Chapter 2
INVESTING IN SMART INFRASTRUCTURE

2.1 Broadband penetration

Key findings

Broadband communication networks and the services provided over them support existing economic and social activities and hold potential for tremendous innovation.

Broadband diffusion remains uneven across OECD economies but continues to increase everywhere. Progress has been particularly swift in mobile (terrestrial wireless) broadband. Since the end of 2009 the rate of mobile wireless broadband penetration has more than doubled for the OECD area, reaching 72% in December 2013.

Penetration rates reached over 100% in Australia, Denmark, Finland, Japan, Korea and Sweden and the United States. Australia edged into the second place after a 13% surge in smartphone subscriptions in the first half of 2013. Mobile wireless broadband penetration stood at 32% or less in Hungary, Mexico and Turkey, but progress to date and the universal diffusion of standard mobile subscriptions indicate strong potential for catch-up by lagging economies.

Fixed (wired) broadband subscriptions in the OECD area reached 339 million as of December 2013, giving an average penetration rate of 27%, up from 23% at the end of 2009.

Take-up for fixed broadband has increased at a slower pace than for mobile, and in some countries this latter has been substituting fixed broadband rather than complementing it. The general trend, however, indicates significant improvement in available technologies.

Deploying fibre closer to the home has been an on-going process in all OECD countries for many years. More recently, network operators have started to evaluate whether to bring fibre directly to a premise or to a nearby point and use existing or upgraded DSL and cable infrastructure. The majority of fixed wired broadband connections are currently provided over DSL (51%) and cable modem (31%) technologies. In December 2013, the share of direct fibre connections in the OECD area was 17%, up from 11% in December 2009.

Two-digit growth in fibre over the December 2012-13 period was sustained by increases in large OECD economies with low penetration levels, such as France (73%), Spain (84%), Turkey (85%) and the United Kingdom (116%). Japan and Korea remain the OECD leaders, with fibre making up 70% and 65% of fixed broadband connections.

DID YOU KNOW?

In December 2013, almost 3 out of 4 OECD inhabitants had a mobile wireless broadband subscription.

Definitions

Broadband penetration indicators comprise the number of subscriptions to fixed wired and mobile wireless broadband services, divided by the number of residents in each country.

Fixed (wired) broadband includes DSL, cable, fibre to the home (FTTH) and other fixed wired technologies.

Mobile wireless broadband includes satellite, terrestrial fixed wireless and terrestrial mobile wireless (standard mobile and dedicated data).

All components include only connections with advertised data speeds of 256kbit/s or more.

A standard mobile subscription is counted as an active broadband subscription only when it allows for full access to the Internet via HTTP (subscriptions that only offer walled gardens or email access are not counted) and when content or services were accessed using the Internet Protocol (IP) during the previous three months.

All active mobile subscriptions are counted. Hence, penetration rates can be over 100%. For fixed subscriptions saturation is reached at much lower rates, as these typically consist of one per household.

Measurability

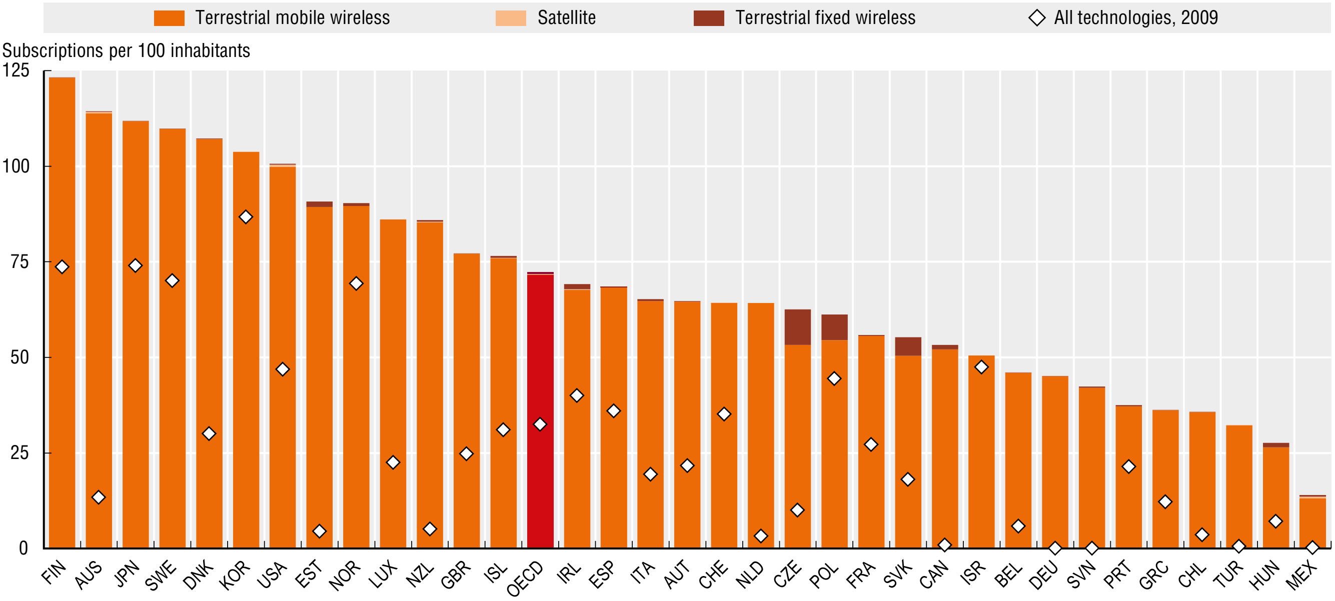
Fixed (wired) and mobile wireless broadband subscriptions for OECD countries are collected according to agreed definitions and are highly comparable.

Data for wireless broadband subscriptions improved greatly in recent years, especially with regard to measurement of standard mobile and dedicated mobile data subscriptions.

In the case of standard mobile subscriptions, these need to be active during the last three months before the date of measurement, which can pose difficulties. Data respecting these standards are now available for most OECD countries.

Mobile wireless broadband penetration, by technology, December 2009 and 2013

Subscriptions per 100 inhabitants

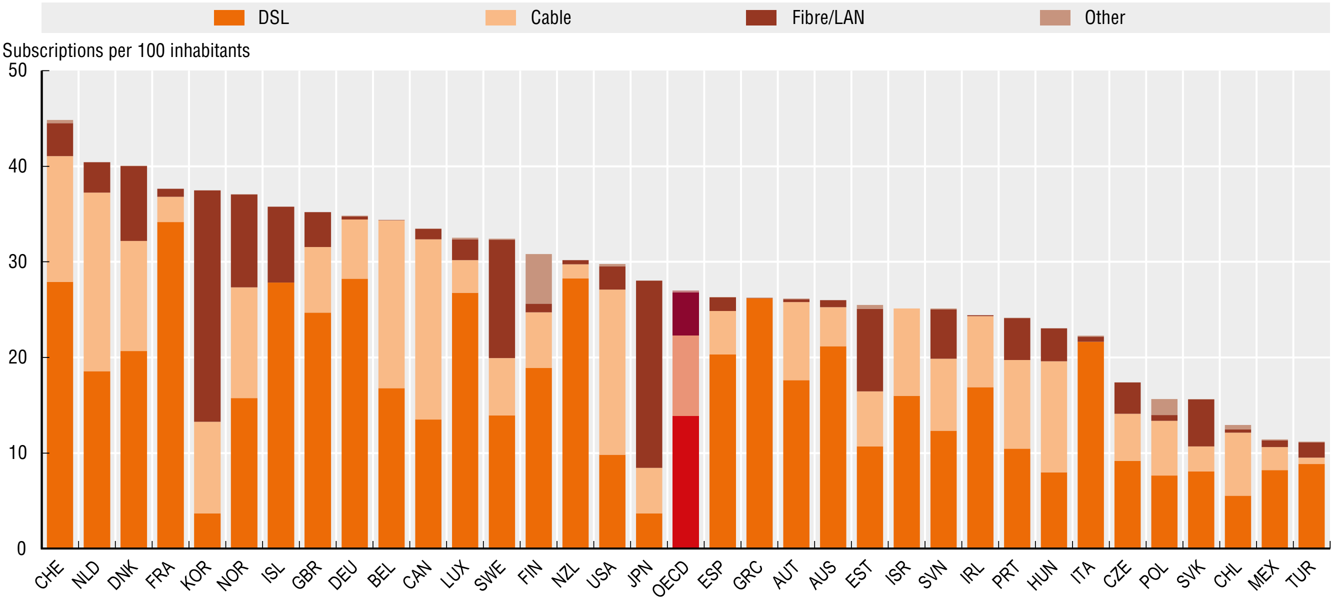


Source: OECD, Broadband Portal, www.oecd.org/sti/broadband/oecdbroadbandportal.htm, July 2014.

StatLink http://dx.doi.org/10.1787/888933147973

Fixed (wired) broadband penetration by technology, December 2013

Subscriptions per 100 inhabitants



Source: OECD, Broadband Portal, www.oecd.org/sti/broadband/oecdbroadbandportal.htm, July 2014.

StatLink http://dx.doi.org/10.1787/888933147981

Key findings

The popularity of smartphones has stimulated greater use of mobile Internet. The average subscription rate of mobile Internet access in OECD countries rose to 72.4 per 100 inhabitants in December 2013, up from just 32.4 in December 2009.

Mobile broadband subscriptions represent 73% (910 million) of all broadband access paths in the OECD. Broadband mobile penetration was highest in Australia, Finland and Japan and lowest in Hungary, Mexico and Turkey.

In calculating the number of mobile connections it is important to factor in users that have more than one subscription. Some people use multiple SIM cards to take advantage of different tariffs or for different uses, for example, a mobile handset with a separate dedicated mobile data connection, such as a mobile broadband dongle, data card or data-only SIM.

While a large majority of mobile broadband subscriptions in the OECD include a voice connection, an increasing number are now dedicated data connections with subscribers using a mobile device primarily to access the Internet (although telephony is still possible via a VoIP application). In December 2013, about 128 million mobile subscriptions were dedicated data, almost double that of December 2009.

SIM cards for machine-to-machine (M2M) usage account for a growing segment of mobile data subscriptions. These are dedicated exclusively to communication between equipment at a distance and are not intended for interpersonal communications. Some of the functionality of M2M communications is built into navigation services for automobiles, access to the Internet and emergency communications, among others. These devices connect millions of sensors and actuators, providing ever-greater amounts of "big data" to facilitate the monitoring of machines, environments and people's health.

Some telecommunication operators now have specific offers for M2M data services, which are used for e-book readers, vehicles and smart meters. OECD countries are examining or have started to liberalise access to SIM cards for M2M applications independent of mobile operators. This allows users to switch mobile operators or use multiple networks at the same time. The Netherlands is the first country to change regulation in this area. In 2012, there were 35.8 million M2M SIM cards in the 18 OECD countries for which data are available. Sweden is an outlier for M2M penetration with 511 M2M SIM cards per 1000 inhabitants. Finland, Denmark, Italy and France follow with over 100 M2M SIM cards per 1000 inhabitants.

DID YOU KNOW?

In 2012, there were more than 35 million SIM cards for machine-to-machine communication in the 18 OECD countries for which data are available.

Definitions

Mobile broadband connections are used together with a voice connection (standard subscriptions) or are dedicated to mobile broadband services exclusively (dedicated subscriptions).

Subscriptions to dedicated data services over a mobile network are purchased separately from voice services, either as a stand-alone service (modem/dongle) or as an add-on data package to voice services, which requires an additional subscription. All dedicated mobile data subscriptions with recurring subscription fees are included as "active data subscriptions", regardless of actual use. Prepaid mobile broadband plans require active use if there is no monthly subscription.

A segment of *M2M communication* relies on mobile wireless networks and, as with mobile telephony, is based on the use of SIM cards for authentication and telephone numbers for connectivity. SIM card numbers and telephone numbers are obtained from regulators who, as of recently, require that mobile operators use different telephone number ranges for M2M.

