OECD Economics Department Working Papers No. 1171

The Internet Economy - Regulatory Challenges and Practices

Isabell Koske,
Rosamaria Bitetti,
Isabelle Wanner,
Ewan Sutherland

https://dx.doi.org/10.1787/5jxszm7x2qmr-en

OECD

Unclassified **ECO/WKP(2014)67**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **12-Nov-2014**

English - Or. English

ECONOMICS DEPARTMENT

ECO/WKP(2014)67
Unclassified

THE INTERNET ECONOMY - REGULATORY CHALLENGES AND PRACTICES

ECONOMICS DEPARTMENT WORKING PAPERS No. 1171

By Isabell Koske, Rosamaria Bitetti, Isabelle Wanner and Ewan Sutherland

JT03366006

Complete document available on OLIS in its original format

English - Or. English

ABSTRACT/RÉSUMÉ

The Internet Economy – Regulatory Challenges and Practices

The Internet has become an integral part of the everyday life of households, firms and governments. Its proper functioning over the long run is therefore crucial for economic growth and people's wellbeing more generally. The success of the Internet depends on its openness and the confidence of users. Designing policies that protect society while allowing for Internet's great economic potential to be fulfilled, is a difficult task. This paper investigates this challenge and takes stock of existing regulations in OECD and selected non-OECD countries in specific areas related to the digital economy. It finds that despite the regulatory difficulties, the Internet is far from being a "regulation-free" space as there are various industry standards, co-regulatory agreements between industry and the government, and in some cases also state regulation. Most of them aim at protecting personal data and consumers more generally. In many cases generally applicable laws and regulations exist that address privacy, security and consumer protection issues both in the traditional and the digital economy.

JEL classification codes: D18, K2, L1, L5, L81, L82, L86
Keywords: Digital economy, internet, regulation, consumer protection, competition

****

L'économie internet - enjeux et pratiques de la réglementation

L'Internet fait partie intégrante de la vie quotidienne des ménages, des entreprises et des gouvernements. Son bon fonctionnement sur le long terme est donc crucial pour la croissance économique et le bien-être de la population en général. Le succès de l'Internet dépend de son ouverture et de la confiance des utilisateurs. Concevoir des politiques qui protègent les utilisateurs et la société, mais aussi qui permettent que les grands avantages de l'Internet soit pleinement récoltés est une tâche difficile. Cette étude discute quelques-uns des défis liés au développement d'Internet et fait le bilan de la réglementation en vigueur dans l'OCDE et certains pays non membres de l'OCDE dans des domaines spécifiques liés de l'économie numérique. Il constate que, malgré les difficultés réglementaires, l'Internet est loin d'être un espace "libre de réglementation". Il existe diverses normes de l'industrie, des accords de co-régulation entre l'industrie et le gouvernement, et dans certains cas, la réglementation de l'État. La plupart de ces règles visent à protéger les données personnelles et plus généralement les consommateurs. Dans de nombreux cas des lois et règlements d'application générale existent qui adressent les questions de confidentialité, de sécurité et de protection des consommateurs à la fois dans l'économie traditionnelle et numérique.

Codes JEL : D18 , K2 ; L1 , L5 , L81 , L82 , L86
Mots clé : économie numérique, internet, règlementation, protection des consommateurs, concurrence

TABLE OF CONTENTS

Tables

Figures

Boxes

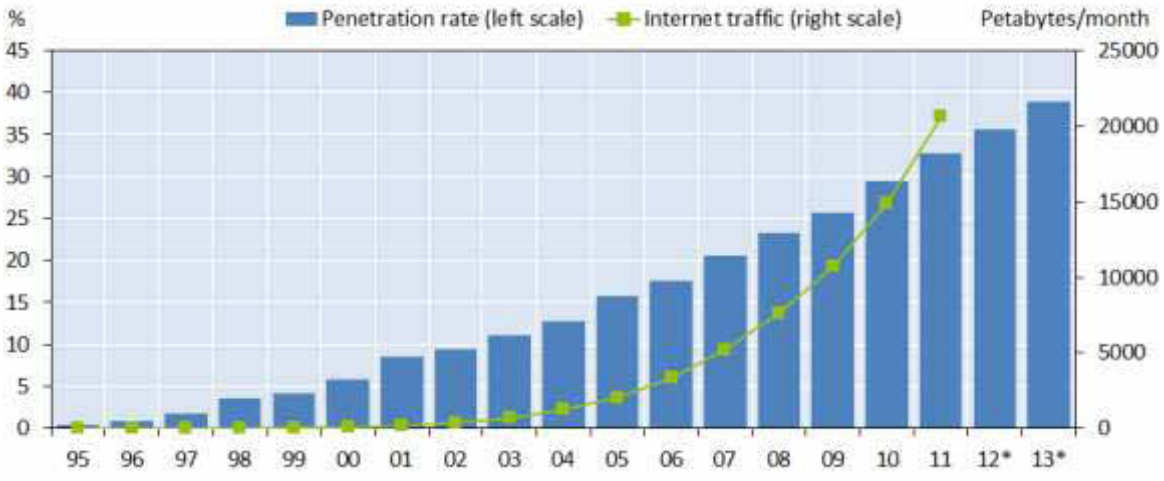
THE INTERNET ECONOMY – REGULATORY CHALLENGES AND PRACTICES

Isabell Koske, Rosamaria Bitetti, Isabelle Wanner and Ewan Sutherland[1]

1. Introduction

The emergence of the Internet as a means of global communication has fundamentally altered the way people and businesses interact. [2] It has become an integral part of the everyday life of households, firms and governments and for many day-to-day activities has become the default tool. While in the year 2000 Internet penetration was below 5%, today almost 40% of the world population is connected to the Internet (Figure 1). Internet traffic has expanded even more rapidly than the number of Internet users, thanks to a rising traffic volume per user.[3] The proper functioning of the Internet over the long run is thus crucial for individuals, businesses and governments. Its success depends on its openness and the confidence of users, with both features having been given increasing policy attention in recent years. The openness of the Internet has stimulated innovations, promoted new services and applications, and encouraged their widespread use. At the same time, the architecture of the Internet has provided opportunities for some to engage in illicit practices, to breach privacy and to undertake fraudulent activities that might harm users.

Figure 1. Internet users and traffic, 1995 to 2013



Note: The Internet penetration rate is the number of people using the Internet as a share of the world population. * Estimate.
Source: International Telecommunication Union (ITU), Cisco VNI.

1. Isabell Koske and Isabelle Wanner are with the OECD, Rosamaria Bittetti is a Researcher at Luiss LAPS, Luiss Guido Carli, Rome, Ewan Sutherland is with the LINK Centre at the University of the Witwatersrand and the CRID at the University of Namur. The authors would like to thank Anne Carblanc, Alain de Serres, Michael Donahue, Jørgen Elmeskov, Sam Paltridge, Taylor Reynolds, Rudolf van der Berg and Jean-Luc Schneider and Andrew Wyckoff for their useful comments and suggestions, Jean-Marc Fournier for his help in designing the questionnaire, the World Bank and the European Commission for voluntary contributions that have allowed computing PMR indicators for nine non-OECD countries from Latin America and the Caribbean and for all seven non-OECD EU countries. They are also grateful to Caroline Abettan for technical and editing support. OECD Working Papers should not be reported as representing the official views of the OECD or of its member countries. The opinions expressed and arguments employed are those of the author(s).

2. The term 'Internet economy' is sometimes used to mean many things. Under the 2008 Seoul Declaration for the Future of the Internet Economy, the term covers the full range of economic, social and cultural activities supported by the Internet and related information and communications technologies (OECD, 2008).

3. Today, twenty households with average broadband usage generate as much traffic as carried by the entire Internet in 1995 (Weller and Woodcock, 2013).

Policymakers have reacted to these developments by encouraging industry initiatives, co-regulatory agreements between industry and government, and in some cases by imposing regulation. While some observers argue that regulation is becoming excessive and overly prescriptive, in ways that may undermine the open and dynamic nature of the Internet, others consider that further government involvement may be needed to ensure that it can continue to function smoothly and develop rapidly, but in ways that do not harm competition and that provide adequate protection for consumers. This paper sheds further light on the discussion by summarizing the main regulatory challenges that are raised by the Internet economy and takes stock of existing regulations in OECD and non-OECD countries.

The rest of the paper is organised as follows. Section 2 provides an overview over the main players in the Internet economy and their interactions to better understand where potential competition issues may arise and who and what needs or does not need to be regulated. Section 3 then discusses the regulatory policy issues that arise, touching upon issues such as third party access to networks, net neutrality, personal data protection and the regulation of search engines and clouds. Section 4 then sheds light on the approaches that OECD and non-OECD countries have taken to regulate the Internet economy.

2. The structure of the Internet

The Internet is complex, involving multiple players and activities, with on-going innovations. Using a simple categorization, it can be thought of as consisting of four main activities (Figure 2):

- *Content*: Internet content can be generated by end-users (*e.g.* an individual's tweet on Twitter or photos uploaded on Instagram) or provided by content rights owners, typically media companies such as Kluwer, BBC or Time Warner that own the property rights over books, news, games, music and movies.

