GSR discussion paper

Consumer protection in the online world

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by XX.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

Table of Contents

Page

Consumer protection in the online world

Author: Cullen International[1]

1 Introduction

This paper is for discussion by the GSR and is aimed at examining the changing usage patterns of consumers and what the local and globalised ICT consumers of digital services expect in terms of protection when they conduct various types of activities online.

The paper examines the need for revised regulatory frameworks and explores the various options available, such as co-regulation and self-regulation, based on country experiences from around the world. It discusses the need for greater collaboration and cooperation at the regional and international levels. This paper complements the study carried out in 2012 on consumer protection in a converged world[2].

The discussion paper starts by looking at consumer protection in the online world. It describes the needs and concerns of digital consumers when they engage in the most common forms of online activities: searching the internet, shopping online, making payments, consuming music and video, gaming and using apps, using social media and cloud services.

The paper identifies a number of cross-cutting regulatory issues that need to be addressed by policy makers, regulators[3] and industry to ensure that digital consumers are correctly protected when engaged in these online activities:

- privacy
- security
- fighting illegal and harmful content
- copyright
- net neutrality
- payments
- consumer rights and trust
- delivery
- consumer redress and education

It highlights some of the responses that have been given around the world and shows some recent attempts to address specifically the conduct of new market players such as search engines, cloud and app service providers.

---

[1] Michèle Ledger, Javier Huerta Bravo, James Thomson

[2] http://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Regulation%20and%20consumer%20protection.pdf

[3] In this report, the term 'regulator' means a regulatory authority or body, or a public authority or agency responsible for exercising some sort of authority over an activity or category of operator: a telecom NRA, a financial authority, a media regulatory authority, a competition authority, a privacy authority etc..

2 Setting the scene

2.1. Rapid growth

It is now clear that in many regions of the world, consumers have a strong online presence for many aspects of their lives (working, socialising, communicating, consuming...) and this trend is set to continue.

A recent OECD report[4] highlights that e-commerce has been growing steadily since it first emerged[5]. From 2004 to 2010, e-sales grew from 9 to 14% of the turnover of non financial enterprises in the European Union, and from 10% to 16% in the United States.

The OECD highlights that growth is uneven among countries and regions of the world and that:

B2B sales dominate in terms of value of transactions

E-commerce is dominated by business-to-business (B2B) sales, with around 90% of the value of e-commerce transactions coming from B2B.

B2C transactions growing faster than other segments

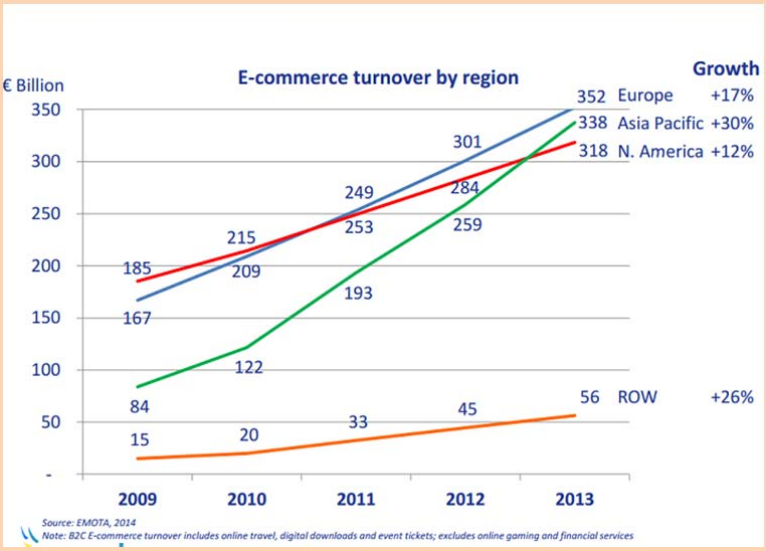
The remaining 10% of transactions are a combination of business-to-consumer (B2C), business-to-government (B2G) and consumer-to-consumer (C2C) activities. Recently, B2C transactions have been growing faster than other segments, but from a lower base.