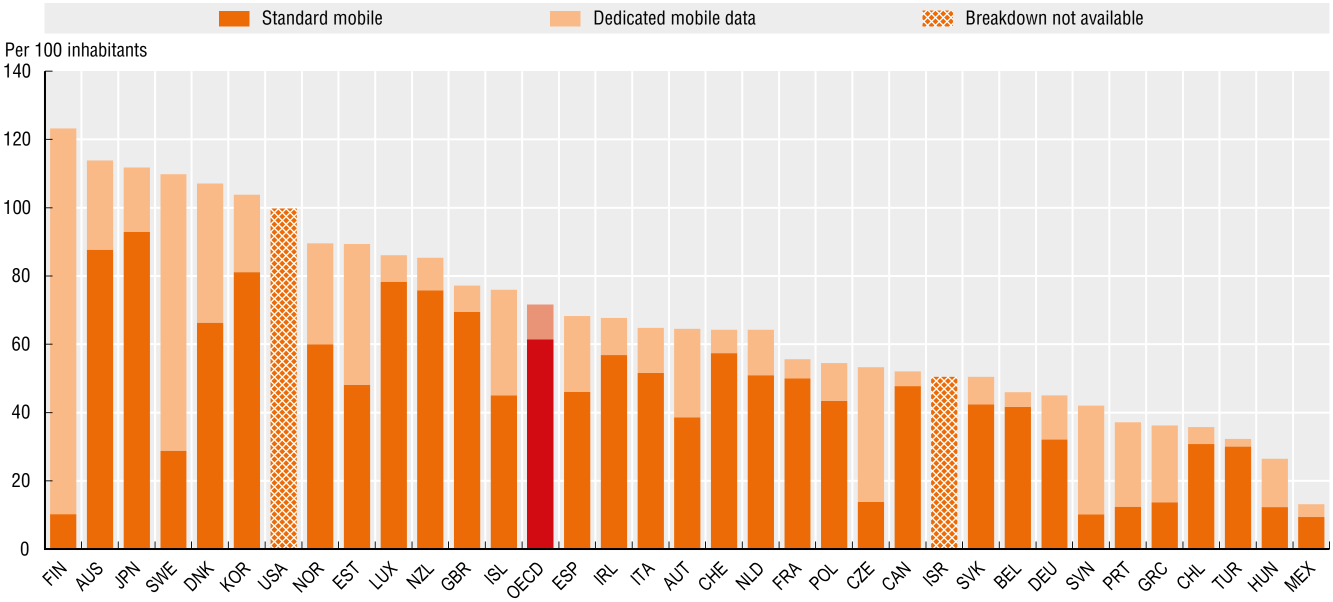
Measurability

International comparability of mobile communications statistics is limited by the fact that not all countries are able to comply with the same definitions. For example, the number of standard mobile subscriptions should include only subscriptions in use over the previous three months; however, not all countries are able to provide this information.

In addition, coverage of dedicated data mobile statistics tends to vary across countries, which may contribute to explaining the very high penetration rates found in some of them. A few countries do not report separate statistics for standard and dedicated mobile subscriptions.

Finally, there is not yet an official methodology to define the limits of M2M SIM cards. National telecom regulators in some OECD countries have begun to release M2M SIM cards figures along with mobile and wireless broadband subscriptions. However, M2M use may still be mixed in with other subscriptions. Therefore, the indicators presented here are still at an initial stage.

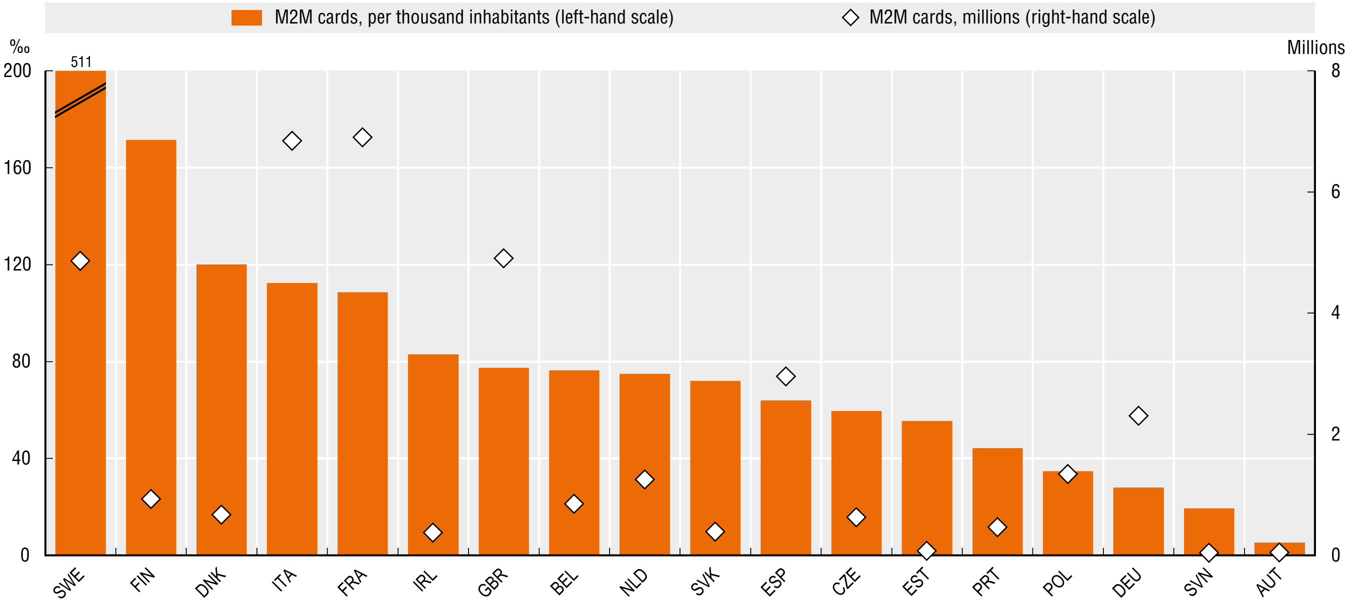
Mobile data subscriptions, by type, December 2013



Note: The figure refers to the sum of standard and dedicated data mobile subscriptions.
Source: OECD, Broadband Portal, www.oecd.org/sti/broadband/oecdbroadbandportal.htm, July 2014.

StatLink http://dx.doi.org/10.1787/888933147993

The penetration of M2M SIM cards, 2012



Source: OECD computations based on data from communications regulatory bodies and ministries, May 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148000

Key findings

In May 2014, registered domains reached 241 million, up from 233 million in mid-2012. This increase represented a marked slowdown in comparison with earlier years, reflecting possible saturation of the domain name market. About 150 million domains are registered under generic top-level domains (gTLD) (i.e. "com", "org", "net", etc.), with .com (commercial) accounting for three-quarters of registrations. The recent availability of new addresses (e.g. ".hotel") might provide new impetus to gTLD registration. Registrations under OECD-related country code top-level domains (ccTLDs) stood at almost 65 million at the end of the first quarter of 2014.

Statistics on domain name registration offer a partial but valuable perspective on the development of the World Wide Web. These indicators can inform discussions in areas such as domain name pricing policies, and help to ensure transparency in registration management for service providers, business users and consumers.

Cross-country differences are wide and reflect diversity in the presence of websites combined with country specificities in terms of ease and cost of registration and maintenance. Denmark, the Netherlands and Switzerland have 200 or more ccTLDs registered per 1 000 inhabitants, while other OECD countries have 50 per 1 000 users or less. This latter group includes countries where use of ccTLDs is historically lower, for example, Korea, where users rely on second-level domains, and the United States, where some gTLDs are "domestic" (e.g.: .gov for government, or .edu for educational institutions) and gTLDs have consistently been used more widely than the .us domain. For other countries in this range, such as Mexico and Turkey, the rate generally reflects lower Internet penetration.

The number of Internet hosts has historically provided a complementary perspective on the size of the Internet and its growth. However, this indicator is gradually losing ground, as the one-to-one relationship between a host and an IP address is blurred, not least due to the depletion of IPv4 addresses. As of January 2014, hosts worldwide reached 1.01 billion, up 6% annually from 888 million in 2012, but representing a slowdown from 10% in the previous biennium and a 26% compound annual growth rate from 2000 to 2010.

The number of routed autonomous systems (AS) that a country has may be a proxy for the amount of competition in a market. It indicates the ease with which a company may take control over routing its traffic and exchange with other networks. Most countries saw an increase in the number of AS per capita between 2010 and 2012.

DID YOU KNOW?

There were about 241 million registered domains in the world in mid-2014.
On average, there was one geographical top-level domain (ccTLD) per ten OECD Internet users.

Definitions

The Domain Name System (DNS) translates user-friendly host names (e.g. www.oecd.org) into IP addresses. The hierarchical syntax of a domain name is supported by the "dot" in the name and is read by the DNS server from right to left (.org is the top level domain and .oecd is the sub-domain of this TLD.) *Generic top level domains* (gTLDs) include ".com" or ".org", *country code-top level domains* (ccTLDs) consist of two-letter codes generally reserved for a country or a dependent territory (e.g. ".au" for Australia). Registry operators, known as Network Information Centres (NICs), distribute two-letter codes.

An *Internet host* is a machine or application connected to the Internet and uniquely identified with an IP address.

An *autonomous system* (AS) can be defined by the aggregate of IP blocks for which the network is responsible. Such networks are termed autonomous because they can determine the routing of their traffic independently from any other network. Every AS is assigned a unique number (ASN) by a regional Internet registry (RIR).

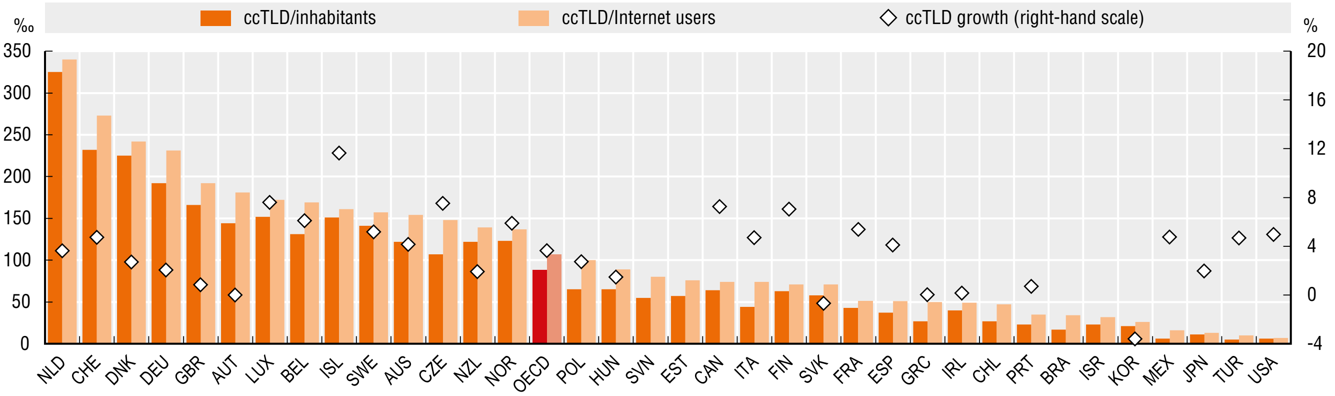
Measurability

The measure of domain names works by asking the network a question such as "where is OECD.org located?" The DNS answers using resolvers that query the data stored in a hierarchical and widely distributed sets of machines known as DNS servers that are essential for the smooth functioning of the Internet. The number of Internet hosts is measured by the Internet Systems Consortium (ISC) survey, which queries the domain system for the name assigned to every possible IP address. Hosts used to proxy for IP addresses; the one-to-one relationship between a host and an IP address is now being blurred by the use of Network address translation (NAT), which allows many computers to share a single IP address, to mitigate the depletion of IP(v4) addresses.

Autonomous systems vary significantly and differ considerably in size. The majority of measurement forms available calculate the extent of the Internet the network can reach directly. Another approach examines the number of IP addresses behind an AS. These data only show information from routing tables, not on number of customers, revenues or geographic size.