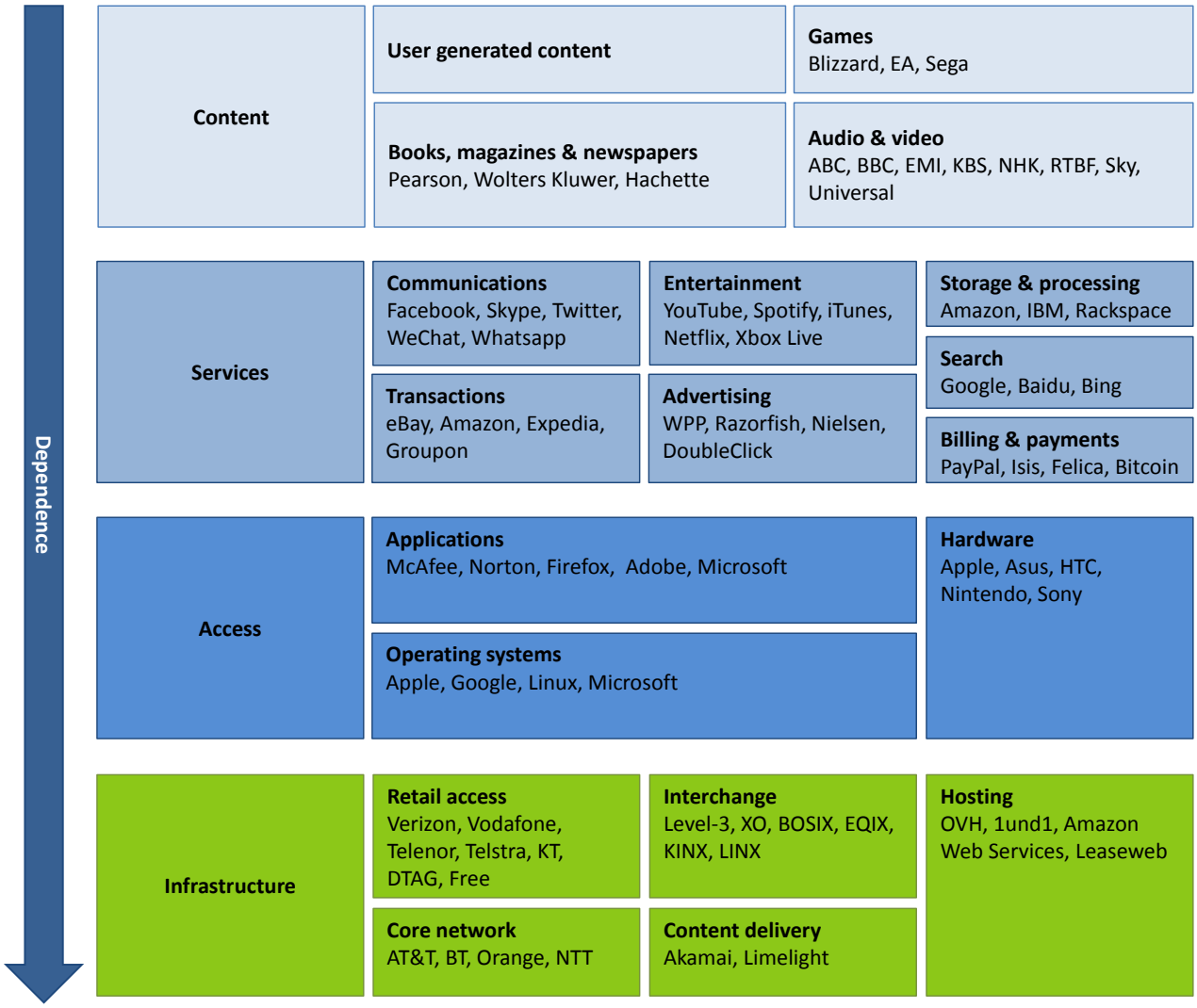
- *Services*: Online services include a wide range of applications accessed by users and consumers, including communication services (*e.g.* voice over IP, social networking, blogging and emailing), search services (in particular web search engines, local directories such as the Yellow Pages and new social search engines such as Facebook's graph search), entertainment services (*e.g.* downloading of audio-visual content, online gaming, streaming and gambling), and transaction services (*e.g.* online shopping). Though often invisible to end-users, enabling technologies and services are indispensable for the delivery of web content and the generation of revenues. Examples include online storage and processing, billing and payment services, and advertising (including both the planning and implementation of online advertising campaigns and the provision of Internet user and usage analyses).[4]

- *Connection*: This comprises the producers of the hardware necessary to access the Internet (*e.g.* PCs, mobile phones and tablets), devices that are attached to the Internet (*e.g.* sensors, machines, vehicles) and the related software (*e.g.* operating systems, browsers, media players and anti-virus programs).

- *Infrastructure*: The physical infrastructure that underlies the Internet consists of transit networks, which interconnect end-networks. (*i.e.* the so-called 'backbones' of Internet traffic transport), Internet exchange points (IXPs) (*i.e.* locations that enable operators to exchange traffic with other ISPs and transit providers that make up the Internet), and the local access network. The first/last mile is provided by Internet service providers (ISPs) and enables end-users to connect to the Internet. This connection can be fixed (via the home telecommunications provider, a cable company or an independent Internet service provider) or, increasingly, mobile.

4. For a discussion of the economic, social and policy role of Internet intermediaries see OECD (2010a) and OECD (2011a).

Figure 2. **The Internet's main stakeholders**



The lines between the different types of players are not always clear cut, as companies might simultaneously engage in several activities. For instance, companies building and operating the core network often also offer Internet access. Similarly firms might engage in a variety of services. A prominent example is Google that operates as search engine, but also offers communication services (Gmail and Google+). Companies such as Google and Facebook own and operate their own network infrastructure, even participating in trans-oceanic submarine fibre networks as full partners on a par with traditional telecommunication operators. Even the line between firms that provide the physical infrastructure and the applications that run on this infrastructure is not always clear in practice, with some ISPs also offering applications such as voice over IP. Services that were traditionally limited to a particular network can now be offered independent of the network.

The Internet has also enabled changes to the competitive forces in the real economy as traditional distribution networks often work in parallel with online networks. Most products can today be purchased both online and from traditional retailers, either in the same format (*e.g.* clothing and physical books) or in different formats (*e.g.* DVDs versus streaming and physical books versus e-books). Online sales affect retail competition through different channels (Buccirossi, 2013). *First*, they make price competition more intense by lowering search costs (though not to zero, because consumers have exogenous search costs and

firms adopt tactics to make price comparisons more difficult for consumers). *Second*, they expand the geographic scope of transactions (even though most e-commerce still takes place within neighbouring countries as consumers prefer to shop within limited distances both for cultural and security reasons). *Third*, they lower distribution costs as manufacturers and consumers can trade directly and online retailers can carry a wider variety of products. *Fourth*, purchasing products online can create information asymmetries because consumers cannot test the product or service they are going to buy, making it more difficult for retailers to build a reputation. Many online retailers address this issue through sophisticated methods for providing peer reviews and recommendations. *Fifth*, network externalities might make it harder for new firms to enter certain electronic markets, though in others, entry barriers might actually fall thanks to, for instance, open source software or clouding computing.

3. The regulatory challenge

At the Seoul ministerial meeting in 2008, OECD countries agreed "to promote the Internet Economy and stimulate sustainable economic growth and prosperity by means of policy and regulatory environments that support innovation, investment, and competition in the information and communications technology sector" (OECD, 2008). When thinking about regulating the Internet economy, it may thus be useful to have in mind three potentially conflicting policy goals: (*i*) enabling the Internet, (*ii*) boosting or preserving competition within and outside the Internet, and (*iii*) protecting privacy and consumers more generally. While there might be synergies between these three policy objectives, they also often involve trade-offs:

- Encouraging the development of the Internet implies a growing pervasiveness of network externalities that exist with communication systems and certain software. In some areas of the economy the likelihood of seeing more firms with dominant market positions may hence increase. Such firms may adopt pricing practices and other strategies that may be seen as incompatible with basic competition rules and yet bring large overall benefits to consumers and producers.

- Conversely, pushing for more intense competition among the firms that operate networks, in particular Internet service providers, might reduce incentives to invest in the maintenance and expansion of existing networks and the deployment of new networks (*e.g.* fibre and 4G).

- Preserving intellectual property rights to provide incentives for new investment might reduce competition and the desire to have easy access to the Internet, which might, in turn, impede its development.

- While stronger consumer protection might help to preserve trust in the Internet, and thus enable its wider use, it might also slow down innovations by inhibiting some applications.

- There is a risk that regulation is designed to suit a particular business model, preventing the emergence of newer models, better adapted to the development of the Internet.

In assessing the need for, and nature of, regulation of Internet content, operation and infrastructure a number of factors need to be borne in mind:

- *Rapid pace of change*: The Internet is evolving rapidly, making it difficult for policy makers to keep up with new technologies, new players and new forms of use. Only a fraction of the devices that could be connected to the Internet are already connected and some of the recent innovations such as mobile phone software platforms may take several years to fully play themselves out.[5] Moreover, the fast-changing technological landscape means that the dominant position of firms in specific markets at specific points in time may be more fragile than appears. The rapid evolution of the Internet warrants caution in imposing long-lived laws and regulations on the industry.

- *Convergence of media*: The Internet involves the convergence of several media, in particular telecommunication, information technology and broadcasting services. The result of this convergence manifests itself in TV sets with added Internet connectivity, and audiovisual media services provided via PCs, laptops, tablets and other mobile devices (EC, 2013). While traditionally the various media were considered as separate markets, facing separate regulatory regimes, this distinction seems no longer appropriate as in today's interconnected world the different media directly compete with each other (*e.g.* households can get fixed-line Internet access from the telecom operator or the cable TV operator). This convergence poses challenges to both competition authorities, for which the definition of the relevant market has become more complex, and regulators which must ensure that they do not cause market distortions through the regulatory differentiation of forms of media. A few countries have already reacted to this challenge, for instance by subsuming telecommunications and broadcasting services under the same regulatory agency.

- *Elimination of geographical boundaries*: The Internet transcends national boundaries and thus puts in question traditional legal concepts such as national sovereignty and jurisdiction (Eko, 2010). The network is not physically controlled by any one country and very large amounts of data are sent across national borders every day. In order to work with the resulting complexity, the Internet has been subject of various regulations and agreements at the international level, for instance with respect to domain names, intellectual property and cybercrime. Nonetheless, the vast majority of Internet transactions are governed by national legislation. This poses problems in cases where a transaction involves different jurisdictions (for instance, a user in one country conducting a transaction with a user in another country through a server in a third country could theoretically be subject to the laws of all three) with conflicting laws (*e.g.* a certain activity being ruled illegal by one country but not by another).

Given these challenges, the central question for policymakers relates to the type of regulatory approach that is best suited for the Internet economy. Options range from self-regulation where users and companies (or their representatives) are urged to solve problems among themselves before turning to the state regulator, over models of co-regulation where the public and the private sector co-operate in joint institutions, to command-and-control regulation where the government or parliament sets the rules of the game. Compared with command-and-control regulation self-regulation has the advantage that the decisions about technical or behavioural standards are taken by industry representatives, who are likely to be more familiar with the functioning of the industry than the state, which seems particularly relevant in a market as complex as the Internet economy. Moreover, self-regulation might be more flexible than command-and-control regulation in adjusting to the dynamic environment of the Internet economy. The downside is that self-regulation might not provide an outcome that is in the best interest of the wider economy, including

5. For instance, connected televisions are still their infancy. In addition there are many other devices beyond these that would benefit from an Internet connection, including cars and various household appliances (Evans, 2011). A recent OECD study estimates that by 2022 an average household will have 50 Internet connected devices, up from 10 in 2012, resulting in 14 billion connected devices in households just in the OECD alone (OECD, 2014).

consumers. Industry often argues that co-regulation is be the best approach, while, Weiser (2009), proposes a model of co-regulation where a self-regulatory body is subject to public agency oversight and backstop.

4. Taking stock of Internet regulations in OECD and non-OECD countries

Irrespective of the general considerations of the previous section, countries have already put in place a wide range of laws and regulations governing the economy, which includes activities conducted via the Internet. This section presents an overview of the existing regulations in OECD and selected non-OECD countries. The data that underlie the analysis were gathered through a questionnaire sent out to country authorities as part of the 2013 update of the OECD's *Product Market Regulation Database* and reflect the situation on 1 January 2013. All OECD countries with the exception of the United States and the following non-OECD countries answered to the questionnaire and are thus covered by the analysis of this paper: Brazil, Bulgaria, Croatia, India, Latvia, Lithuania, Malta, Romania, Russia, and South Africa.[6] Not all countries answered to all questions and Table A1 in the Annex provides an overview of the share of missing values for each question.