Figures from Emota, the European Distance Selling Association, show that growth is fastest in the Asia Pacific region (wih a 30% increase between 2009 and 2013).

[4] OECD (2013), "Electronic and Mobile Commerce", OECD Digital Economy Papers, No. 228, OECD Publishing. http://dx.doi.org/10.1787/5k437p2gxw6g-en

[5] B2C E-commerce started in the mid-1990s with the birth of major companies: Amazon (1994) and eBay (1995)

Figure 1 - e-commerce turnover by region



Source: Emota, 2014

Ofcom, the communications regulator in the United Kingdom, has also published figures[6] which show that the United Kingdom spends the most per head on online shopping among a group of comparator countries (UK, France, Germany, Italy, USA, Japan, Australia and Spain).

Online spend per head in the United Kingdom was £1,175 ($1.974) in 2012. Australia was second highest with spend per head of £867 ($1.456), followed by the US £663 $1.113) and Japan £560 ($940,8).

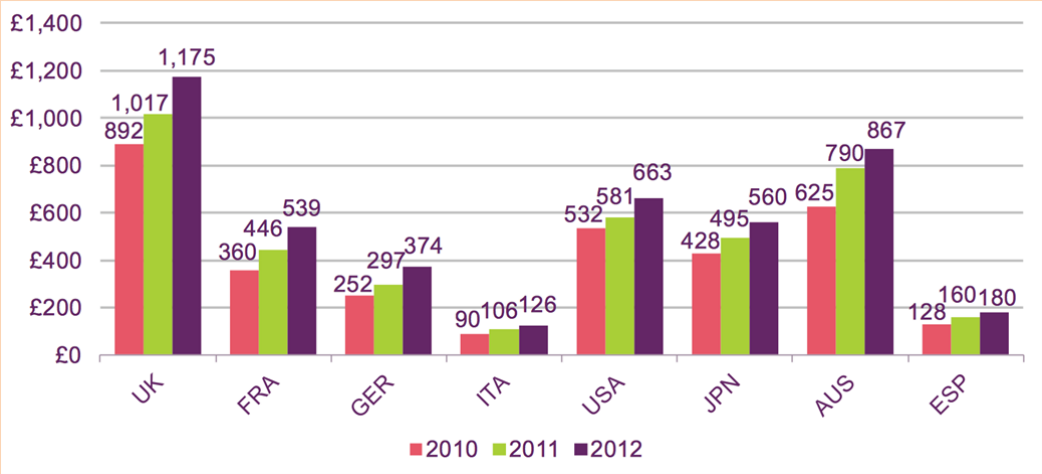
Online sales accounted for 10.5% of total retail sales in the UK in October 2013[7]; and 6.0% in the US in the fourth quarter of 2013[8].

6 http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr13/international/

7 http://www.ons.gov.uk/ons/rel/rsi/retail-sales/october-2013/sty-internet-sales.html

8 https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Figure 2 - Online spend per head



Source: Ofcom (uk)

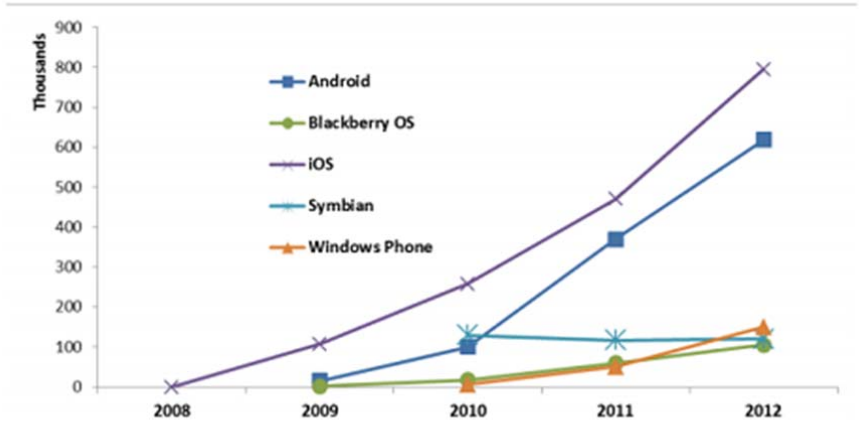
A clear trend is that increasingly, B2C e-commerce is taking place through smartphones, tablets and apps. The OECD[9] predicts that the widespread use of smartphones and mobile apps provides a powerful new platform for the growth of e-commerce, especially given the fact that technologies enabling payments (such as Near Field Communication, NRF) are increasingly being integrated into handsets.