Country code top-level domain registration (ccTLD) density 2014 Q1 and growth (2013 Q1-2014 Q1)

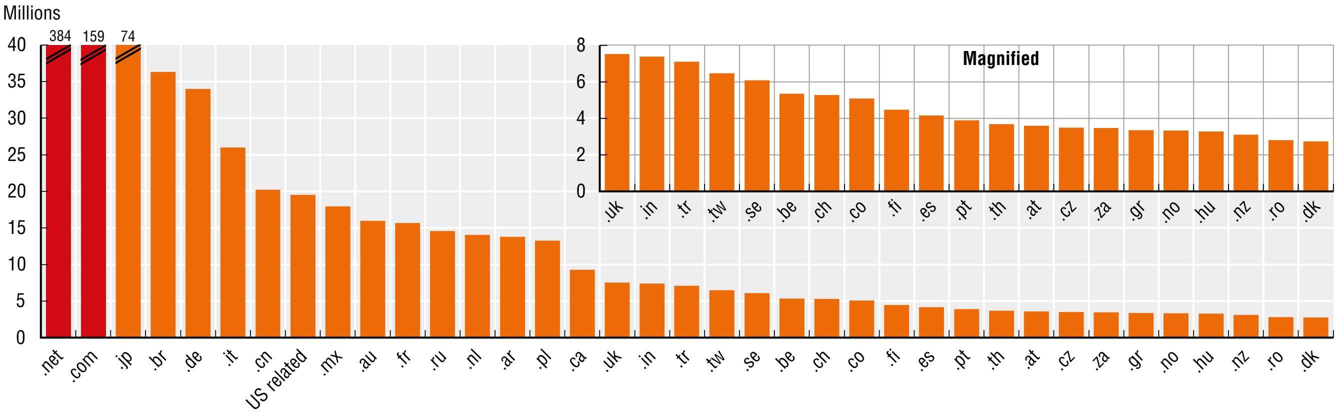
Per thousand inhabitants and Internet users, annual growth rate (right-hand scale)



Source: OECD computations based on countries' Network Information Centres (NICs) and KISA, May 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148012

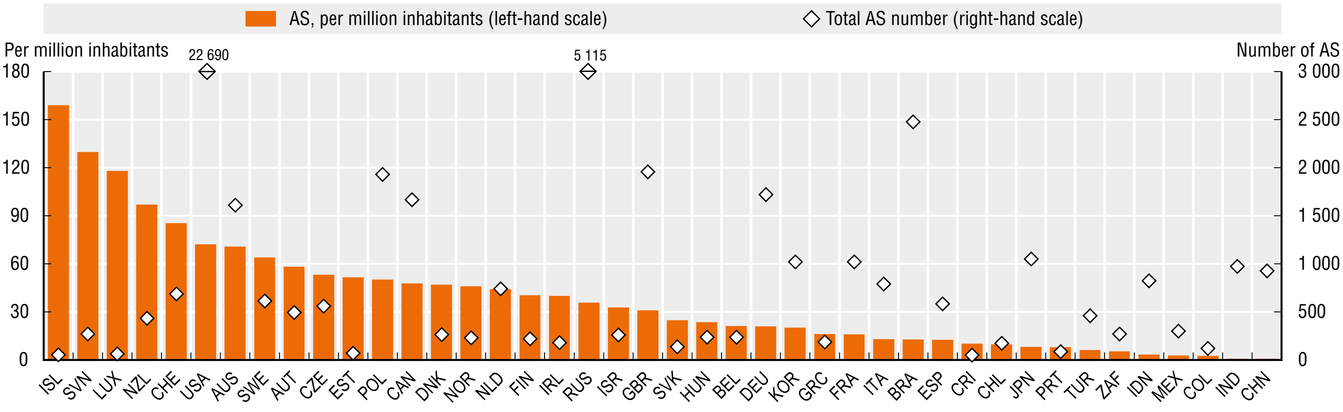
Hosts by type of domain, January 2014



Note: US-related domains include .us, .edu, .mil and .gov.
Source: Internet Systems Consortium (ISC), ftp.isc.org/www/survey/reports/current/bynum.txt, June 2014.

StatLink http://dx.doi.org/10.1787/888933148021

Routed autonomous systems, 2013



Source: OECD computations based on Potaroo, April 2014.

StatLink http://dx.doi.org/10.1787/888933148033

2.4 Toward higher speed

Key findings

Adequate network access speed is essential to fully exploit existing services over the Internet and to foster the diffusion of new ones.

In December 2013, fixed (wired) broadband subscriptions rates in the OECD area reached 27%, up from 23% at the end of 2009. In Denmark, the Netherlands and Switzerland, subscription rates are 40% or above, but remain below 20% in six other OECD countries.

Distribution of fixed broadband subscriptions across speed tiers varies significantly across countries, due to a variety of factors (e.g. level of competition, population density in the market addressed, availability of back-haul, type of technology most widespread, etc.).

In December 2013, Korea was the OECD country with the highest share of fixed broadband subscribers with a download speed above 10 Mbit/s (71%), followed by Japan (47%), the Netherlands (45%) and Switzerland (42%). The share of subscribers with a download speed below 4 Mbit/s was largest in Chile (74%) followed by Mexico (65%) and Turkey (56%).

Users in Korea and Japan are recorded as having the highest speed levels, as a result of extensive deployment of fibre to the home. Countries with competing DSL and cable television networks also perform well with cable networks overcoming some distance barriers, particularly in places with lower population densities. It is notable that the countries with the three lowest penetration rates also offer the lowest actual speeds.

Differences in speed levels are important for customers. For example, high-speed broadband subscribers (above 10 Mbit/s) can download a high-quality movie (1.5 GB) in less than 22 minutes, while the same process takes at least 52 minutes for low-speed subscribers (below 4 Mbit/s).

In most OECD economies, mobile connectivity is undergoing major advancements through the deployment of *Long Term Evolution* (LTE) networks. Mobile broadband providers are advertising download speeds at levels increasingly closer to those of some fixed broadband offers. The two networks are complementary as wireless networks are effective only to the extent that traffic can be quickly offloaded to fixed networks (a consequence of spectrum limitations).

DID YOU KNOW?

In 2013, the share of fixed high-speed broadband subscribers (above 10 Mbit/s) ranged between over 70% and less than 2% across OECD countries.

Definitions

Fixed (wired) broadband penetration is computed as the number of subscriptions to fixed (wired) broadband services, divided by the number of residents in each country.

Fixed (wired) broadband includes DSL, cable, fibre to the home (FTTH) and other fixed wired technologies.

All components include only connections with advertised data speeds of 256kbit/s or more.

Measurability

Measurement of broadband performance is affected by the potential gap between advertised and "actual" speeds delivered to consumers. Several tools are available to measure actual download and upload speeds, together with other quality-of-service parameters.

Among the major providers of broadband speed data, M-Lab and Ookla compile results from Internet access speed tests conducted by users. The willingness to perform the test, the overall broadband adoption rate, the extent to which ISPs promote the tool and the languages spoken, are all factors that may affect the number of tests and the comparability of the results among countries.

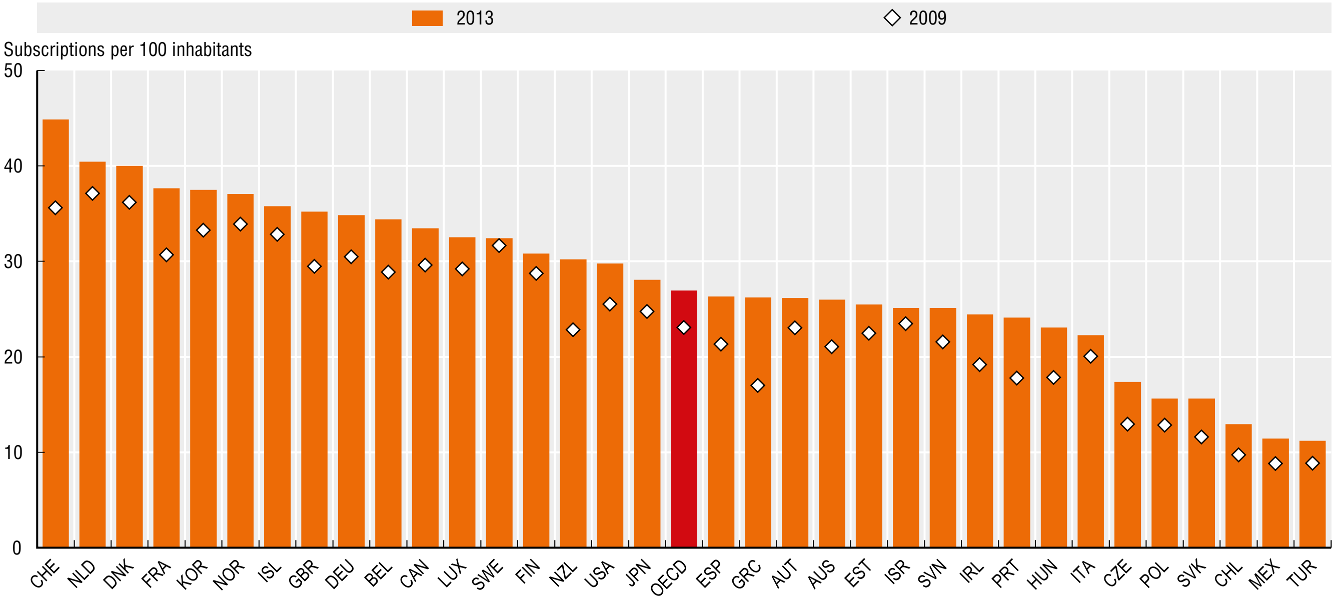
By way of contrast, Akamai runs tests on the speed at which content is delivered to users through its server network located around the world.

Despite significant differences in methodologies, the results from Akamai, M-Lab and Ookla are strongly correlated, except in the case of Japan, where Akamai reports lower broadband speed. It can also be observed that Ookla delivers systematically higher download speed measurement than the other two tools.

The breakdown of fixed broadband penetration by speed tiers presented here is based on Akamai.

Fixed (wired) broadband penetration rates, December 2009 and 2013

Subscriptions per 100 inhabitants

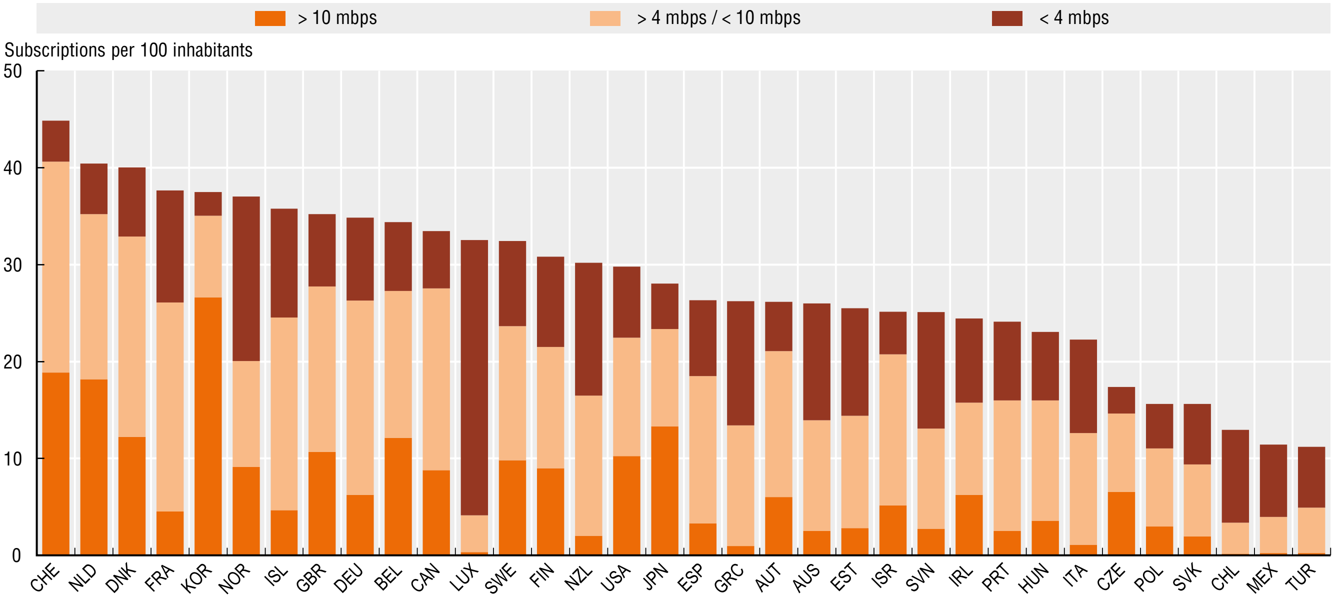


Source: OECD, Broadband Portal, www.oecd.org/sti/broadband/oecdbroadbandportal.htm, July 2014.