Sections 4.1 to 4.3 deal mainly with the companies that build and operate the physical infrastructure (the segment called 'infrastructure' in Figure 2) and section 4.4 deals with the interaction between these companies and all the others that use the Internet to provide content and applications to end-users. Sections 4.5 to 4.7 deal with specific types of content and application providers, notably search engines (the box called 'search' in the segment 'services'), cloud computing (in a strict sense cloud computing is the provision of infrastructure for online 'storage and processing', but in a broader sense it can also include 'communication' services and some 'entertainment' services such as virtual worlds) and social network services. Sections 4.8 and 4.9 treat the overarching issues of personal data protection and consumer protection.

4.1. Wholesale access to fixed line networks

As the Internet relies on fixed and mobile telecommunication networks, competition in the telecommunication sector plays an important role for the Internet economy. Telecommunication networks show large economies of scale and scope that could, in some cases, impede competition in the absence of open access policies. Over the past three decades, the sector has undergone major reforms, starting with the corporatisation and then privatisation of telecommunication operators. This process raised the question of the separation of the competitive and non-competitive activities of the incumbent operators to ensure fair competition, avoid inappropriate cross-subsidies and discrimination in the wholesale supply to rivals. While the scope of that concern has diminished, even today local access networks, the copper wires from homes and offices to the telephone exchange, generally remain a bottleneck, with governments having had to consider how to ensure that incumbent operators do not discriminate against other players. With the copper wires having to be replaced with optical fibres, to meet demand for higher speeds, a considerable investment is required for upgrading, necessitating a very careful evaluation of the incentives of the various operators and the setting of prices that balance competition and the deployment of next generation access networks.

For fixed line networks, most OECD countries have implemented open access policies in the form of mandated regulated access to the wholesale network and the local loop (Table 1). While the price level of this regulated access has often been contested, many OECD countries have achieved a far higher degree of competition than would have been the case if they had not intervened to assist in the development of market access (OECD, 2012). In addition to access to the local loop or wholesale services at higher levels of the network, access to key products such as ducts or in-building wiring also play a major role and need

6. The data for all non-OECD EU countries was gathered in co-operation with the European Commission.

to be taken into account by policy makers and regulators as they may represent major barriers for the entry of alternative operators.

Table 1. Many countries regulate network access

In per cent of all countries that answered the question

		Mobile network		Fixed-line network (for Internet traffic)		Fixed-line local loop	
		Access to and use of network is mandated	Wholesale access prices are regulated	Access to and use of network is mandated	Wholesale access prices are regulated	Unbundling is mandated	Unbundling prices are regulated
OECD	yes	82	67	94	70	91	94
	no	18	33	6	30	9	6
Non-OECD	yes	50	75	50	50	73	64
	no	50	25	50	50	27	36

Note: No data on mobile network and fixed-line network access (for Internet traffic) are available for non-OECD countries because the STRI database does not yet cover these countries.

Source: OECD Product Market Regulation Database, Services Trade Restrictiveness Database.

Open access arrangements have also been used at the backhaul and backbone network levels, for example by municipal backhaul networks, undersea cables or wholesale backbone networks, often as a result of regulatory intervention. In the case of Internet exchange points (IXPs) open access arrangements have been concluded voluntarily among market players, without public intervention.[7] IXPs typically allow parties to exchange traffic based on agreed terms and conditions, and usually have a clear and transparent policy for members to adhere. They are often run directly by industry participants, such as ISPs, that set their own policies and practices on a voluntary basis and under mutually beneficial terms and conditions that are open for others to join upon adherence to these rules.

4.2. Wholesale access to mobile networks

In recent years, many countries have started to mandate access also to mobile networks as a means to improve competition, obliging mobile network operators to host mobile virtual network operators (Table 1). The extent to which the entry of mobile virtual network operators, either through voluntary agreements with mobile network operators or through some form of prescribed access, has improved the level of competition, is debated. OECD (2012) argues that mobile virtual network operators have not been able to drive substantial changes in some markets (*e.g.* international mobile roaming) where their influence is limited by a lack of access to competitive wholesale arrangements.

4.3. Interconnection

The Internet is a collection of several thousand separate and distinct networks, which are interconnected with one another. A network can be a telecommunication company, but also a government agency, sports club, search engine, news agency and many others. Each of the interconnecting links takes one of two forms, transit or peering. Transit agreements are commercial contracts in which a network operator pays another network operator for access to the whole Internet. Peering agreements are agreements between two network operators to exchange traffic between each other's users freely for

7. An IXP is a physical infrastructure through which Internet service providers exchange Internet traffic between their networks. IXPs consist of one or more network switches (*i.e.* a computer networking device that links network segments or network devices), to which each of the participating ISPs connects.

mutual benefit. This allows these networks to bypass transit networks and save on the associated payments, but requires the two networks to be in the same physical location. Peering agreements are typically not formalized in written contracts.[8]

De-peering (or the threat thereof) might be used by the largest of networks (so-called Tier 1 networks) as a lever to attempt to compel the other party to buy transit for the use of its network. While in the core of the Internet, network operators rely on multiple interconnecting links (*i.e.* they are multi-homed), such disagreements can cause disruptions at the edges of the networks that have the disagreement as end-users typically rely on one network (*i.e.* they are single-homed). Some disagreements on peering arrangements have led network operators to seek intervention by regulatory authorities.[9] While such intervention might be beneficial in markets that are not well established and where competition is low, in well-functioning Internet markets competition should prevent persistent disagreements and the possibility of intervention to influence parties' negotiating positions runs the risk of distorting the outcomes in ways that are not beneficial (Weller and Woodcock, 2013).

4.4. Net neutrality

Network administrators who manage networks have the possibility to control, prioritise or block specific data transmissions.[10] Traffic management (*e.g.* prioritizing traffic or favouring certain packets such as voice and video from one provider or corresponding network over others) is typically used to minimise latency and allocate bandwidth on data networks so as to improve quality of service on a network. Traffic management might thus be beneficial to consumers, in particular in the presence of capacity constraints and heterogeneous consumer preferences (Cave, 2011). There is, however, debate in the commercial and technical communities as to whether future services might require guaranteed levels of quality, as opposed to the current "best effort" Internet, or whether it is more efficient and cost-effective to upgrade or manage networks in ways that address related issues (e.g. the models use for pricing services, improving interconnectivity through the use of Internet exchange points, negotiating better peering and transit relationships and so forth).[11]

However, traffic management could also potentially be employed by network administrators in an anti-competitive manner to block or disadvantage competing services.[12] This concern has spurred the so-called net neutrality debate – one of the most prominently discussed topics in Internet regulation. The term 'net neutrality' is used in many different ways, which often complicates discussions. Schuett (2010) defines net neutrality as 'the principle that all data packets on an information network (such as the Internet) are treated equally'.

8. Weller and Woodcock (2013) analysed over 140,000 Internet carrier interconnection agreements and 99.51% were 'handshake' agreements in which the parties agreed to informal or commonly understood terms (*e.g.* to exchange only routes to customer networks and to use Border Gateway Protocol (BGP) 4 for routing decisions) without creating a written document.

9. For instance, in 2005, Level 3 terminated a peering agreement with Cogent. As many of Cogent's customers had no alternative path to Level 3, their access to Level 3's customers was cut off and Cogent appealed to the Federal Communications Commission and United States Congress for intervention.

10. For a detailed discussion of the underlying technology see OECD (2007).

11. For an explanation of the difficulty of using traffic management see Huston (2012).

12. For instance, several voice-over-IP providers have complained about being blocked by mobile and fixed line operators, whose voice services are a very close substitute to voice-over-IP services. In other countries mobile operators have tried to implement surcharges for the use of messaging services, such as WhatsApp and Blackberry Messenger, which are competing with SMS.

The traffic management aspects of this issue are likely problematic only if market forces do not provide sufficient safeguards against anticompetitive behaviour by network operators. For anticompetitive effects to emerge, three conditions must be met (Crocioni, 2008):

- *First*, network operators need to have market power. If there is sufficient access competition and end-users can easily switch their Internet provider, network operators are much less likely to block or throttle certain applications or to under-provision facilities to specific networks with which they exchange substantial traffic. This is because less content and fewer applications (or poorer access to them) would reduce end-users' willingness to pay that provider for Internet access. That being said, it may not be a simple matter for a user to identify, in a network of networks, the origin of unsatisfactory performance.

- *Second*, networks would need to have an incentive to prioritise transport or provision of Internet content and applications, if they were to treat traffic differently. Examples could be, particularly for vertically integrated companies, treatment of their own traffic or that of a particular service provider over similar traffic by rivals or other corresponding networks (e.g. in the latter case strengthening their position in commercial negotiations over peering and transit with other networks).

- *Third*, they must have an incentive to exclude competitors (for instance, even a monopolist ISP may benefit from a broader range of services offered via the network to allow charging higher prices for Internet access).

The decision to apply regulation should depend on whether regulators find evidence of persistent problems with traffic prioritisation and whether market forces are unable to sufficiently protect consumers (OECD, 2007). Where such behaviour has historically occurred on fixed networks, it was typically resolved via market forces or through quick regulatory intervention.[13] On mobile networks more limitations apply, with over 90% of consumers on mobile networks in the EU facing restrictions on the use of the network (BEREC, 2012). However, to what extent significant anti-competitive problems will emerge in the future is very uncertain and intensely debated. Amidst mounting concerns over anti-competitive practices by network access providers, an increasing number of countries have held or have launched public consultations on net neutrality and some have developed guidelines or enacted legislation.[14] These include objectives such as promoting and protecting the global free flow of information or the open, distributed and interconnected nature of the Internet as set out in the OECD Council Recommendation on Principles for Internet Policy Making (OECD 2011b).

Table 2 shows the present status of regulatory obligations imposed on network access providers. Around one quarter of all countries require Internet service providers to not give precedence to some form of traffic over another and not to block the use of some applications, while another 38% of countries at

13. See for example the case that involved Madison River Communication and intervention by the Federal Communications Commission in the United States: https://apps.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf

14. For instance, the European Commission has recently launched a debate on stronger enforcement of network neutrality principles in a review of its regulatory framework for telecommunications (Kroes, 2013). This is intended to strengthen the position adopted in 2011 in which it undertook to maintain the open Internet and to ensure the maintenance of a robust 'best-effort' Internet (EC, 2011; BEREC, 2012). Brazil passed a law in early 2014 (the "Marco Civil da Internet") that, among others, aims at safeguarding net neutrality.

least recommend this practice.[15] Around 60% of the countries that do not mandate net neutrality require network access providers to disclose their network management practices to customers. This means that network access providers are required to disclose, for example, blocking or "throttling" of access to otherwise lawful applications. This is done in the hope that disclosure will bring competition to bear on the terms of those services. In around one third of the countries, network access providers are not allowed to give network bandwidth priority to content and application providers that pay for quality of service (access-tiering).[16] In one third of all countries that allow access-tiering, the regulator sets conditions for the priority setting (*e.g.* an obligation of non-discrimination).

