelines for Consumer Protection", A/C.2/70/3, para 5(e), Resolution 70/186 of 22 December.

United States Department of Commerce (2016), "Quarterly Retail E-commerce Sales, 2nd Quarter 2016", United States Department of Commerce, www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

US NTIA (United States National Telecommunications & Information Administration) (2016), "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities", www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities, accessed 2 December 2016.

Van Ark, B. et al. (2002), "ICT Investment and Growth Accounts for the European Union, 1980-2000", Final Report on ICT and Growth Accounting for the DG Economics and Finance of the European Commission, Brussels.

Van Ark, B., R. Inklaar and R. McGuckin (2003), "Changing Gear: Productivity, ICT, and Services Industries: Europe and the United States", in Christensen and Maskell (eds.), *The Industrial Dynamics of the New Digital Economy*, Edward Elgar Publishing, Cheltenham, United Kingdom.

Van Reenen, J. et al. (2010), "The Economic Impact of ICT", Research report, Enterprise LSE, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.180.3621&rep=rep1&type=pdf.

WEF (World Economic Forum) (2015a), "Global Risks 2015; 10th Edition", WEF, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

WEF (2015b), "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services", http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

Weller, D. and B. Woodcock (2013), "Internet Traffic Exchange: Market Developments and Policy Challenges", *OECD Digital Economy Papers*, No. 207, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k918gpt130q-en.

Wilson, K. and F. Silva (2013), "Policies for Seed and Early Stage Finance: Findings from the 2012 OECD Financing Questionnaire", *OECD Science, Technology and Industry Policy Papers*, No. 9, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k3xqsf00j33-en.

World Bank (2016), *World Development Report 2016: Digital Dividends*, World Bank, Washington, DC, http://dx.doi.org/10.1596/978-1-4648-0671-1.

Yusuf, M.O. (2005), "Information and communication education: Analyzing the Nigerian national policy for information technology", *International Education Journal*, Vol. 6, No. 3, pp. 316-321.

NOTES

1. Chapter 2 discusses policies for addressing the barriers to deploying high-quality broadband infrastructure in more detail, including issues related to infrastructure for the IoT.
2. Backhaul facilities are the intermediate links that transport traffic to the core of a network, after which it is further distributed through a hierarchical structure on that network or to others around the world (i.e. over larger backbone networks).
3. Data Over Cable Service Interface Specification (DOCSIS) is an international telecommunications standard that permits the addition of high-bandwidth data transfer to an existing cable television system.
4. ETSI has also a direct representation mode.
5. This approach is rooted in five key elements: fostering confidence and protecting opportunities**;** collective responsibility**;** fundamental properties and values**;** evolution and consensus; and think globally, act locally.
6. “Semantic interoperability is achieved when interacting systems attribute the same meaning to an exchanged piece of data, ensuring consistency of the data across systems regardless of individual data format” (Murdock, 2016).
7. In this section, the expression “data protection” refers to the protection of personal data. However, some technical experts also use it sometimes as a synonym for “digital security” or “information security”.
8. "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data" (OECD, 2013d).
9. This work contains statistical data from ONS which is Crown Copyright. The use of the ONS statistical data in this work does not imply the endorsement of the ONS in relation to the interpretation or analysis of the statistical data. This work uses research datasets which may not exactly reproduce National Statistics aggregates.
10. In order to assess whether disparities are present between firm size and age for other types of advanced software, this chapter also exploits an ICT specific panel dataset known as the CiTDB. This dataset surveys larger firms and is composed of plant level information of either a stand-alone firms with 100 or more employees, or a plant with less than 100 employees connected to a multi-plant firm. Any plant-level adoption gap identified here is therefore likely to be a lower bound compared to a representative sample of plants, since the dataset is comprised of older more established firms.
11. This suggests that the results are robust to possible mismeasurement of firm entry in business registers due to legal changes in firm names and status or mergers and acquisition activities.
12. The toolkit is available in 17 languages and can be downloaded at www.oecd.org/daf/competition/assessment-toolkit.htm.

www.oecd.org/innovation

www.oecd.org/ieconomy

http://oe.cd/depseries


@OECDInnovation

STI.contact@oecd.org