StatLink http://dx.doi.org/10.1787/888933148044

Fixed (wired) broadband penetration rates by speed tiers, December 2013

Subscriptions per 100 inhabitants



Source: OECD computations based on Akamai, July 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148053

Key findings

Prices for connectivity provide useful insights into competition and efficiency levels in communication markets. Benchmarking these prices allows stakeholders, including telecommunication operators, policy makers and consumers, to evaluate progress towards their objectives.

The OECD uses a set of telecommunication prices based on a basket approach. It selects the least costly options among surveyed offers, thereby providing a tool to compare prices available to consumers and businesses with a range of differed usage patterns.

Assessment of any market requires consideration of prices from a range of baskets, including for users that have widely varying requirements and significant differences in their ability to pay. Here, one basket is shown by way of example, but a full range is available in the *OECD Communications Outlook 2013*.

In 2014, a fixed-line broadband subscription basket with 33 GB usage and at least 15 Mbit/s download speed costs from USD 58 to less than USD 17 per month, expressed in purchasing power parity (PPP).

Country performance for any single basket can vary widely, hence the need to examine a range of baskets. In this case, the average price for the same basket across the OECD decreased from USD 38.1 to USD 34.5 PPP in the 18 months from September 2012 (with the largest decreases observed in Iceland, Mexico and Turkey).

Broadband mobile services are rapidly gaining a larger share of the wireless and overall market for communication services. Nonetheless, wireless and fixed services are viewed as being complimentary, even though they may be substitutable for some services such as telephony.

Operators in all countries offer voice and data packages that include a specified volume of traffic or unlimited offers, with mobile data traffic nearly always more costly than fixed-line services. This is one reason why smartphone users predominantly access data services when connected to Wi-Fi in locations such as offices and at home.

One of several mobile baskets tracked by the OECD includes 100 calls, 140 SMS and 500 MB of data. In February 2014, this basket was priced between USD 19 and USD 36 PPP a month in half of OECD countries. Monthly subscription prices were lowest in the United Kingdom (USD 10.4 PPP), Estonia (11.9) and Austria (13.6) and highest in Japan (77.0), Chile (58.6) and Hungary (54.5).

DID YOU KNOW?

Depending on the country of residence, smartphone users in the OECD can pay up to seven times more for a comparable basket of mobile services.

Definitions

Broadband services are frequently sold as mixed bundles including Internet access, telephony and (for fixed networks) television. As broadband bundles are sometimes sold at a lower price than stand-alone services, connectivity prices are not always directly comparable among offers and across countries.

The OECD methodology for measuring *prices of communication services* is based on "baskets" of fixed broadband and mobile communication services, collected from several operators with the largest market shares in each country. USD PPP is used to facilitate international comparisons, with data also being available in USD using exchange rates.

The OECD has developed a new set of baskets for broadband services, both for fixed broadband (adopted in 2009) and wireless broadband (2012).

Measurability

To collect broadband price data, 1 950 stand-alone fixed broadband offers from 102 operators and 1 300 mobile voice plus data offers from 74 operators in the 34 OECD countries were surveyed for the OECD/Teligen baskets. Where stand-alone broadband was not available from a given operator, the least expensive bundled package was selected and included in the comparison.

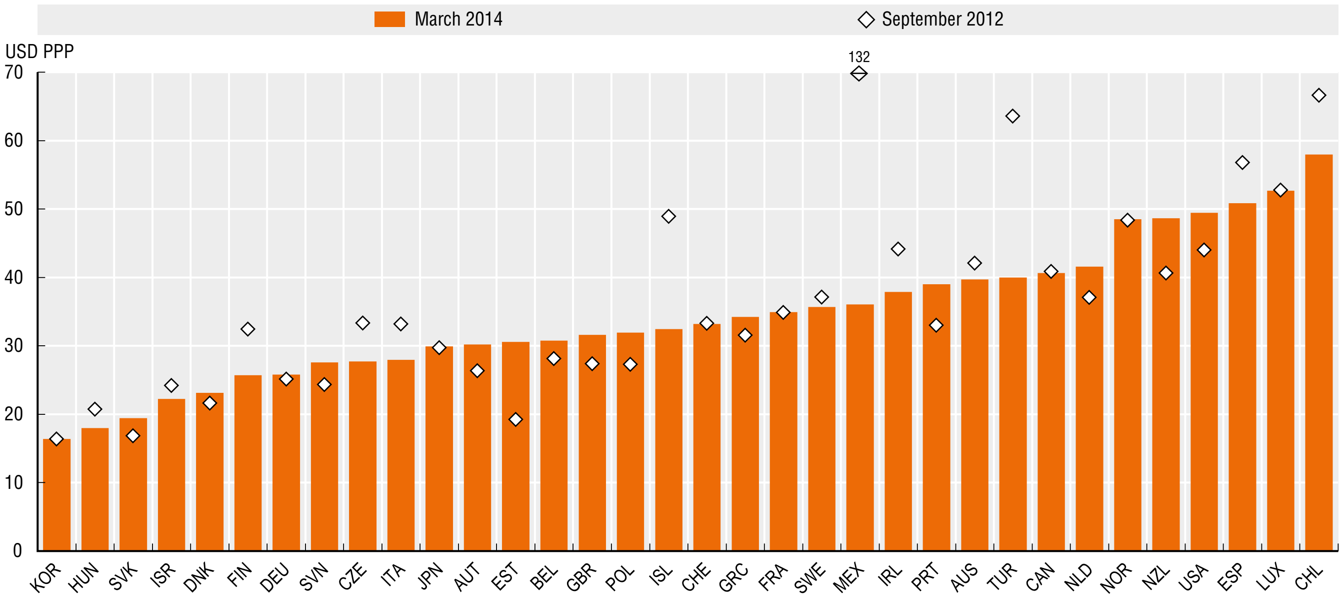
For fixed broadband, a set of three operators per country was chosen (with an average of 19 offers per operator). These included the incumbent telecommunications operator, the largest cable provider (if cable exists) and one alternative provider, if available, over DSL, cable or fibre.

The surveyed offers had to be advertised clearly on the operator's website. In the case of DSL, cable and fibre offers, these were recorded but not used in calculations when speeds were below 256 Kbit/s. The considered offers were for month-to-month service and had to be available in the country's largest city or in the largest regional city for firms with only regional coverage.

Mobile baskets were based on consumer profiles and offers available from the largest operators in each country.

Prices of fixed broadband basket, 33 GB, 15 Mbit/s and above, September 2012 and March 2014

USD PPP per month

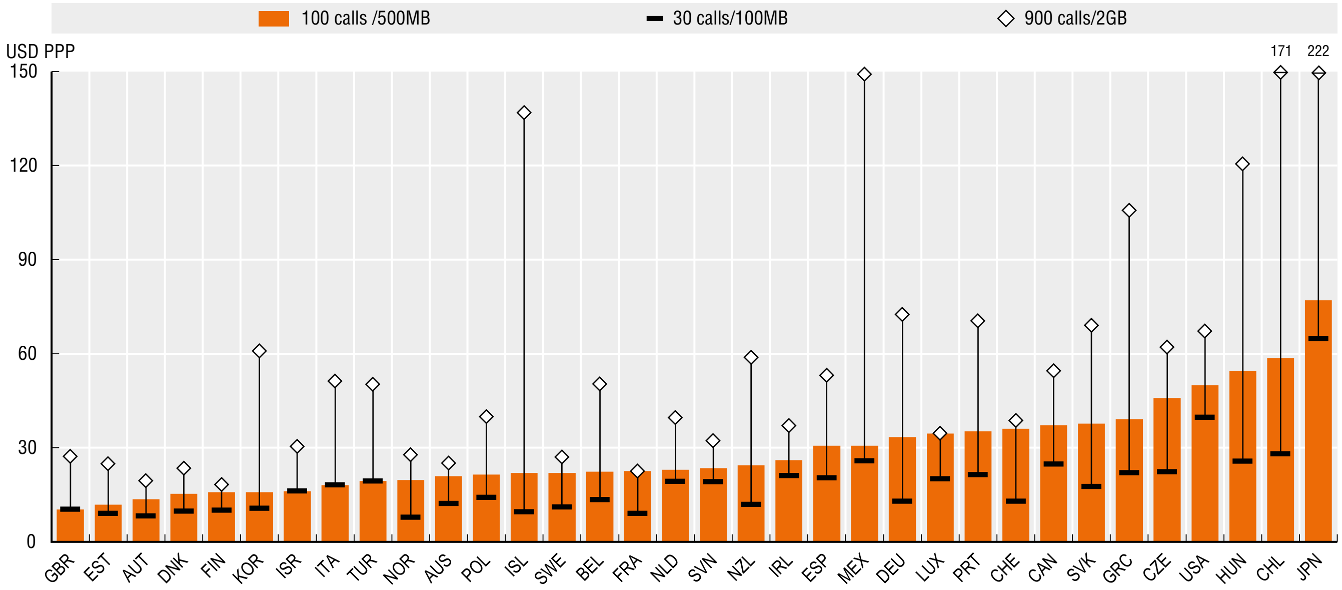


Source: OECD and Teligen, April 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148062

Prices of mobile voice calls plus data traffic reference baskets, February 2014

USD PPP per month



Source: OECD and Teligen, April 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148078

2.6 ICT devices and applications

Key findings

Most ICT devices today are Wi-Fi enabled, allowing users to connect to the Internet anywhere and anytime.

More than 60% of Internet users in the OECD area employ a laptop computer and almost as many use a desktop. Meanwhile, 37% of users now connect to the Internet via smartphones and 13% via tablets. In some OECD countries, well above 10% of users report connecting through other devices as well, such as game consoles or TVs.

Overall, the number of devices per user is associated with rates of Internet usage and other factors, including per capita income and age. These factors affect, in particular, the diffusion of tablets and smartphones, which show the highest variability across countries and, together, influence to a large extent their position with respect to the average number of devices per user.

The diffusion of smartphones and tablets is accompanied by the multiplication of dedicated software applications, otherwise known as "apps".

Apps extend the rich communication potential of the Internet beyond the traditional desktop computer and enable users to benefit from a myriad of services, including many related to mobility, such as location-based services and a growing array of sensors available with handheld devices. They also represent an increasingly important channel for governments and companies to deliver content, information and services to users.

The average smartphone user in the OECD has on average 28 applications installed, but uses only about 11. In general, the number of apps installed is closely correlated with the number of apps in use.

Familiarity is an important factor in explaining sophistication of usage. Other things being equal, in countries where the diffusion of smartphones is comparatively high, a higher share of individuals are likely to install and use a broader array of applications.

There are exceptions, however. On average, users in Japan are among those with the highest number of apps installed (37), but also among those with lowest number of apps in use (less than 8).

DID YOU KNOW?

The average user in Korea connects to the Internet using 2.5 different devices, against 1.2 in Hungary. The average OECD smartphone user has about 28 apps available, but uses only 11.

Definitions

The *average number of devices used* is an approximation based on the sum of the items surveyed in ICT usage surveys.

Apps are computer software (applications) meant to execute specific tasks, as opposed to the system software. Here, they are considered with respect to mobile devices only. Statistics on apps are based on a survey commissioned by Google to specialised enterprises in different countries. The reference period for the number of apps in use was the previous 30 days.