Table 2. Many countries have regulation or guidelines on traffic management practices

In per cent of all countries that answered the question unless specified otherwise

	OECD		non-OECD		Total	
	yes	no	yes	no	yes	no
Is net neutrality required?[1]	31	69	10	90	26	74
If net neutrality is not required, is it recommended?[2]	32	68	44	56	35	65
If net neutrality is not required, are ISPs required to disclose network management practices to customers?[2]	50	50	78	22	58	42
Is access-tiering allowed?[3]	61	39	70	30	63	37
If access-tiering is allowed, does the regulator set conditions for the priority setting?[4]	33	67	14	86	28	72

1. Net neutrality is defined here as the prohibition to give precedence to some form of traffic over another and to block the use of some applications
2. In per cent of countries which do not require net neutrality; numbers do not add up to 100% because of missing values.
3. Access-tiering is defined as the granting of network bandwidth priority to content and application providers that pay for quality of service?
4. In per cent of countries which allow access-tiering; numbers do not add up to 100% because of missing values.

Source: OECD Product Market Regulation Database.

4.5. Search engines

Search engines typically generate their revenue from advertising. They either allow advertisers to have their listings ranked higher in search results for a fee or run search related ads alongside the regular search engine results and paying every time a user clicks on one of their ads. In the first half of 2012, total Internet advertising revenues in the United States amounted to USD 17 billion, of which 48% was attributed to Internet search, with 21% from display or banner advertising (PWC, 2012).

Even though it is relatively easy for users to switch to an alternative search engine, the highly concentrated nature of the search engine market has led to calls for the regulation of Internet search, because of its status as a pivotal information gatekeeper (Argenton and Prüfer, 2012). Bias in the display of results may arise from "editorial" decisions made by those running the various search engines (Goldman, 2006). Web pages may be omitted in whole or in part, while the terms associated with a particular page may be incomplete or inaccurate. Principally, these judgments are made as parameters for automated operations, the algorithms for which are kept as trade secrets, with a modest level of subsequent human intervention. Search engines also store and analyse searches, with these data being used to improve the future display of results, reinforcing market strength, since a crucial step is to be able to infer from a few

15. For two case studies on net neutrality regulation in Korea and Norway see Box 1 and Box 3 in OECD (2014). Chile, the Netherlands and Slovenia have adopted specific net neutrality legislation.

16. However, network access providers could provision more capacity to certain networks which may lead to the same result.

keywords the intention of the searcher in order to deliver the most relevant results, which is improved by access to a greater number of searches and the subsequent actions of the searchers. Among users there is often very limited understanding of how the results of a search are given the priorities displayed on the screen and how different results might be delivered.

Governments and regulators in the countries covered in this paper do not require providers of Internet search to disclose how they ranked their results. Rather, they seem to be taking the stance that the competition law is sufficiently well placed to deal with the concern of competition distortion. For instance, several investigations have been opened into the market power of Google, notably by the European Commission.[17] The US Federal Trade Commission reached a comprehensive settlement of all of its competition-related investigations of Google. It closed the investigation, finding the claim that the prominent display by Google of its own content on its general search page had a legitimate justification, while accepting a binding commitment concerning the "most problematic" practices of misappropriating or "scraping" content from rivals for use in its search results.

4.6. Cloud computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services (Box 1). Data and software are located "in the cloud" and are accessible on-demand by users more readily and more flexibly than on their own computer or server, with resources made available in the quantity and for the time required for the process they wish to execute. Cloud computing has the potential to significantly reduce the cost and complexity of doing both routine computing tasks and computationally-intensive problems. Cloud users only pay for what they need and do not have to invest in IT infrastructure that may be unused most of the time and complex to manage.

Box 1. Cloud computing

Cloud computing enables on-demand network access to a shared pool of configurable computing resources that can be rapidly delivered with minimal management effort or service provider interaction. Following the US National Institute of Standards and Technology (NIST), three main types of Cloud services can be distinguished OECD (2009):

- *Cloud Software as a Service (SaaS).* The service provided to the client is to use the provider's applications. The applications run on the provider's infrastructure and are accessible from various client devices through an interface such as a web browser. The client neither controls the underlying infrastructure nor the applications (with the possible exception of certain pre-defined configurations).
- *Cloud Platform as a Service (PaaS)*. The service provided to the client is the deployment onto the cloud of applications supported by the provider. The client does not manage or control the underlying cloud infrastructure (e.g. networks and servers), but controls the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service (IaaS).* The service provided to the client is the provision of processing, storage, network and other fundamental computing resources. With these resources the client can deploy and run a range of software, including operating systems and applications. The client does not manage or control the underlying cloud infrastructure, but has control over the operating system, storage, deployed applications, and possibly selected networking components such as firewalls.

Four different deployment models can be distinguished: In the case of *private clouds*, the cloud infrastructure is operated solely for an organization and may be managed by the organization itself or a third party on the premise of the organization or elsewhere. In the case of *community clouds*, the cloud infrastructure is shared by several organizations that have shared concerns (*e.g.* a common mission or common security requirements) and is managed by the organizations or a third party on the premises of one of the organizations or

17. Also, the Office of Fair Trading in the United Kingdom asked leading price comparison websites in 2012 to provide clear information to consumers on the way search results were presented and the identity of the business operating the website, including any commercial relationships with companies included in the comparisons.

elsewhere. In the case of *public cloud*s, the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. *Hybrid clouds* are a composition of two or more clouds (private, community, or public clouds) that remain unique entities but are bound together by standardized or proprietary technology that enables the portability of data and applications.

In the consumer sector, cloud services are either provided free of charge (e.g. social network services), with revenue generated through advertising and the sale of data on user behavior, or sold through monthly subscriptions (*e.g.* hard-drive back up). In the corporate sector, cloud services are typically sold by subscription, with the charges depending on the amount and type of services that are used. The cloud services might also be sold to firms as part of larger packages of IT services.

In terms of regulation, many countries deal with cloud computing simply by applying general data protection laws to clouds. According to the questionnaire, this is the case in EU countries as well as in Canada, Iceland, Japan and Switzerland. A few countries, namely Israel, Korea and Mexico, have put in place special regulation that specifically addresses issues related to cloud computing. Cloud computing raises a number of important questions for policy makers (OECD, 2009):

- *Data portability*: Will a single company or a small number of companies be able to achieve a dominant position in the market for cloud services over the coming years or will the cloud become an open, interoperable system where a large number of companies build and run part of an interlinked, interoperable cloud? The answer to this question will determine whether private and corporate customers will have a choice between different cloud service providers or whether they will be locked in with a particular provider. Even with a small number of providers, competition would likely be limited since proprietary formats or software make it extremely difficult for a customer to transfer the data or applications from one provider to the next. Governments thus may need to find ways to promote open, international standards for clouds that will enable users to switch between different providers at low cost and risk without imposing a particular architecture or set of standards. Countries so far do not regulate data portability. However, the European Commission has included a 'right to data portability' in Article 8 of the draft of the new data protection regulation that is supposed to replace Directive 95/46/EC. In particular, the draft regulation would grant individuals the right to obtain a copy of their profiles uploaded onto Internet platforms in a suitable format for further processing and use by themselves, and for such profiles not to contain technical or other impediments to it being subsequently uploaded onto the Internet platform of another provider (De Hert and Papakonstantinou, 2012; EC, 2012).

- *Data privacy*: Companies providing cloud services such as e-mail, social networks and virtual worlds collect vast amounts of data – much of it being sensitive, personal information – and store it in data centres around the world. Third parties might get access, either involuntarily or voluntarily, if the cloud service provider intentionally shares the data with them. Within the OECD, cloud service providers must refrain from secondary uses of the data without customers' consent in Israel, Korea, and Mexico. The same applies to EU countries based on the Directive 95/46/EC. The way in which privacy issues are addressed could be critical for the acceptance and hence deployment of cloud computing. If cloud service providers fail to earn the trust of their clients by not adopting clear and transparent policies on how their customers' data will be used, stored, and protected, governments might come under increasing pressure to regulate privacy in the cloud.

- *Data security*: If the cloud service is down for a protracted period of time or, worse, the data stored in the cloud is lost, this might cause serious damage to the companies and individuals that rely on the cloud. In many OECD countries cloud service providers are required to implement special security measures to protect the platform and the related infrastructure, either through the general data protection law or through specific laws on cloud computing. In the case of protracted

unavailability of the cloud service or the loss of data users will most likely seek recourse to the courts. An important question is thus what kind of liability a cloud service provider can be expected to assume in such cases and the jurisdiction.[18]

- *Intellectual Property and liability*: By giving users access to large computing power and storage, cloud services could facilitate the online sharing of copyrighted material. A key question is thus whether cloud service providers should be required to implement special measures to prevent these potentially illegal activities. On the one hand, a lack of protection against online piracy might slow down companies' take-up of cloud services, but on the other hand, a too onerous burden on cloud service providers in terms of security measures might make it impractical for them to provide cloud services to the general public.

- *Electronic surveillance*: Electronic surveillance is another important concern. In particular the 'Snowden' affair and new findings regarding the scale and scope of national security activities involving the Internet have triggered a heated international debate about the Internet's trustworthiness for social and economic activity.[19] In most OECD countries citizens are protected against unreasonable searches by requiring a search warrant to examine data on a person's computer. The same data might not be protected in the same way if backed up in the cloud, particularly if the cloud's data centre is in another country. Uncertainty about law enforcement surveillance (*e.g.* for taxation or national security) might lower companies' willingness to use the cloud for important functions.

- *The blurring of jurisdictions*: A more general problem of cloud computing is the mix of different jurisdictions, whereby the cloud's data centre might be located in a different jurisdiction than the users. No OECD country requires cloud service providers generally to inform the user about the jurisdiction in which the cloud is located. However, in EU countries, users must be informed if the cloud is located in a country other than the EEA and a number of jurisdictions that are deemed to provide 'adequate protection' for personal data under the European Data Protection Directive. While crafting a consistent, global approach to the regulation of clouds might considerably increase consumer trust and accelerate the adoption of cloud services, it would be extremely difficult in practice. A global self-regulatory approach based on best practices, insurance, and contract law might thus be faster and better suited to flexibly adjust as technology evolves and new services come on stream.

4.7. Social media

The use of social media (including blogs and social networking sites) is becoming pervasive from both fixed and, especially, mobile devices. More than 50% of all Internet users worldwide are using Facebook and more than 20% are using Google+, YouTube or Twitter (globalwebindex, 2013). Social networking sites (SNS) are seen as increasingly important in marketing with the logos for a variety of SNS appearing on hoardings, vans, packaging and being embedded in services, such as connected television (*e.g.* Deloitte, 2012).

As a specific type of cloud computing, social networking services are subject to some of the same regulatory issues discussed in the previous section. However, a number of additional concerns arise regarding privacy rules. For instance, users might not always be aware how much of the information they

18. OECD (2009) also points to the practical problem of tracking technical failures in the cloud and assigning responsibility for these failures.

19. Snowden's revelations have already led to some new regulations (e.g. regarding data retention) and might lead to more (e.g. regarding forced data localisation).

publish on the SNS can be seen by other users. Also, SNS providers might alter their privacy policies without giving networks users sufficient time to consent to the changes or the opportunity or to remove information that they do not want to be disclosed (Lemons, 2011). Consumer endorsements and testimonials that appear on social networking sites and blogs and other web platforms have also raised concerns (OECD, 2013b). They do not always indicate in a clear way whether they are sponsored by the providers of the products and are sometimes even inaccurate or fraudulent. In addition, there are concerns specific to younger Internet users.[20] Peer pressure encourages teenagers to use SNS, which raises safety concerns, given their still developing social and emotional competencies in self-expression, intimacy, and relationships. Particular concern has been expressed about bullying, harassment, sexual "grooming", self-harm and suicide.[21] An important question is how to protect minors from such problems. Prominent approaches being the use of co- and self-regulation, in preference to legislative solutions, for example, the European Safer Social Networking Principles. However, research has found many underage children using SNS, sometimes having given a false age to do so, and who lack the skills to use SNS safely (Livingstone *et al*., 2013).

Only a small number of the countries covered in this study have specific laws governing SNS (in additional to the application of general data protection laws). In some countries, such as Japan, Korea and Norway, guidelines have been or are being developed by governments/consumer protection enforcement agencies to protect consumers purchasing products through, notably, social media. Among OECD countries, Denmark, France, Israel, Korea and Sweden prohibit the creation of a profile or account in the name of another person (Table 3). Korea and France require the default profile settings to be those that provide the most privacy, and Korea additionally requires the SNS provider to follow special procedures to change privacy rules. The United Kingdom prohibit the registration of SNS accounts below a certain age, while France and Korea have special rules concerning private information of children (*e.g.* profiles restricted to users specifically added as 'friends' or parental consent are needed before collecting such information) and France, Israel, Korea, Sweden and Switzerland impose restrictions on the material that can be transmitted to children (*e.g.* no material that is for commercial purposes). However, France and Korea are the only OECD countries covered in this analysis that require SNS providers to verify the age of users.[22]

20. For a detailed discussion of these concerns see, for instance, Whitman (2008).

21. For a detailed discussion on the risks faced by children online and policies to protect them see OECD (2010b).

22. In the United States, which is not covered by the analysis, the Children's Online Privacy Protection Act (COPPA) requires age verification by parents.

Table 3. Regulation of social network services (SNS)

	DNK	FRA	ISR	KOR	SWE	CHE	GBR
Is a minimum age required to register an account?	no	no	no	no	no	no	yes
Are there special rules concerning private information of children?	no	yes	no	yes	no	no	no
Are there restrictions on the material that can be transmitted to children?	no	yes	yes	yes	yes	yes	no
Are SNS providers required to verify the age of users?	no	yes	no	yes	no	no	no
Do SNS providers have to follow a special procedure to change privacy rules?	no	no	no	yes	no	no	no
Do default profile settings have to be those that provide the most privacy?	no	yes	no	yes	no	no	no
Is creating a SNS site in someone else's name without their permission prohibited?	yes	yes	yes	yes	yes	no	no

Source: OECD Product Market Regulation Database.

4.8. Data privacy protection

The protection of data privacy has become a major concern for policy makers in OECD countries, fuelled by the emergence of the 'data-rich economy' for which personal data act as an important resource. Personal data has emerged as a new asset class, with companies deriving value from it by creating new forms of interactions and personalised services, targeting advertising or geo-localised services to help match supply and demand, trading and sharing personal data with third parties to merge disparate data sets together, or generating new insights about individuals through profiling and from exploiting advanced predictive analytical tools with large data sets (*e.g.* Acquisiti 2010). As pointed out by Luchetta (2013), the companies that collect personal data are very diverse and are often subject to different regulations (*e.g.* banks may face stricter regulations regarding the use of (non-sensitive) personal information than Google or Facebook), which risks distorting competition.

In regulating the protection of personal data policy-makers have to strike a balance between these commercial interests of companies and the interests of individuals.[23] Trust in the technology and in the way personal data are used by companies might be a key enabler of the new information-rich economy (Irion and Luchetta, 2013). Worries about privacy have been shown negatively to impact e-commerce and online services (*e.g.* Eurostat, 2009; Pew, 2012) and consumers and users still seem to lack assurance about the use of their personal information.[24] For instance, in the 2011 Eurobarometer survey, 70% of the respondents said that they are concerned by how their data are used and about 75 to 80% said that they do not feel in control of the data they disclose online. The trust in Internet companies was very low, at 22% (EC, 2011).

The data collected for this study shows that almost all countries have provisions and institutions in place for data protection (Table 4). Typically the privacy rules are those generally applicable to all data processing, irrespective of whether the data are processed online or offline. Almost all countries covered

23. In addition to depriving companies of lucrative business models, data protection also entails sizable compliance costs. Estimates suggest that companies with more than 1000 employees spend up to EUR 2.5 million per year to comply with EU privacy laws (Ponemon Institute, 2011).

24. The study by Berendt *et al*. (2005), however, which summarizes the results from a large-scale online shopping experiment, indicates that online users may easily forget about their privacy concerns and communicate even very personal details without any compelling reason to do so.

have a law that specifies the purposes for which personal data can be used by Internet service and application providers. While some laws list concrete purposes such as subscriber billing and interconnection payments, others are rather general, referring for instance to 'lawful purposes' and leaving it up to the data controllers to translate this into more concrete terms. Around two-thirds of the countries also specify the maximum time period for which personal data can be stored by Internet service and application providers. 40% of these countries define this period as being 'no longer than necessary for legitimate purposes, while 60% specify a precise time period. The typical length of this period is six or twelve months (notable exceptions being Estonia with one month, Malta with two years and Korea with three years). In 90% of the countries, Internet service and application providers have to inform users about the type of personal data collected and the purpose for which the data are used. In about half of them they also need to inform users about the duration of data storage. More than two thirds of the countries require Internet service and application providers to seek the consent of the user before storing personal data. In around three-quarters of the countries users have the right to request, at any time, the deletion of personal data and the omission of the use of certain personal data. The right to demand rectification of errors in certain personal data exists in around 88% of all countries covered by the analysis. Around 75% of the countries require Internet service and application providers to implement special technical or organisational measures to ensure the security of personal data (*e.g.* to prevent data theft and loss). In most cases, the laws are rather vague in order to leave the choice of the precise security measure up to the providers. Not specifying concrete technical requirements in the laws avoids the risk of the laws getting out of date very quickly. In 20% of the countries the government is aware of voluntary protection by Internet service and application providers that go beyond those provided under existing laws and regulations.

In EU countries, the laws and regulations governing personal data protection are framed by a number of directives (the cross-country variations apparent from Table 4 might be due to differences in implementation). The Data Protection Directive (95/46/EC, currently under revision) provides that personal data must be processed fairly and lawfully and be collected for specified, explicit and legitimate proposes and not further processed in a way incompatible with those purposes (Art. 6). The legitimacy of data processing is based on six alternative legal grounds, of which the individual's unambiguous consent to the data processing is one possibility (Art. 7). Individuals also have several other rights in relations to their data, such as the comprehensive right of access concerning all matters of personal data processing (Art. 12), the right to demand rectification, erasure or blocking of the data (Art. 12), and the right to object, which can pre-empt certain legitimate bases for data processing and, in particular, the use of personal data in direct marketing (Art. 14). The e-privacy Directive (2002/58/EC), as amended by Directive 2009/136/EC, regulates electronic communications and, for instance, allows the processing of traffic and location data (which are increasingly used by mobile apps when offering geo-localised services such as maps or information about nearby shops and restaurants) if the subscriber has given his/her consent.

Table 4. Most countries have provisions for the treatment of personal data by ISPs and CAPs

In per cent of all countries that answered the question

	OECD		non-OECD		Total	
	yes	no	yes	no	yes	no
Is there a law that specifies the purposes for which personal data can be used?	91	9	100	0	93	7
Does a law specify the maximum time period for which personal data can be stored?	64	36	70	30	65	35
Must users be provided with the following information?						
Types of personal data collected	94	6	78	22	90	10
Duration of data storage	55	45	75	25	59	41
Uses to which the data are put	94	6	78	22	90	10
Must the user's consent be obtained before personal data can be stored?	81	19	70	30	78	22
Do users have the right by law to request, at any time, the following actions?						
Deletion of certain personal data	70	30	80	20	72	28
Rectification of certain personal data	91	9	70	30	86	14
Omission of the use of certain personal data	73	27	70	30	72	28
Do special technical or organisational measures have to be implemented to ensure data security?	79	21	78	22	79	21

Source: OECD Product Market Regulation Database.

The tracking of online consumer behaviour is another wide-spread concern. Thanks to the development of new technologies such as Deep Packet Inspection (DPI) it has become possible to access IP packets in real time as they are travelling through the Internet. This allows compiling lists of the webpages that users visit, the links they click on, and the key words they type into the search bar of search engines. This information is often shared by businesses with third parties for commercial purposes including online advertising. While customized ads might offer benefits for consumers, the tracking, collection and use of their data, often without their knowledge and/or their consent, may raise privacy concerns. The survey suggests that currently slightly more than 60% of the countries covered by the analysis regulate online user tracking (Table 5). In virtually all countries that do regulate user tracking companies have to inform users that they gather information about their browsing behaviour and about the purpose of data collection (*e.g.* behavioural advertising). 21 out of the 26 countries with tracking regulation require companies to seek the consent of users before tracking their browsing behaviour (opt-in) and in another 2 countries users must have the possibility to (persistently) opt out of the data collection process. In around two-thirds of the countries collected data must be deleted or 'rendered anonymous' after a certain period of time.