Measurability

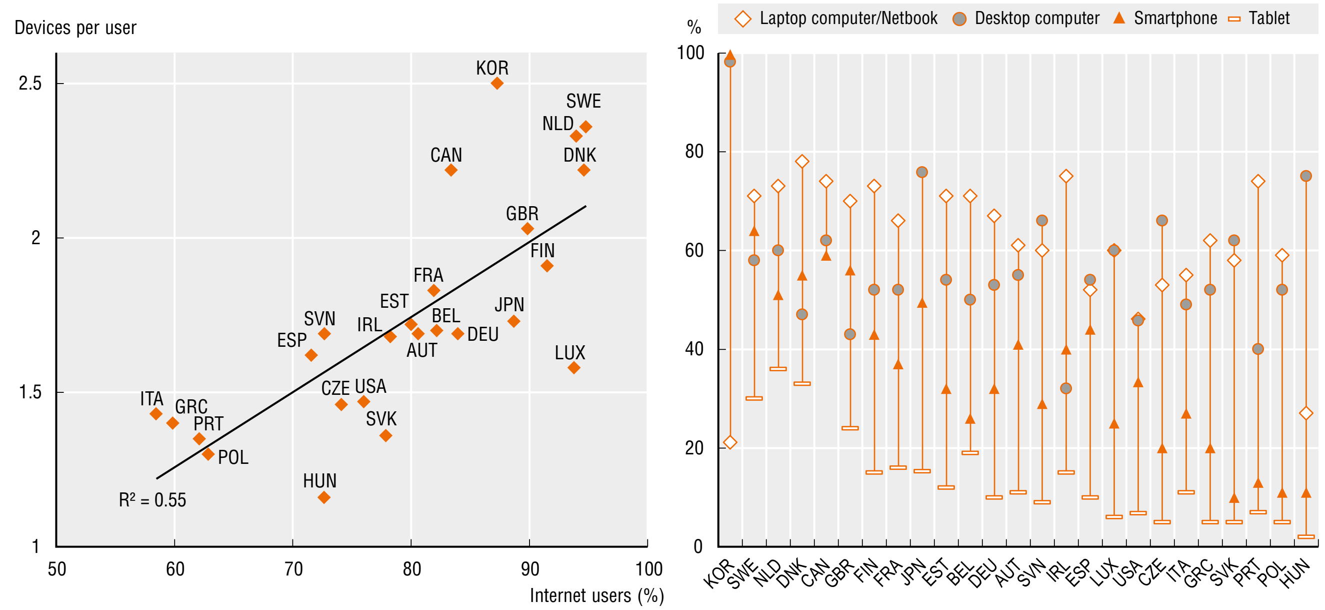
The design and breadth of surveys on ICT usage by individuals is quite diverse across countries (see 3.1). Data on the variety of devices in use, in particular, ought to be considered as indicative only.

Devices are surveyed in different ways and are sometimes bundled together (e.g. laptops combined with personal computers). As such it is not possible to achieve fully comparable indicators. In particular, the average number of devices per user might be underestimated for Canada and Japan, due to the lack of specific figures for tablets and laptops, respectively.

Apps-related information from the Google multi-country survey can be considered sufficiently reliable, but is based on relatively small country-level samples (about 1000 individuals) limiting its use. A specific module on apps has been included in the 2014 revision of the OECD Model Survey on ICT Access and Usage by Households and Individuals. In the future it will be possible to collect data for applications on mobile phones with official statistics, using much larger samples and capturing a richer set of policy relevant metrics. These include the diffusion of specific types of apps (e.g. health or education related) or aspects related to security, distinguished by different groups of individuals.

Devices used to access the Internet, 2013

Variety of devices per user linked to the percentage of Internet users (left-hand panel) and Users by device as a percentage of Internet users (right-hand panel)

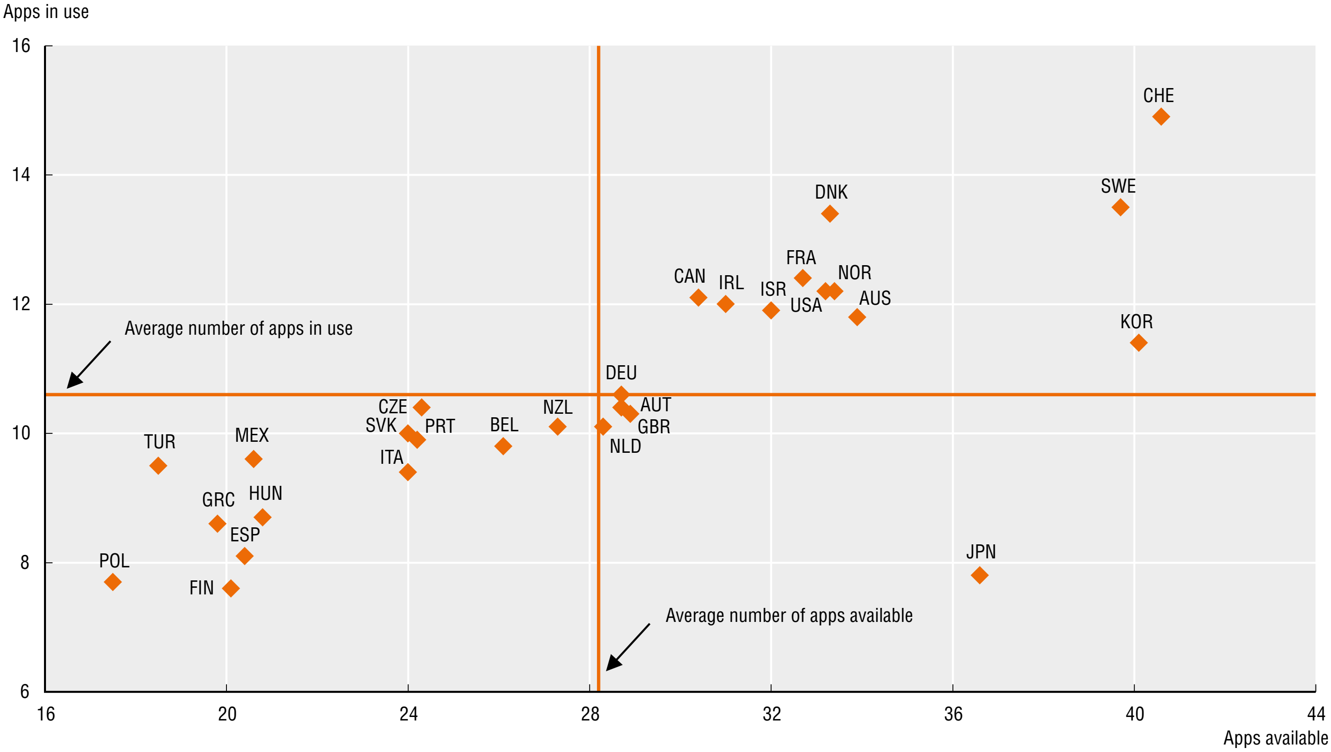


Source: OECD, ICT Database, May 2014; European Commission (2013), *Cyber security*, Special Eurobarometer, No. 404, Brussels and national sources. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148083

Smartphone apps availability and usage, 2013

Average number per user



Source: Google, Our Mobile Planet, Smartphone research 2013, think.withgoogle.com/mobileplanet/en/downloads. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148094

Key findings

The Internet opens up new opportunities on global markets for consumers and businesses. IT infrastructure, regulatory framework and economic integration of countries are among key factors that impact cross-border e-commerce uptake by individuals and enterprises.

Despite recent initiatives both at the national and international level to foster cross-border online transactions, e-commerce activities mostly remain within national borders. In 2012, in a majority of countries for which data are available, the percentage of enterprises that engaged in electronic sales (e-sales) in their own country was much higher than those who carried out cross-border e-sales. Exceptions were Ireland and Luxembourg, where multinational enterprises (MNEs) play a larger role.

In Finland and Norway, the share of enterprises that conducted cross-border online sales within the EU was less than 30%, as opposed to Austria and Italy, where this share was 62% and 56% respectively.

In general, European countries prefer EU partners both for online sales and purchases, while consumers in Canada mostly order from the United States as regards cross-border online purchases. In 2013, 26% of individuals who ordered goods or services over the Internet in the EU28 chose sellers located in other EU countries, against 14% from those located in the rest of the world. In Canada, 63% of e-consumers reported ordering from sellers in the United States.

Most OECD countries are placing greater emphasis today on policies and programmes that promote market transparency and provide information and guidance to empower citizens by strengthening their ability and confidence to buy goods and services across borders, in particular online.

In 2012, at the EU level, consumer trust in purchasing goods or services via the Internet from retailers located in another EU country was highest in Iceland, Ireland and Luxembourg, and lowest in Germany.

Language appears to be one of the enabling factors related to consumer trust. Available data from the EU28 show that trust in cross-border online purchases in non-English speaking European countries increases with willingness to place orders in another EU language.

DID YOU KNOW?

In 2013, 63% of e-consumers in Canada ordered goods or services from the United States, and 26% of e-consumers in the EU28 ordered products from other EU countries.

Definitions

An e-commerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders *(OECD Guide to Measuring the Information Society 2011)*. For individuals, whether sellers or purchasers, such transactions typically occur over the Internet. For enterprises, *e-commerce sales* figures presented here include all transactions carried out over webpages, extranet or Electronic Data Interchange (EDI) systems.

MNEs are treated as *national sellers* once their website declares them to be registered as a company with an address in the surveyed country. National sellers include the trade business or sales offices established in the country by foreign owners.

Partner countries refer to the EU members for countries in the European Statistical System and to the United States for Canada.

Shares of *Internet users who trust in EU cross-border sellers* and of those who are *willing to use another EU language for purchases over the Internet* are computed as a percentage of those who expressed an opinion about the statements (agree or disagree).

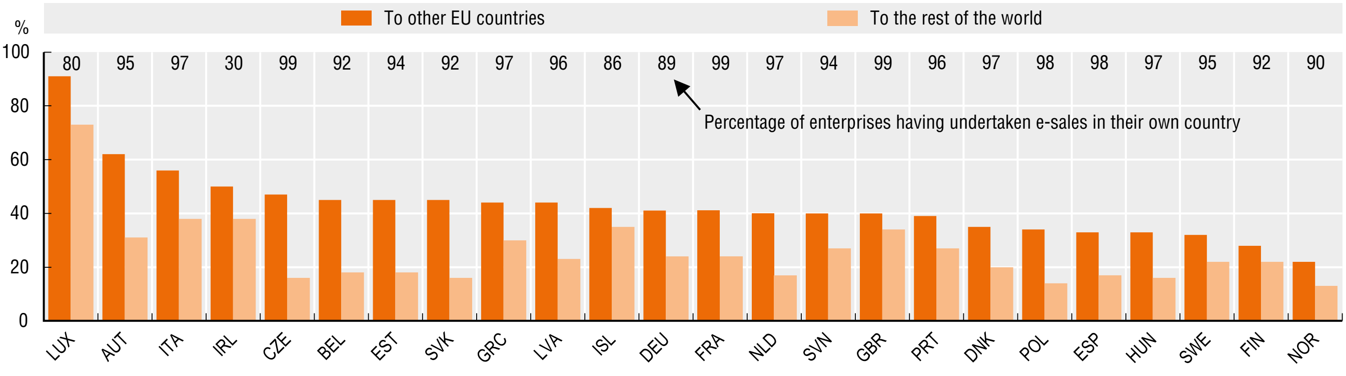
Measurability

Flash Eurobarometers are thematic public opinion surveys conducted at the request of the European Commission to obtain relatively rapid results by focusing on a specific target group. The survey on consumer attitudes towards cross-border trade and consumer protection was carried out in the 28 EU countries, Iceland and Norway in September 2012 across a sample of 25 543 individuals aged 15 years and more. Different social and demographic groups were interviewed via telephone in their mother tongue on behalf of the European Commission Directorate-General for Health and Consumers (DG SANCO).

As is the case for all public opinion surveys, interpretation of the results is subject to caution. As the samples used are relatively small, marginal differences observed across countries might be the result of sampling errors and not necessarily represent differences in the underlying population.