Table 5. Regulation of online user tracking

In per cent of all countries that regulate online user tracking

	OECD	non-OECD	Total
Do companies have to inform users that they gather information about browsing behaviour?			
yes	91	100	92
no	0	0	0
Do companies have to inform users about the purpose of data collection?			
yes	91	100	92
no	5	0	4
Must companies seek the consent of users before tracking browsing behaviour?			
yes	82	67	80
no	18	33	20
Must users have the possibility to (persistently) opt out of the data collection process?			
yes	38	50	40
no	23	0	20
Must collected data be deleted or 'rendered anonymous' after a certain time?			
yes	55	100	60
no	36	0	32

Note: Numbers might not add up to 100% because of missing values.

Source: OECD Product Market Regulation Database.

4.9. Data retention

A growing body of legislation requires or obliges the processing and storage of personal data, *e.g.* for the prosecution of criminal offences (Table 6). In around 85% of the countries Internet service providers are obliged to retain certain traffic data, including IP addresses.[25] The question of the time period for which data may be held can be subject to a specific legal measure, but in some countries there can be different obligations, for example, for the retention of traffic data for law and order purposes and to have sufficient data to be able to respond to customer complaints and litigation, which may be much longer. Within the EU the Data Retention Directive (2006/24/EC) harmonises member states' obligations to retain certain data for law enforcement purposes. It defined sets of traffic and location data that have to be retained for periods between 6 months and 2 years, but does not specify the legal requirements under which these data can be accessed. The European Court of Justice recently declared the Data Retention Directive to be invalid, arguing that it interferes with the fundamental rights to respect for private life and to the protection of personal data (Art. 8 of the European Charter on Human Rights).

25. In addition, Norway has passed a law in parliament requiring the retention of certain traffic data for 6 months in line with the EU data retention Directive, but the law is not yet in force.

Table 6. Maximum period for which ISPs have to retain certain traffic data

In months

Country	Period	Country	Period	Country	Period
Australia	36	Iceland	6	Spain	12
Austria	6	Ireland	12 - 24	Sweden	6
Belgium	36	Italy	12	Switzerland	6
Chile	6	Korea	3 - 12	Turkey	12
Czech Republic	6	Luxembourg	6	Bulgaria	12
Denmark	12	Netherlands	6	Croatia	12
Estonia	12	Poland	12	Latvia	18
France	12	Portugal	12	Malta	12
Greece	12	Slovakia	6 - 12	Romania	6
Hungary	12	Slovenia	14	Russia	36[1]

Source: OECD Product Market Regulation Database.

4.10. Consumer protection

The Internet economy has also raised issues about consumer protection, both at a general level (*e.g.* which content can be viewed online) and with respect to specific activities such as e-commerce, online banking, spamming and online user tracking.[26] According to the survey, most countries force search engine providers to edit the search results to filter out certain material such as links to sites inappropriate for children or intended to defraud consumers and a bit more than half outright prohibit certain websites (*e.g.* websites that promote child abuse and pornography, suicide, drug use, racism, violence or gambling). Examples of prohibited website content include child abuse and pornography (12 countries), the promotion of suicide (*e.g.* Australia, Turkey, the United Kingdom and Russia) or drug use (*e.g.* Russia), the promotion of racism (*e.g.* France, Italy and Lithuania) and violence (*e.g.* New Zealand and Lithuania) and gambling (*e.g.* Belgium, Korea and Turkey).

Apart from general regulations of content, consumer protection issues arise with respect to specific online transactions, such as e-commerce and online banking. E-commerce has expanded rapidly over the past decade. In the OECD area, the average proportion of consumers purchasing products via e-commerce increased from about 25% of individuals in 2007 to 32% in 2011 (OECD, 2013c).[27] In light of this, many countries have passed laws that specially deal with e-commerce transactions (e.g. the E-commerce Directive, 2000/31/EC). Slightly more than half of the countries which answered the survey questions about e-commerce said that they have legal protections that specifically cover e-commerce transactions and go beyond general consumer protection rules (Table 7). Almost 90% of these e-commerce laws deal with the ordering and confirmation process, around 80% of them address information disclosures about the business, the goods or services and the transaction, and a bit more than 70% of them cover business, advertising and/or marketing practices. Issue relating to payment, dispute resolution and redress as well as privacy are covered somewhat less frequently. One third of the countries restrict the types of goods and

26. See OECD (2013a) for a discussion of policies to empower and protect consumers in the purchase of digital content products and OECD (2012) for a discussion of policy issues related to e-commerce payment systems.

27. E-commerce is also on the rise in some emerging market economies. In China, for example, the volume of online sales increased from about EUR 16 billion in 2008 to about EUR 94 billion in 2011. This represents an average growth rate of more than 80% a year."

services that can be sold online, prohibiting for instance the online sale of medical products, alcohol or tobacco.

Table 7. Some e-commerce provisions are more common that others

Issues addressed in per cent of all countries with specific e-commerce laws

	OECD		non-OECD		Total	
	yes	no	yes	no	yes	no
Business, advertising and/or marketing practices	67	33	100	0	71	29
Information disclosures about the business	75	25	100	0	78	22
Information disclosures about the goods or services	71	29	100	0	75	25
Information disclosures about the transaction	81	19	100	0	83	17
Ordering and confirmation process	85	15	100	0	87	13
Payment	60	40	67	33	61	39
Dispute resolution and redress	58	42	67	33	59	41
Privacy	53	47	0	100	48	52

Source: OECD Product Market Regulation Database.

In one third of the countries the level of domestic legal protection provided to consumers who buy physical goods via e-commerce is lower than the protection provided when the goods are bought elsewhere (*e.g.* by mail or at a retail store), while in two thirds of the countries the protection is generally higher if the good is bought via e-commerce (Table 8). For the online subscription to services or the purchase thereof protection is higher in only half the countries. In almost all countries, consumers have a statutory right to return physical goods purchased through e-commerce under certain conditions, for a full or partial refund, or to cancel services purchased through e-commerce (the exceptions in the OECD are Iceland, Mexico, New Zealand (for services), the Slovak Republic and Switzerland). In one third of the countries, companies (including payments providers, merchants and e-commerce platform providers) 'fairly frequently' provide voluntary consumer protection in e-commerce purchases of physical goods beyond those required by law, and in another 40% of the countries this is at least 'sometimes' the case. For the online purchase of services, voluntary protections are slightly less common, at respectively 21% ('fairly frequently') and 41% (sometimes). Examples of voluntary protections include a lengthening of period to return the good or service, dispute resolution mechanisms, and shorter delivery deadlines than those foreseen by law.

Table 8. Consumer protection in e-commerce transactions

In per cent of all countries that answered the question

	Goods			Services		
	OECD	non-OECD	Total	OECD	non-OECD	Total
What is the level of legal protection for e-commerce purchase relative to traditional purchases?						
higher	70	20	63	60	20	54
lower	27	80	34	33	80	40
same	3	0	3	7	0	6
depends	0	0	0	0	0	0
Do consumers have a statutory right to return goods/services purchased through e-commerce?						
yes	87	88	87	87	88	87
no	13	13	13	13	13	13
Do businesses provide any voluntary consumer protection in e-commerce purchases beyond those required by law?						
fairly frequently	38	20	35	24	0	21
sometimes	38	40	39	36	75	41
rarely or not at all	23	40	26	40	25	38

Note: In the first question, 'higher' means that protection is generally higher if the good or service is bought via e-commerce, 'lower' means that protection is generally lower if the good or service is bought via e-commerce, 'same' means that protection is the same, irrespective of how the good or service is bought, and 'depends' means that protection is higher in some cases and lower in others.

Source: OECD Product Market Regulation Database.

An interesting question regarding consumer protection in e-commerce transactions relates to the international dimension of its enforcement. According to the questionnaire, consumer protection enforcement agencies typically have the authority to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers and to share investigative information with foreign consumer protection enforcement agencies (Table 9). In particular the authority to share information with foreign agencies is however often only granted for certain cases.

Table 9. Consumer protection agencies and e-commerce transactions

In per cent of all countries that answered the question

	OECD	non-OECD	Total
Do consumer protection enforcement agencies have the authority to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers in e-commerce transactions?			
in all cases	66	80	68
in some cases	31	20	29
No	3	0	3
Do consumer protection enforcement agencies have the authority to share investigative information with foreign consumer protection enforcement agencies, with respect to e-commerce transactions?			
in all cases	41	40	41
in some cases	45	60	47
No	14	0	12

Source: OECD Product Market Regulation Database.

One special category of e-commerce is online banking, which has shown significant growth over the past decade. A number of different approaches have evolved for authentication for online banking, from

the use of passwords to two-part encryption systems.[28] The different approaches taken by regulators in the OECD countries are shown in Table 10. At the simplest level, a customer can authenticate themselves to some banks or for some functions with a password. One third of the countries consider this insufficiently secure. Among these countries, about half prescribe a specific alternative authentication procedure for online banking such as two-factor authentication) of a digital signature, for which a minimum level of complexity may be specified (*e.g.* the length of the cryptographic key). Only four OECD countries (Greece, Italy, Luxembourg and Portugal) specify the minimum size of cryptographic keys that financial service providers need to use for online transactions.

Table 10. Regulation of online banking

In per cent of all countries that answered the question

	OECD	non-OECD	Total
Is password-based single-factor authentication ruled to be an inadequate authentication procedure? (share of all countries that answered the question)			
yes	34	40	36
no	66	60	64
Do laws or regulations prescribe a specific alternative authentication procedure? (share of all countries that answered 'yes' to the previous question)			
yes	56	25	46
no	44	75	54
Do laws or regulations specify the minimum size of cryptographic keys that financial service providers need to use for online transactions? (share of all countries that answered the question)			
yes	19	11	17
no	81	89	83

Source: OECD Product Market Regulation Database.

Electronic spam or unsolicited commercial email (UCE) is another area of the Internet economy that many countries have regulated over the past 10 to 15 years.[29] While spam is an extremely cost-effective way of advertising for those who generate it, it creates sizable costs for ISPs for filtering and virus-checking systems, handling customer complaints and wasted network bandwidth and storage capacity (*e.g.* Munukutla-Parker, 2006). Most OECD and non-OECD countries have made the sending of spam illegal, meaning that prior consent of the recipient must be obtained before unsolicited commercial email be sent to a person. For EU countries, the 2002 e-privacy Directive requires prior consent unless the person's contact details were obtained within the context of an existing customer relationship.[30] Countries that do not outright prohibit spam emails include Brazil, Chile, Korea, Mexico, and Turkey.[31] Brazil, Chile and Korea require special labelling of spam emails, and Korea additionally requires that recipients have the ability to opt out of future emails (Table 11). A practical constraint for developing anti-spam policy is that

28. For a more extensive discussion of policy issues related to e-commerce payment systems see OECD (2012). The report identifies five issues that policy makers may need to address to strengthen consumer confidence in new and emerging e-commerce payment systems: clarity, transparency and completeness in information disclosure, variability in regulatory and protection regimes, fraudulent, misleading and deceptive commercial practices, dispute resolution and redress, and security and interoperability.