Cross-border e-commerce sales by enterprises, 2012

As a percentage of all enterprises having undertaken sales via e-commerce

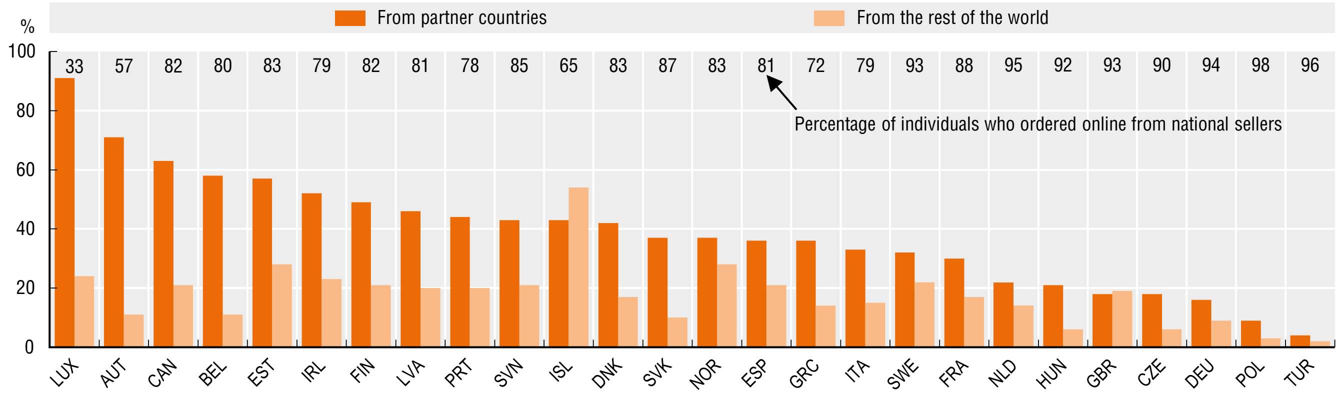


Source: OECD based on Eurostat, Information Society Statistics, June 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148101

Cross-border online purchases by individuals, 2013

As a percentage of individuals who ordered goods or services over the Internet in the last 12 months

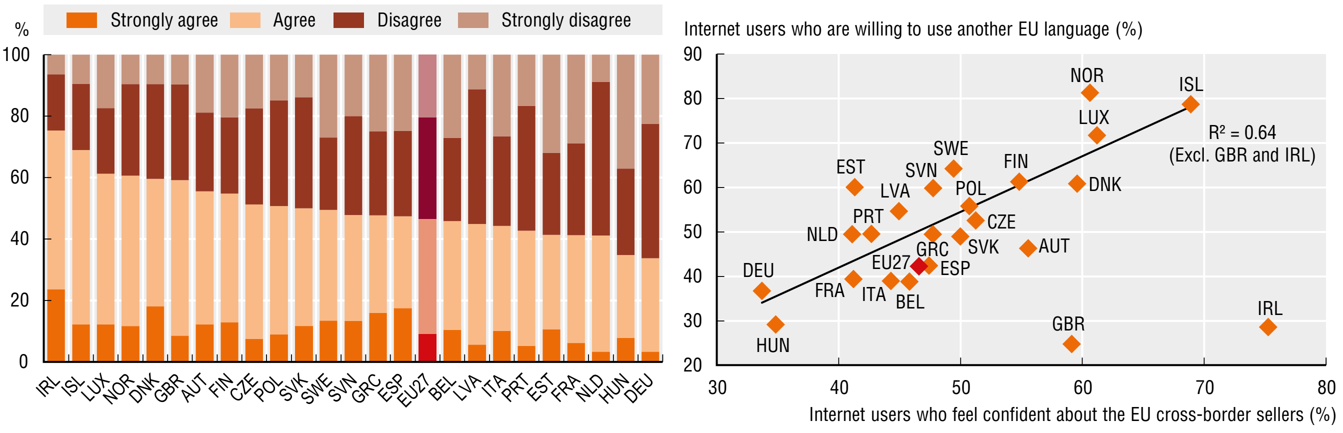


Source: OECD based on Eurostat, Information Society Statistics and national sources, June 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148115

Consumer trust in cross-border online purchases, 2012

"I feel confident purchasing goods or services via the Internet from retailers/providers in another EU country" (left-hand panel) linked to the willingness to use another EU language for purchases over the Internet (right-hand panel)



Source: OECD based on European Commission (2012), *Consumer attitudes towards cross-border trade and consumer protection*, Flash Eurobarometer, No. 358, Brussels.

StatLink http://dx.doi.org/10.1787/888933148121

Key findings

The digitisation of information and network connectivity create new challenges for the protection of sensitive data and network communications.

Most businesses adopt security measures to protect their digitised information and networks. The extent to which they undertake these measures depends on their awareness and capabilities and the digital security risks they face. This in turn relates to factors such as their size and the industry in which they operate.

In 2010, the most widespread security measures adopted by enterprises included offsite backup of archives and strong-password authentication. A minority of firms adopted intrusion detection systems (IDS) and authentication and identification tools such as hardware tokens and biometric methods. Offsite backup was used by 75% or more of enterprises in Denmark and Norway, against less than 20% in Hungary, the Slovak Republic and Turkey. In 2012, this rate was also low in Korea, possibly due to the substitution of offline with online backup over the cloud. The use of strong passwords is still the easiest way to protect access to information, in particular for SMEs, and in 2010 was used by most firms, especially in Ireland, Italy and Spain where the business sector is dominated by small enterprises.

Major security issues include denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, the latter employing several machines. Such attacks often target access to the networks of individual organisations (e.g. banks) and can result in partial or complete disruption of Internet access in whole areas when a major service provider is affected. Taking into account the number of active hosts, data on (D)DoS attacks provide an indication of threat levels and show that certain areas are particularly attractive to this type of security threat.

In general, large enterprises are more prone to DoS attacks. Differences across economies are significant, but are difficult to explain. The share of enterprises suffering from DoS attacks in 2010-12 was 1% or below in Hungary, Japan and New Zealand, but above 10% in the Slovak Republic.

At the global level and in absolute terms, China, the Russian Federation and the United States lead both in terms of DDos attacks originating from or targeting each geographical area. These two measures are highly correlated, suggesting to some extent the local nature of many attacks. Exceptions include Chinese Taipei, the Netherlands, Panama and Romania, which are at the origin of many more attacks than they receive, while the opposite is the case in Canada, Estonia, Italy, Norway, Poland, Spain and Sweden.

DID YOU KNOW?

In 2010-12, between 2% and 6% of businesses in most economies experienced an IT security problem resulting in denial-of-service. Large firms are targeted proportionally more frequently than SMEs.

Definitions

Security methods considered here include two information protection systems: *offsite data backup* and the *use of digital intrusion detection systems* (devices or software applications monitoring for malicious activities or policy violations). Three identification and authentication tools are also considered: *strong passwords* (where the concept of strength encompasses length, the use of different types of characters and limited duration), *hardware tokens* (including smartcards) and *biometric methods*. Tools within each group are not mutually exclusive (i.e. are not additive) and the two groups are complementary. The information is collected by national surveys on ICT usage in businesses.

Denial-of-service (DoS) attacks aim to make machines or network resources unavailable by interrupting or suspending the services of a host connected to the Internet (websites, Internet services or whole network). Attacks can take several forms; a *distributed denial-of-service (DDoS)* attack occurs when the bandwidth or the computing resources of the targeted systems is flooded using multiple machines, which are often controlled remotely by the attacker by means of malware. The indicator on businesses experiencing DoS problems highlights the diffusion of attacks on enterprises by employment size and is based on user survey information drawn from official statistics. The indicators on numbers of DDoS attacks by origin and target geographical area are based on monitoring of websites undertaken by a not-for-profit organisation, Shadowserver (shadowserver.org).

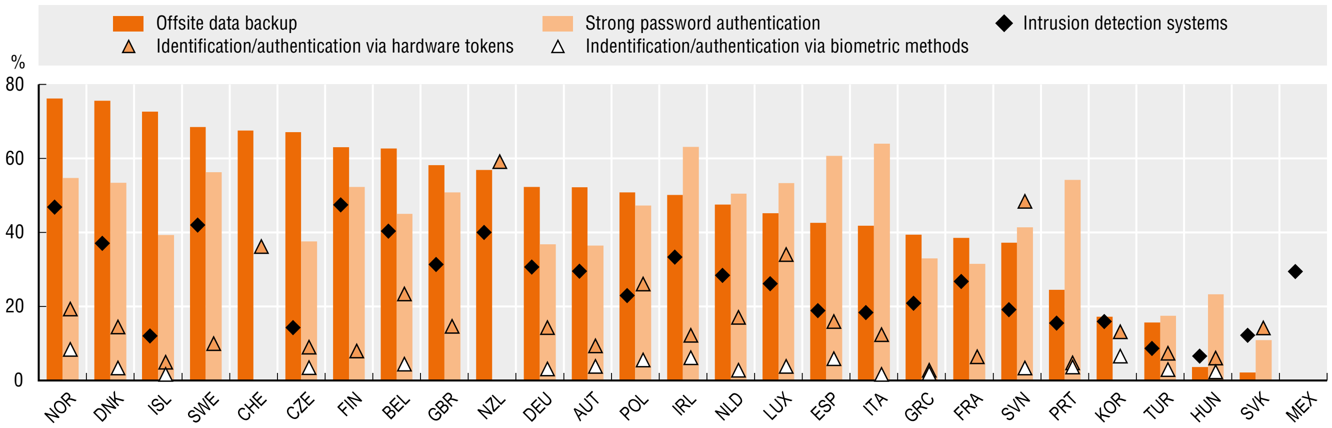
Measurability

Data availability and comparability on security topics still pose challenges. Security tools and issues evolve rapidly, and the latest collection of data by Eurostat dates from 2010. Information on incidence of security issues also requires the validation of methodologies used to gather data from the Internet, and should be complemented by an appreciation of the gravity of security incidents.

The OECD is working with National Computer Security Incident Response Teams to develop a common set of metrics on incidents (see 2.10), and proposed a dedicated module on security and privacy in its 2014 revision of the OECD Model Survey on ICT Usage by Businesses.

Use of security methods for authentication/identification and the protection of data by enterprises, 2010

As a percentage of all enterprises

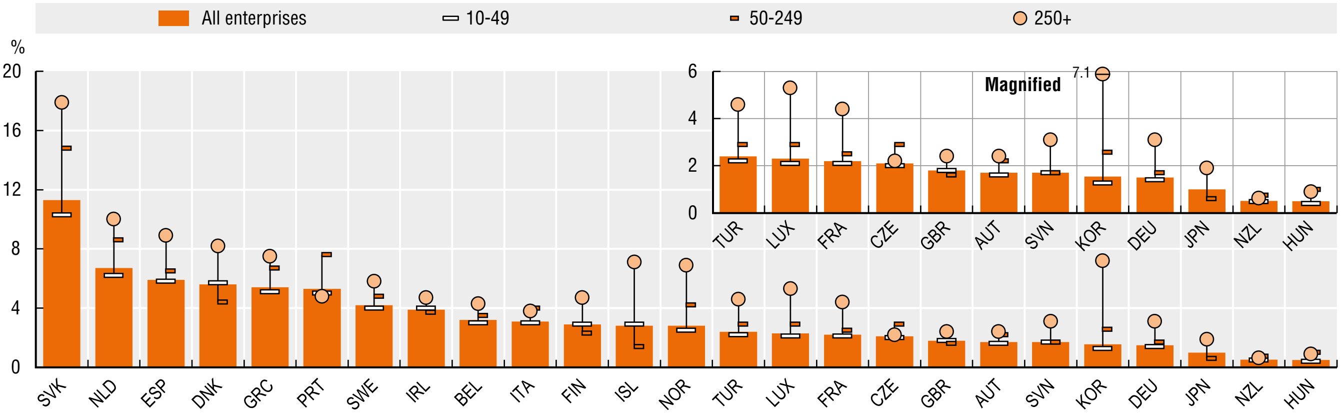


Source: OECD, ICT Database and Eurostat, Information Society Statistics, June 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148133

Businesses having encountered IT security problems, attacks resulting in denial-of-service, by size, 2010

As a percentage of all businesses in each employment size class

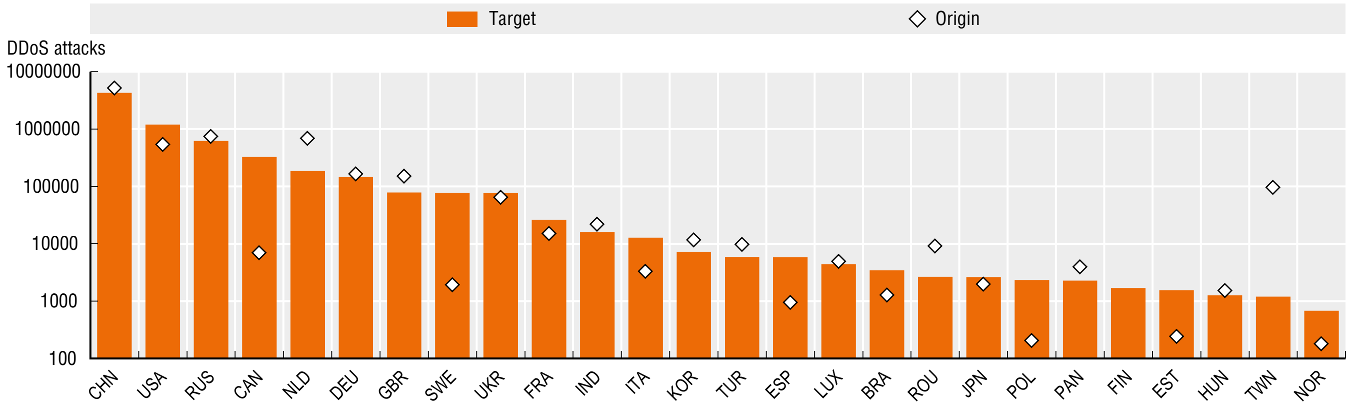


Source: OECD, ICT Database and Eurostat, Information Society Statistics, June 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148142

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: Shadowserver, www.shadowserver.org/wiki/pmwiki.php/Stats/GeoLocations, May 2014.