29. For an overview of early anti-spam regulations see OECD (2005).

30. An 'existing customer relationship' in this context would not only exist between the customer and the company with which the customer has concluded a transaction, but also with third parties in case the customer has given consent to share his/her data with third parties.

31. While Canada did not yet prohibit spam emails on 1 January 2013 (the date to which the Internet regulation database refers), the Canadian Anti-spam Law (CASL) came into force on 1 July 2014 and the sending of commercial electronic messages is since then prohibited without the recipient's consent.

a substantial portion of received spam crosses international boarders, thus necessitating international co-operation successfully to fight UCE (OECD, 2006).

Table 11. Regulation of spam emails in countries without an outright prohibition

In per cent of all countries that answered the question

	Are there special restrictions on spam emails?	Is special labelling required?	Must recipients have the ability to opt out of future emails?	Must the physical address of the sender be included in the email?
CHL	yes	yes	no	no
KOR	yes	yes	yes	.
BRA	yes	yes	no	no

Note: A dot means that the country did not answer the question.

Source: OECD Product Market Regulation Database.

5. Conclusions

This paper reviews some of the main regulatory challenges brought about by the rapid development of the Internet and the digital economy. In addressing these challenges, governments need to reconcile competition objectives with the need to preserve the capacity of the Internet to develop and stimulate innovation, while ensuring that consumers, enterprises and citizens are adequately protected against fraudulent behaviour and breach of privacy. The task of regulating the Internet is further complicated by the multitude of players, activities and media involved as well as by the rapid shifting of the economic and technological landscape and the virtual absence of geographical boundaries.

Against this background, the paper takes stock of existing regulations in OECD and selected non-OECD countries in specific areas related to the Internet and the digital economy. Despite the challenges, it finds that the internet is far from being a "regulation-free" space as there are various industry standards, co-regulatory agreements between industry and the government, and in some cases also state regulation. For instance, many countries have put internet-specific legislation in place to protect personal data and consumers more generally (*e.g.* in e-commerce transactions). On the other hand, only few countries are regulating specific applications such as search engines, cloud computing and social networks through special laws.

The generally cautious approach taken by governments with respect to the regulation of the Internet is understandable considering the novelty of some of the main challenges and the difficulty in identifying good practices, let alone best ones. The information presented in this paper on the various regulatory approaches may provide useful input in on-going and future efforts to understand the role and impact of regulation on the development of the Internet and thereby help identify good practices.

BIBLIOGRAPHY

Acquisiti, A. (2010), The Economics of Personal Data and the Economics of Privacy" Background paper #3 for the Joint WPISP-WPIE Roundtable on the Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines. http://www.oecd.org/sti/ieconomy/46968784.pdf

Argenton, C. & J. Prüfer (2012), "Search Engine Competition with Network Externalities", Journal of Competition Law & Economics, Vol. 8, No. 1, pp. 73-105.

BEREC (2012), "BEREC Has Adopted Two Summaries and the Updated Reports on Net Neutrality", 10 December. http://berec.europa.eu/eng/news_consultations/whats_new/1281-berec-has-adopted-two-summaries-and-the-updated-reports-on-net-neutrality

Berendt, B., O, Günther and S. Spiekermann (2005), Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. Communication of the ACM (CACM), Vol. 48, No. 3, pp. 101-106.

Buccirossi P., L. Ciari, T. Duso, G. Spagnolo and C. Vitale (2013), "Competition Policy and Productivity Growth: An Empirical Assessment", The Review of Economic and Statistics, Vol. 95(4), pp. 1324–1336.

Cave, M. (2011), "Competition and Consumer Protection Issues in the Net Neutrality Debate, with Special Reference to Europe", http://www.oecd.org/regreform/sectors/48848979.pdf.

comScore (2013), comScore Releases December 2012 U.S. search engine rankings. http://www.comscore.com/Insights/Press_Releases/2013/1/comScore_Releases_December_2012_U.S._Search_Engine_Rankings.

Crocioni, P. (2008), "Leveraging of Market Power in Emerging Markets: A Review of Cases, Literature, and a Suggested Framework" Journal of Competition Law & Economics, Vol. 4, No. 2, 449-534.

De Hert, P. and V. Papakonstantinou (2012), "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", Computer Law & Security Review, Vol. 28, pp. 138-142.

Deloitte (2012). "Connected TV: Hits and Misses", https://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/TMT%20Predictions%202013%20PDFs/dttl_TMT_Predictions2013_ConnectedTV.pdf.

EC (2011), The Open Internet and Net Neutrality in Europe. COM (2011) 222. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0222:EN:NOT.

EC (2012), Impact Assessment on the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). SEC(2012) 72. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

EC (2013), Green Paper, "Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values". Brussels: European Commission. COM (2013) 231. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013DC0231:EN:NOT.

Eko, L. (2010), "American Exceptionalism, the French Exception, Intellectual Property Law, and Peer-to-Peer File Sharing on the Internet" John Marshall Review of Intellectual Property Law, Vol. 10, No. 1, 95-153.

Eurostat (2009), Internet usage in 2009 - Households and Individuals, Data in Focus 46/2009 http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-046/EN/KS-QA-09-046-EN.PDF.

Evans, D. (2011), "Some Remarks on Net Neutrality and The Evolution Of The Internet-Economy", http://www.oecd.org/regreform/sectors/48848964.pdf.

Globalwebindex (2013), "SOCIAL PLATFORMS GWI.8 UPDATE: Decline of Local Social Media Platforms" https://www.globalwebindex.net/social-platforms-gwi-8-update-decline-of-local-social-media-platforms/

Goldman E. (2006), "Search Engine Bias and the Demise of Search Engine Utopianism", Yale Journal of Law and Technology, Vol. 8, pp. 188-200.

Huston, G. (2012), Inductee Into the Internet Hall of Fame and Writer Of Two Books on Traffic Management, https://ripe65.ripe.net/presentations/67-2012-09-25-qos.pdf.

Irion, K. and G. Luchetta (2013), "Online personal data processing and EU data protection reform" CEPS Task Force Report of the CEPS Digital Forum, http://ssrn.com/abstract=2275267.

Kroes, N. (2013), "Net neutrality – Safeguarding the Open Internet for All", 5 June 2013. http://blogs.ec.europa.eu/neelie-kroes/net-neutrality/ and http://europa.eu/rapid/press-release_SPEECH-13-498_en.htm.

Lemons, R. (2011), "Protecting Our Digital Walls: Regulating the Privacy Policy Changes Made by Social Networking Websites", Journal of Law and Policy for the Information Society, Vol. 6, No. 60.

Livingstone S., K. Ólafsson and E. Staksrud (2013), "Risky Social Networking Practices Among 'Underage' Users: Lessons for Evidence-Based Policy", Journal of Computer-Mediated Communication, 18 (3) 303-320.

Luchetta, G. (2013), "Is the Google Platform a Two-Sided Market?" *Mercato Concorrenza Regole*, Vol. 15, No. 1, pp. 85-118.

Munukutla-Parker, U. (2006), "Unsolicited Commercial E-Mail, Privacy Concerns Related to Social Network Services, Online protection of Children and Cyberbullying" I/S: A Journal of Law and Policy for the Information Society, Vol. 2, No. 3, pp. 627-650. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/h-parker.pdf

OECD (2005), "Anti-Spam Regulation", Paris: Organisation for Economic Cooperation and Development, http://www.oecd.org/Internet/ieconomy/35670414.pdf.

OECD (2006), "Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Against Spam". http://www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm.

OECD (2007), Internet Traffic Prioritization: An Overview, DSTI/ICCP/TISP(2006)4/FINAL.

OECD (2008), "Resolution of the Council on the Seoul Declaration for the Future of the Internet economy.

OECD (2009), Briefing Paper for the ICCP Technology Foresight Forum: Cloud Computing and Public Policy, Organisation for Economic Co-operation and Development, DSTI/ICCP(2009)17, September 29, 2009. http://www.oecd.org/sti/ieconomy/43933771.pdf.

OECD (2010a), *The Economic and Social Role of Internet Intermediaries*, Paris: OECD Publishing, http://www.oecd.org/internet/ieconomy/44949023.pdf.

OECD (2010b), "The protection of children online - Risks faced by children online and policies to protect them", http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/iccp/reg (2010)5/final&doclanguage=en.

OECD (2011a), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, Paris: OECD Publishing, http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm.

OECD (2011b), "OECD Council Recommendation on Principles for Internet Policy Making", http://www.oecd.org/sti/ieconomy/49258588.pdf.

OECD (2012), "Report on Consumer Protection in Online and Mobile Payments", *OECD Digital Economy Papers*, No. 204, OECD Publishing.

OECD (2013a), "Protecting And Empowering Consumers in the Purchase of Digital Content Products", *OECD Digital Economy Papers*, No. 219, OECD Publishing.

OECD (2013b), "Consumer Protection and Empowerment in Participative E-Commerce", DSTI/CP(2013)6/REV1.

OECD (2013c), *The Internet Economy on the Rise: Progress since the Seoul Declaration*, Paris: OECD Publishing.

OECD (2014), "Building Blocks for Smart Networks", *OECD Digital Economy Papers*, No. 215, OECD Publishing.

Pew Research Center (2012), "Privacy and Data Management on Mobile Devices", http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

Ponemon Institute (2011), "The True Cost of Compliance – A Benchmark Study of Multinational Organisations", http://www.tripwire.com/tripwire/assets/File/ponemon/True_Cost_of_Compliance_Report.pdf.

PWC (2012), "IAB Internet Advertising Revenue Report", New York: Internet Advertising Board. http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_HY_2012.pdf.

Schuett, F. (2010), "Network Neutrality: a Survey of the Economic Literature" *Review of Network Economics* 9 (2) article 1.

Weiser, P. J. (2009), "The Future of Internet Regulation", *mimeo*.

Weller D. and B. Woodcock (2013), "Internet Traffic Exchange: Market Developments and Policy Challenges", *OECD Digital Economy Papers*, No. 207, OECD Publishing.

Whitman, M. (2008), "Is MySpace a Good Kids' Space? A Look at the Implications of the January 2008 MySpace-Attorneys General Agreement Concerning Online Age Verification", Journal of Law and Policy for the Information Society, Vol. 4, pp. 727-749.