StatLink http://dx.doi.org/10.1787/888933148153

Key findings

Security and privacy are among the most challenging issues facing online services and the development of e-commerce. Both concern consumer trust that personal information will not be viewed, stored or manipulated during transit and storage by third parties without their consent or for fraudulent purposes.

Trust is a central factor in all economic transactions, both offline or online. However, the importance of trust increases with online shopping, as this is more prone to uncertainty and risk than traditional shopping.

In 2009, security was cited as the main reason for not buying online for over one-third of Internet users in the European Union who had not made any purchases online. Privacy concerns accounted for a slightly smaller share (about 30%). The strong variation in perceptions of security and privacy risks across countries with comparable degrees of law enforcement and technological know-how suggests that cultural attitudes towards online transactions play a significant role.

Online security and privacy concerns show a positive relationship in most countries. In 2009, security concerns among Internet users not buying online were the highest in France, the Slovak Republic and Switzerland and the weakest in the Czech Republic, Ireland and Poland. Privacy concerns were the highest in Switzerland, followed by the Slovak Republic and Finland, and the weakest in Australia, Canada and the Czech Republic.

Traditionally, security issues in e-commerce have been considered in relation to the abilities of e-merchants to protect their online transaction systems. However, e-consumers are becoming increasingly aware that security depends crucially on their behaviour.

In recent years, Internet users have changed their behaviour in a number of ways because of security concerns. They are now less likely to give personal information on websites or in response to open emails from people they know. However, in 2013 only about one-third of Internet users in the European Union had ever changed the security settings of their browsers, ranging from above 50% in Austria to 15% in the Czech Republic.

DID YOU KNOW?

In 2013, only about one-third of Internet users in the European Union had ever changed the security settings of their browsers.

Definitions

Security concerns for regarding online payments include misgivings about giving credit card details over the Internet and related anxiety about financial loss.

Privacy concerns refer to reluctance to provide personal details over the Internet, including names and addresses, but also private photos or private financial information.

Modifying the *security settings of Internet browsers* refers to any action to improve browser settings to ensure higher protection against viruses and other attacks or attempts at intrusion (normally accessible under "Tools", "Internet options" in the web browser menu).

Measurability

Information on perceived security and privacy is collected through the e-commerce module of the ICT usage surveys in households and by individuals. Information on whether Internet users have ever changed their browser's security setting is collected through a module on e-skills.

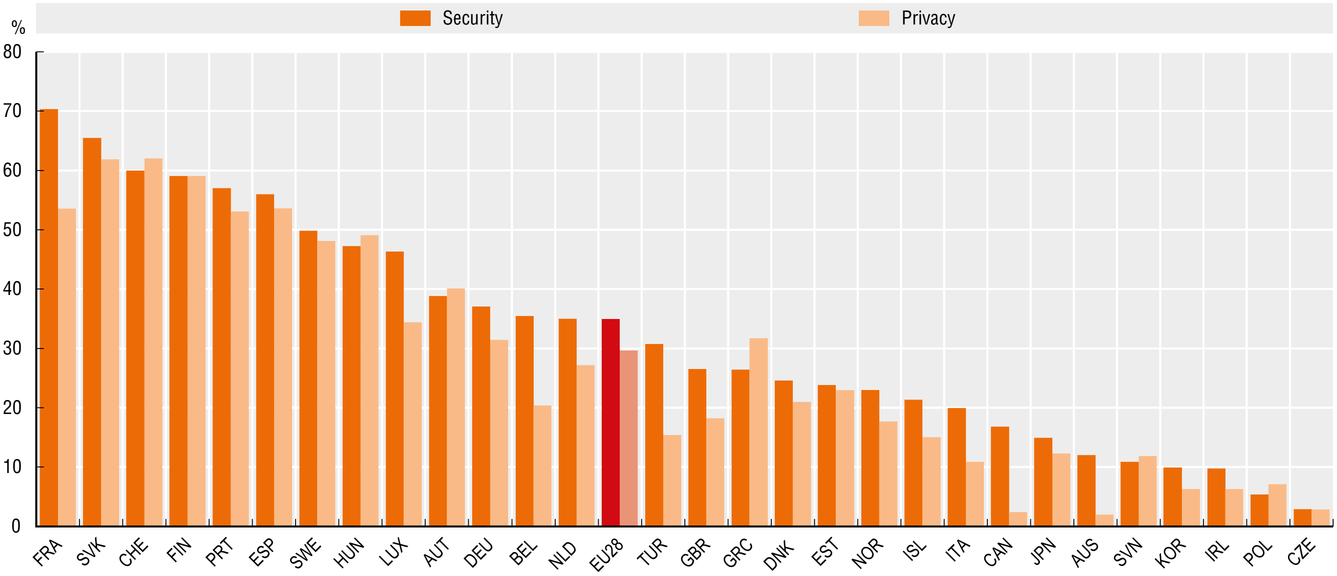
Both the European and OECD model surveys on ICT usage ask direct questions about security and privacy, including on the use of protection from IT threats, the frequency of security updates and security incidents.

The 2014 revision of the OECD Model Survey on ICT Access and Usage by Households and Individuals includes a specific module on security and privacy, based on policy-relevant indications from the OECD Working Party on Security and Privacy in the Digital Economy.

It is a matter of debate among statisticians whether respondents are able to answer technical questions about IT security. To minimise this problem, coverage of the OECD security module is limited to home use, as this is the ICT environment about which users are more likely to have information, as opposed to ICT use at work or school.

Main reasons for not buying online because of privacy and security concerns, 2009 or more recent year available

Percentage of Internet users who did not make online purchases

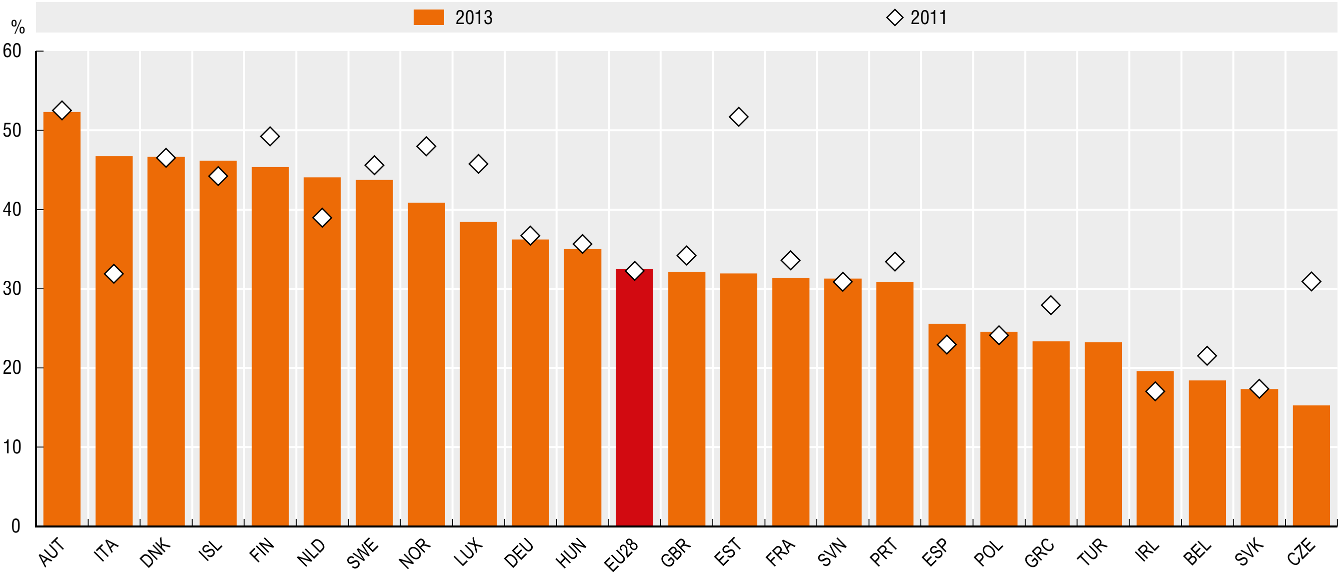


Source: OECD computations based on Eurostat, Information Society Statistics and national sources, May 2014. See chapter notes.

StatLink http://dx.doi.org/10.1787/888933148160

Acknowledging the issue of Internet security: users changing browser security settings, 2011 and 2013

As a percentage of Internet users



Source: OECD computations based on Eurostat, Information Society Statistics, May 2014.

StatLink http://dx.doi.org/10.1787/888933148178

Why do we need indicators?

The protection of security and privacy online has become a key policy issue as individuals, businesses and governments shift large parts of their daily activities to the Internet. Malware are reported to be spreading at high rates, increasing the risks of compromising information infrastructures (van Eeten *et al.*, 2010). Advances in trans-border flows of personal data, as well as big data storage and analytics, amplify the risk of misuse of personal data and challenge the application of privacy protection regulation (OECD, 2011).

These issues have reached a tipping point where policy makers can no longer neglect their implications on innovation, economic growth and prosperity. A recent OECD work on the economics of personal data, for example, highlights the value of personal data and its contribution to innovation as a "New Source of Growth" in sectors as diverse as healthcare, finance, energy and marketing. Likewise, the OECD report *National Cybersecurity Strategies* reveals that OECD governments now recognise that the Internet has evolved from a useful platform for e-commerce and e-government to an essential infrastructure for the functioning of society, making online security a "national security" concern (OECD, 2012).

These evolving challenges and opportunities call for improvement in the evidence base for security and privacy policies, for at least three reasons – first, to assess whether policy interventions on online privacy and security are warranted, second, to design more effective measures for online security and privacy and, finally, to better assess the benefits and costs of online security and privacy policies currently in place.

What are the challenges?

Statistical information on online security and privacy are typically drawn from three major sources: user surveys, activity reports and the Internet.

Surveys among individuals and business have a number of major advantages. These include comparable data based on international standards that can be associated to characteristics of respondents, the possibility to collect subjective information and the flexibility to adjust to new policy needs. They also have several drawbacks when it comes to the measurement of online security and privacy. Respondents may not answer the surveys correctly, either because they do not have the necessary information or knowledge to understand or to answer the questions correctly (e.g. about security threats), or because they do not wish to answer questions on sensitive matters (e.g. illegal downloading).

Activity reports are intended to give stakeholders information about an organisation's routine work, for example, firms' financial statements and reports by privacy enforcement authorities. One of the biggest advantages of activity reports as a source of data is their periodic release, which allows the building of time series from the reported data. However, international differences in reporting requirements and changes in national reporting rules may make the collected information non-comparable across countries and over time.

The *Internet* is itself a rich source of data. When it comes to measuring Internet-related activities, Internet traffic can provide big data sets for analysis. The main strength of Internet-based data is that it is automatically generated and can be collected and distributed in real-time via the Internet. For example, data collected on malware, whether through antivirus or firewall solutions, can be transmitted directly to providers of these tools, thus circumventing sensitivity and information issues raised by household and business surveys. The most severe drawback of Internet-based data, however, is statistical: it is very hard to define an Internet sample and to generalise the results from particular users, service providers or websites to the whole Internet population. Therefore, Internet-based data should be linked to more traditional sources, such as surveys and reports. However, this data linking is not without problems. In order to protect the privacy of users, Internet identifiers (e.g. IP addresses) are usually anonymised or aggregated, making the link to individual or firm-level data unfeasible.

Besides the issues specific to each data source, there is a more fundamental challenge to the measurement of security and privacy, whether online or offline. Because of the illegal nature of privacy and security violations, not all incidents are identified or reported. Only incidents that have been identified as such can be measured, and such incidents represent an unknown share of the total number of incidents. This has some serious implications concerning how to interpret numbers of privacy and security incidents. For example, a decrease in the number of reported malware infections may reflect an actual decrease in malware or a reduced ability to detect it.

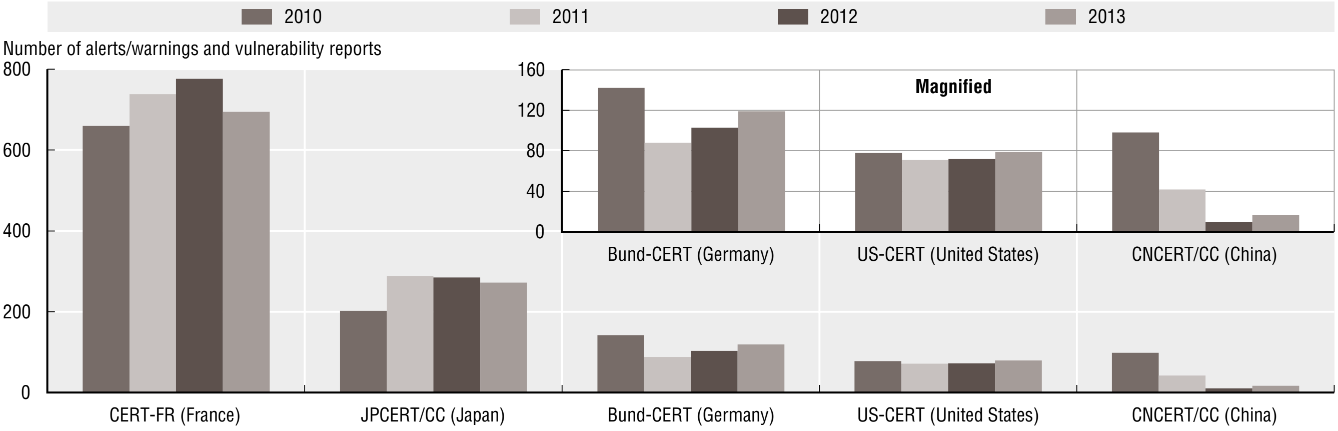
Options for international action

A number of internationally coordinated actions have been undertaken or are currently ongoing to improve the measurement of online security and privacy. The OECD Working Party on Security and Privacy in the Digital Economy issued a series of suggestions for improving ICT use surveys for policy makers in the areas of cybersecurity and privacy, notably the economics of personal data and security, prevention measures and incident response. These recommendations were implemented in the 2014 revision of the OECD Model Surveys on ICT usage by households/individuals and by businesses.

The OECD is also undertaking a project to improve the use of data generated by Computer Security Incidents Response Teams with national responsibilities ("national CSIRTs"), as a source of internationally comparable statistics. Many national CSIRTs already produce and report statistics based on data about their activities and the incidents they handle. However, these statistics are often difficult to compare for reasons including differences in CSIRT constituencies, lack of common reporting rules and divergent taxonomies of key aspects of CSIRT operations, such as the notion of "incident". These current statistics are thus not ideal to inform policy-making decisions.

The following figure shows this point by comparing the number of alerts/warnings and vulnerability reports issued by five national CSIRTs in 2010-13. In general, these CSIRTs use a different basis for publishing alerts/warnings and vulnerability reports. For example, some CSIRTs separate publications of alerts/warning from that of vulnerabilities while others bring them together. In addition, some provide a single publication for multiple vulnerabilities while others do the opposite. This explains why cross-country differences in the number of alerts/warnings and vulnerability reports are not correlated to the size of the country, either in terms of population or number of Internet users.

Number of alerts/warnings and vulnerability reports issued by five national CSIRTs, 2010-13



Source: OECD computations based on CSIRTs reports, July 2014.

StatLink http://dx.doi.org/10.1787/888933148183

The OECD is engaging with CSIRTs from member countries as well as non-members to improve this situation. The overall objective of the work is to develop guidance for CSIRTs to produce and report internationally comparable statistics. This guidance would provide statistical definitions for a set of indicators (e.g. budget, personnel, skills and co-operation, along with specific kinds of incidents) that national CSIRTs could report on a voluntary basis, in addition to suggestions for CSIRTs to better leverage existing data, such as from third-party institutions, for statistical purposes.

References

OECD (2012), "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. Doi: http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 176, OECD Publishing. Doi: http://dx.doi.org/10.1787/5kgf09z90c31-en.

Van Eeten, M., J.M. Bauer, H. Asghari and S. Tabatabaie (2010), "The role of Internet service providers in botnet mitigation: An empirical analysis based on spam data", *OECD Science, Technology and Industry Working Papers*, No. 2010/5, OECD Publishing. Doi: http://dx.doi.org/10.1787/5km4k7m9n3vj-en.

Notes

Israel

"The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities or third party. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

2.2 Mobile data communication

The penetration of M2M SIM cards, 2012

Data originate from the following national sources: Austria (RTR), Belgium (BIPT), Czech Republic (CTU), Denmark (ERST), Estonia (MKM), Finland (FICORA), France (ARCEP), Germany (Bundesnetzagentur), Ireland (Ofcom), Italy (AGCOM), the Netherlands (ACM), Poland (Ministry of Administration and Digitization), Portugal (ANACOM), the Slovak Republic (Ministry of Transport, Construction and Regional Development), Slovenia (AKOS), Spain (CMT), Sweden (PTS) and the United Kingdom (Ofcom).

For France, Ireland and Portugal, data refer to 2013.

2.3 The growth of the Internet

Country code top-level domain registration (ccTLD) density 2014 Q1 and growth (2013 Q1-2014 Q1)

For Brazil, Chile, Estonia and Slovenia, data refer to end-May 2014.

2.4 Toward higher speed

Fixed (wired) broadband penetration rates by speed tiers, December 2013

This figure is based on OECD subscription data (December 2013) merged with Akamai's actual speed data (1st quarter, 2014).

For Luxembourg, there is a technical issue in the Akamai data related to the use of Network Address Translators and IPv6. It is estimated that if modified, to account for both these factors, the ratio of connections above 10 Mbit/s would climb from 1% to more than 30%.

2.5 Prices for connectivity

Prices of fixed broadband basket, 33 GB, 15 Mbit/s and above, September 2012 and March 2014

The OECD basket of fixed broadband services includes total charges for a subscription with a minimum speed of 15 Mbit/s and 33 GB for 60 hours of usage per month. USD purchasing power parities (PPP) are used to facilitate international comparisons.

Prices of mobile voice calls plus data traffic reference baskets, February 2014

Price benchmarking results for mobile broadband services presented here cover services provided over a handset or smartphone.

The 30 calls/100 MB, 100 calls/500 MB and 900 calls/2 GB OECD baskets of mobile telephone charges include fixed and usage charges for respectively 30, 100 and 900 voice calls, and a volume of 100 MB, 500 MB and 2 GB of data traffic per month. These baskets portray approximately small, average and large users of voice and mobile data. USD purchasing power parities (PPP) are used to facilitate international comparisons. Additional information on the computation methodology can be found in the *OECD Communications Outlook 2013*.

Mobile tariff plans in some OECD countries (e.g. Japan) may focus on a different balance of usage between data and voice (e.g. larger volume of data and fewer minutes of calls), and mobile users may benefit from an extra monthly subsidy for a handset purchase provided by the operator. These points should be taken into consideration when interpreting indicators of mobile prices.

2.6 ICT devices and applications

Devices used to access the Internet, 2013

For Canada, data refer to 2012. Devices per user data originate from the Internet Use Survey 2012 as published in *The Daily* on 28 October 2013 and relate to the percentage of households with Internet access by Internet access device. Data include laptops only instead of laptop computers/netbooks, and all wireless handheld devices instead of smartphones only. Data on tablets are not available.

For countries in the European Statistical System, data originate from the Special Eurobarometer No. 404 on cyber security.

For Japan, devices per user data are based on the Internet Usage Trend Survey 2012 and relate to individuals aged 6 or more. Data refer to PC use at home instead of desktop computers. Data on laptop computers/netbooks are not available.

For Korea, data originate from the Survey on the Internet Usage 2012. Devices per user data relate to the percentage of households with Internet access by Internet access device. The smartphone category includes all mobile phones. Data on tablets are not available.

For the United States, data originate from the US Bureau of the Census, relate to individuals aged 15 and more, and refer to 2011. The category laptop computers/netbooks includes laptops only. The category Smartphones includes all cellular phones and tablets includes e-books.

Devices per user data are computed using an additional “Other” category, which typically includes game consoles and televisions with Internet access.

Smartphone apps availability and usage, 2013

For the number of apps installed, data refer to the question: “And of the apps you currently have installed on your smartphone, how many have you used actively in the last 30 days? Please type in a number. If you don’t know the exact number please provide your best estimate.”

For the number of apps actively used, data refer to the question: “And of the apps you currently have installed on your smartphone, how many have you purchased for a certain amount in an app distribution platform such as Apple App Store and Google Play? Please type in a number. If you don’t know the exact number please provide your best estimate.”

The average excludes zero values.

2.7 E-commerce across borders

Cross-border e-commerce sales by enterprises, 2012

For Germany, data refer to 2010.

Cross-border online purchases by individuals, 2013

Partner countries refer to other EU countries for those in the European Statistical System and to the United States for Canada.

For Canada, data refer to 2012.

2.8 Security

Use of security methods for authentication/identification and the protection of data by enterprises, 2010

For Korea, data refer to 2012.

For Mexico, data refer to 2008.

Businesses having encountered IT security problems, attacks resulting in denial-of-service, by size, 2010

For Japan, data refer to 2011.

For New Zealand, data refer to 2012.

2.9 Perceiving security and privacy threats

Main reasons for not buying online because of privacy and security concerns, 2009 or more recent year available

For Australia, data originate from the Multipurpose Household Survey as published in the *Household Use of Information Technology 2012-13* and refer to 2012/2013 (fiscal year ending in June 2013) instead of 2013. "Payment security concern" relates to "concerned about providing personal details online".

For Canada, data originate from the Internet Use Survey 2012.

For Japan, data originate from the Internet Usage Trend Survey 2011. "Security concern" relates to "concerned about security when giving out credit card information" and "Privacy concern" relates to "protection of personal information". Data cover Internet users aged 15 and more, instead of 16-74 year-olds.

For Korea, data originate from the Survey on the Internet Usage 2009 and relate to "Privacy concern" and "Security concern" as reasons for not using Internet shopping.

For Switzerland, data originate from the Omnibus TIC 2010 survey.

References

Cisco (2014), *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, 2013–2018, Cisco White Paper, CISCO, San Jose, CA, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

European Commission (2013a), *Consumer Conditions Scoreboard – Consumers at home in the single market*, 9th edition, Brussels.

European Commission (2013b), *Cyber Security*, Special Eurobarometer, No. 404, Brussels.

OECD (2014a), "The OECD Model Survey on ICT Access and Usage by Households and Individuals", Working Party on Measurement and Analysis of the Digital Economy, DSTI/ICCP/IIS(2013)1/FINAL, OECD, Paris.

OECD (2014b), "The OECD Model Survey on ICT Usage by Businesses", Working Party on Measurement and Analysis of the Digital Economy, DSTI/ICCP/IIS(2013)2/FINAL, OECD, Paris.

OECD (2013), *OECD Communications Outlook 2013*, OECD Publishing. Doi: http://dx.doi.org/10.1787/comms_outlook-2013-en.

OECD (2012), "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. Doi: http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD (2011a), *OECD Guide to Measuring the Information Society 2011*, OECD Publishing. Doi: http://dx.doi.org/10.1787/9789264113541-en.

OECD (2011b), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 176, OECD Publishing. Doi: http://dx.doi.org/10.1787/5kgf09z90c31-en.

OECD (2010), *Consumer Policy Toolkit*, OECD Publishing. Doi: http://dx.doi.org/10.1787/9789264079663-en.

Van Eeten, M., J.M. Bauer, H. Asghari and S. Tabatabaie (2010), "The role of Internet service providers in botnet mitigation: An empirical analysis based on spam data", *OECD Science, Technology and Industry Working Papers*, No. 2010/5, OECD Publishing. Doi: http://dx.doi.org/10.1787/5km4k7m9n3vj-en.

From:

Measuring the Digital Economy

A New Perspective

Access the complete publication at:
https://doi.org/10.1787/9789264221796-en

Please cite this chapter as:

OECD (2014), “Investing in smart infrastructure”, in *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264221796-6-en

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

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