ANNEX

Table A1. Coverage rate of the Internet regulation database

In percent

	OECD	Non-OECD
Wholesale access to fixed line networks		
Are access to and use of the fixed-line network mandated for Internet traffic?	100	40
Are wholesale access prices to the fixed-line network regulated for Internet traffic?	100	40
Is local loop unbundling mandated?	100	100
Are local loop unbundling prices regulated?	100	100
Wholesale access to mobile networks		
Are access to and use of the mobile network mandated?	100	40
Are wholesale access prices to the mobile network regulated?	100	40
Net neutrality		
Is net neutrality required?	97	100
If net neutrality is not required, is it recommended?	97	100
If net neutrality is not required, are ISPs required to disclose network management practices to customers?	97	100
Is access-tiering allowed?	94	100
If access-tiering is allowed, does the regulator set conditions for the priority setting?	88	100
Search engines		
Do Internet search engine providers have to disclose to their customers how rankings are established?	79	80
Cloud computing		
Is cloud computing regulated?	97	80
If yes, are cloud service providers required to inform the user about the jurisdiction in which the cloud is located?	94	80
If yes, are cloud service providers required to implement special security measures to protect the platform and the related infrastructure?	94	80
If yes, must cloud service providers refrain from secondary uses of the data without customer's consent?	91	80
Social media		
Are social network services (SNS) regulated?	100	90
If yes, is a minimum age required to register an account?	100	90
If yes, are there special rules concerning private information of children (e.g. profiles restricted to users specifically added as 'friends' or parental consent needed before collecting such information)?	100	90
If yes, are there restrictions on the material that can be transmitted to children (e.g. no material that is for commercial purposes)?	100	90
If yes, are SNS providers required to verify the age of users?	100	90
If yes, do SNS providers need to follow a special procedure to change privacy rules?	100	90
If yes, must default profile settings be those that provide the most privacy?	100	90
If yes, is creating a social networking site in someone else's name without their permission prohibited?	100	90
Privacy protection		
Is there a law that specifies the purposes for which personal data can be used by Internet service and application providers?	100	90
Does a law specify the maximum time period for which personal data can be stored by Internet service and application providers?	100	100
Do Internet service and application providers have to provide users with the following information? - Types of personal data collected	100	90
Do Internet service and application providers have to provide users with the following information? - Duration of data storage	97	80
Do Internet service and application providers have to provide users with the following information? - Uses to which the data are put	100	90

Table A1. Coverage rate of the Internet regulation database (cont.)

In percent

	OECD	Non-OECD
Do Internet service and application providers need to seek the consent of the user before storing personal data?	100	100
Is there a law or regulation that gives users the right to request, at any time, the following actions from Internet service and application providers? - Deletion of certain personal data	100	100
Is there a law or regulation that gives users the right to request, at any time, the following actions from Internet service and application providers? - Rectification of certain personal data	100	100
Is there a law or regulation that gives users the right to request, at any time, the following actions from Internet service and application providers? - Omission of the use of certain personal data	100	100
Are Internet service and application providers required to implement special technical or organizational measures to ensure the security of personal data?	100	90
If yes, please specify these measures.	88	70
Do Internet service and application providers offer any voluntary protection of personal data that goes beyond that provided under existing laws and regulations?	67	40
If they do, please describe the most frequent types of voluntary protection of personal data.	61	40
Is online user tracking regulated?	97	90
If yes, do companies have to inform users that they gather information about their browsing behaviour?	94	90
If yes, do companies have to inform users about the purpose of data collection (e.g. behavioural advertising)?	94	90
If yes, do companies have to seek the consent of users before tracking their browsing behaviour (opt-in)?	97	90
If yes, do users have to have the possibility to (persistently) opt out of the data collection process?	79	80
If yes, does the collected data have be deleted or 'rendered anonymous' after a certain period of time	91	90
Data retention		
Are Internet service providers obliged to retain certain traffic data (e.g. for the prosecution of criminal offences)?	97	100
If yes, what types of traffic data need to be retained?	85	70
If yes, for how long do these data have to be retained (maximum period in months)?	85	70
Consumer protection		
Is there any regulation that forces search engine providers to edit content provided in the results in order to filter out certain material such as links to sites inappropriate for children or intended to defraud consumers?	88	80
Are certain web sites prohibited (e.g. sites that promote suicide)?	94	90
If yes, which types of sites are prohibited?	91	80
Are there any domestic legal protections that specifically cover e-commerce transactions (e.g. purchases made online or via mobile platforms) and that go beyond general consumer protection rules?	97	70
If yes, do these laws address business, advertising and/or marketing practices?	97	70
If yes, do these laws address information disclosures about the business?	94	70
If yes, do these laws address information disclosures about the goods or services?	97	70
If yes, do these laws address information disclosures about the transaction?	97	70
If yes, do these laws address the ordering and confirmation process?	94	70
If yes, do these laws address payment?	94	70
If yes, do these laws address dispute resolution and redress?	91	70
If yes, do these laws address privacy?	91	60
Are there restrictions on the types of goods and services that can be sold online?	94	50
If yes, which goods and services may not be sold online?	91	50
Does the level of domestic legal protection provided to consumers who buy physical goods via e-commerce differ from the protection provided when the goods are bought elsewhere (e.g. by mail or at a retail store)?	94	60

Table A1. Coverage rate of the Internet regulation database (cont.)

In percent

	OECD	Non-OECD
Does the level of domestic legal protection provided to consumers who buy or subscribe to e-commerce services differ from the level of protection provided when the services are bought or subscribed to by other means?	94	60
Do consumers have a statutory right to return physical goods purchased through e-commerce under certain conditions, for a full or partial refund?	91	80
Do consumers have a statutory right to cancel services purchased through e-commerce under certain conditions, for full or partial refund?	91	70
Do businesses (including payments providers, merchants and e-commerce platform providers) provide any voluntary consumer protection in e-commerce purchases of physical goods beyond those required by law?	82	60
If they do, please describe the most frequent types of voluntary consumer protection.	70	60
Do businesses (including payments providers, merchants and e-commerce platform providers) provide any voluntary consumer protection in e-commerce purchases of services beyond those required by law?	76	40
If they do, please describe the most frequent types of voluntary consumer protection.	64	40
Do consumer protection enforcement agencies have the authority to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers with respect to e-commerce transactions?	91	50
Do consumer protection enforcement agencies have the authority to share investigative information with foreign consumer protection enforcement agencies, with respect to e-commerce transactions?	88	50
Is password-based single-factor authentication ruled to be an inadequate authentication procedure for online banking?	88	90
If yes, do laws or regulations prescribe a specific alternative authentication procedure for online banking (e.g. two-factor authentication)?	85	90
Do laws or regulations specify the minimum size of cryptographic keys that financial service providers need to use for online transactions?	82	80
Are spam emails prohibited?	100	90
If spam emails are not prohibited, are there special restrictions on spam emails?	97	80
If yes, is special labelling required?	97	80
If yes, do recipients have to have the ability to opt out of future emails?	97	80
If yes, does the physical address of the sender have to be included in the email?	94	80

WORKING PAPERS

The full series of Economics Department Working Papers can be consulted at www.oecd.org/eco/workingpapers

1170. *A revival of the private rental sector of the housing market? Lessons from Germany, Finland, the Czech Republic and the Netherlands*
(October 2014) by Rik de Boer and Rosamaria Bitetti

1169. *Secular stagnation: evidence and implications for economic policy*
*(*October 2014) by Łukasz Rawdanowicz, Romain Bouis, Kei-Ichiro Inaba and Ane Kathrine Christensen

1168. *Investment gaps after the crisis*
(October 2014) by Christine Lewis, Nigel Pain, Jan Strasky and Fusako Menkyna

1167. *Factors behind the decline in real long-term government bond yield*
(October 2014) by Romain Bouis, Kei-Ichiro Inaba, Łukasz Rawdanowicz and Ane Kathrine Christensen

1166. *The effect of the global financial crisis on the OECD potential output*
(October 2014) by Patrice Ollivaud and David Turner

1165. *Determinants of households' investment in energy efficiency and renewables – evidence from the OECD Survey on household environmental behaviour and attitudes*
(October 2014) by Nadia Ameli and Nicola Brandt

1164. *Addressing high household debt in Korea*
(September 2014) by Randall S. Jones and Myungkyoo Kim

1163. *Reducing the high rate of poverty among the elderly in Korea*
(September 2014) by Randall S. Jones and Satoshi Urasawa

1162. *Promoting the financing of SMEs and start-ups in Korea*
(September 2014) by Randall S. Jones and Myungkyoo Kim

1161. *Fostering inclusive growth by promoting structural change in the business sector*
(September 2014) by Rauf Gönenç, Oliver Röhn, Vincent Koen and Fethi Öğünç

1160. *Reducing macroeconomic imbalances in Turkey*
(September 2014) by Oliver Röhn, Rauf Gönenç, Vincent Koen and Evren Erdoğan Coşar

1159. *Reinvigorating the EU Single Market*
(September 2014) by Jean-Marc Fournier.

1158. *An exploration of the determinants of the subjective well-being of Americans during the great recession*
(August 2014) by Aida Caldera Sánchez and Caroline Tassot.

1157. *Boosting the development of efficient SMEs in the Netherlands*
(September) by Rafał Kierzenkowski and Jochebed Kastaneer

1156. *Making the banking sector more resilient and reducing household debt in the Netherlands*
(September 2014) by Rafał Kierzenkowski, Olena Havrylchyk and Pierre Beynet

1155. *US long term interest rates and capital flows to emerging economies*
(July 2014) by Eduardo Olaberria

1154. *Productivity measurement with natural capital and bad outputs*
(July 2014) by Nicola Brandt, Paul Schreyer and Vera Zipperer

1153. *Reducing income inequality and poverty and promoting social mobility in Korea*
(July 2014) by Randall S. Jones and Satoshi Urasawa

1152. *Fostering a creative economy to drive Korean growth*
(July 2014) by Randall S. Jones and Myungkyoo Kim

1151. *Economic uncertainties and their impact on activity in Greece compared with Ireland and Portugal*
(July 2014) by Jan-David Schneider and Claude Giorno

1150. *Workplace stress in the United States: issues and policies*
(July 2014) by Michael Darden

1149. *Taxing the rent of non-renewable resource sectors: a theoretical note*
(July 2014) by Julien Daubanes and Saraly Andrade de Sá

1148. *Health, work and working conditions: a review of the European economic literature*
(July 2014) by Thomas Barnay

1147. *Making the best of new energy resources in the United States*
(July 2014) by Douglas Sutherland

1146. *Improving well-being in the United States*
(July 2014) by Aida Caldera Sánchez, Patrick Lenain and Sarah Fléche

1145. *Deconstructing Canada's housing markets: finance, affordability and urban sprawl*
(July 2014) by Calista Cheung
Restructurer les marchés canadiens du logement : financements, accessibilité financière et étalement urbain
(Juillet 2014) par Calista Cheung

1144. *Women's role in the Swiss economy*
(July 2014) by Richard Dutu
Le rôle des femmes dans l'économie suisse
(Juillet 2014) par Richard Dutu

1143. *Overcoming skills shortages in Canada*
(July 2014) by David Carey
Combler les pénuries de compétences au Canada
(Juillet 2014) par David Carey