This figure illustrates the growth of apps available for download between 2008 and 2012. The growth of apps changes the way that people access information, with increased access on smartphones and tablets, and with less access through web browsers[10].

[9] OECD (2013), "Electronic and Mobile Commerce", OECD Digital Economy Papers, No. 228, OECD Publishing. http://dx.doi.org/10.1787/5k437p2gxw6g-en

10 OECD (2013), "The App Economy", OECD Digital Economy Papers, No. 230, OECD Publishing. http://dx.doi.org/10.1787/5k3ttftlv95k-en

Figure 3 - Growth of apps available for download by platform, 2008 -2012



Source: Statista.com, 148apps.biz, appbrain.com, and company profiles (2013)

2.2 Gatekeepers and monopolies

As shown in the table below, some parts of the internet value chain are dominated by a very small number of players. This is particularly the case in online search and social media.

This means that for some of the activities described in the following section, digital consumers will have the choice between a very small number of providers.

Figure 4 - Worldwide market shares in 2012

	Vertical markets					Horizontal markets		
	Operating system (PC)	Operating system (Mobile)	Browser (PC)	Browser (Mobile)	Search	Social network	Internet portals	Online advertising
Google	-	37%	40%	43%	90%	<1%	-	32%
Microsoft	91%	1%	29%	3%	7%	<1%	12%	3%
Apple	7%	25%	8%	39%	-	<1%	-	-
Facebook	-	-	-	-	-	79%	-	4%
Yahoo	-	-	-	-	-	<1%	26%	3%

Source: Italian communications authority, AGCOM[11]

2.3 Advertising

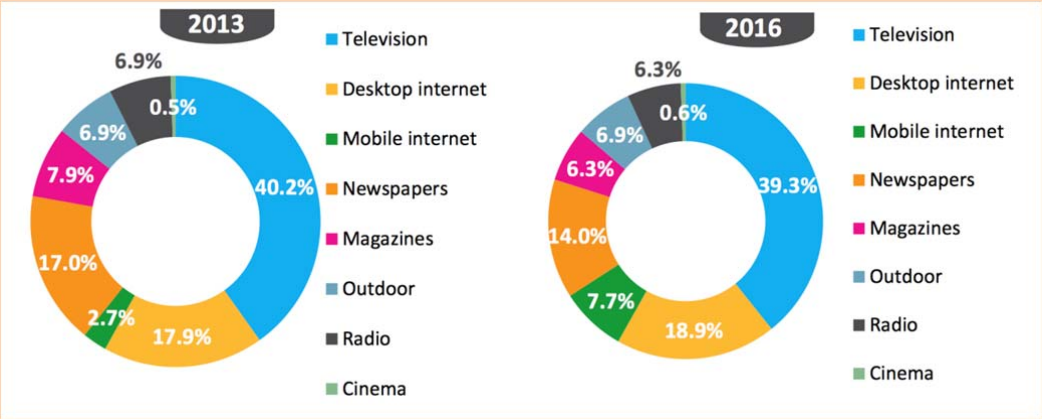
Many of the most popular internet services are free to use (e.g. search and social media) for digital consumers. Digital consumers may not be aware that a completely free service on the internet rarely exists, and that these apparently free services are in fact financed by advertising.

Internet is currently the second largest advertising medium after television globally.

Internet advertising is predicted to increase its share of the global advertising market from 20.6% in 2013 to 26.6% in 2016, according to ZenithOptimedia.[12]

Mobile internet advertising is growing much faster than desktop internet advertising, driven by the rapid adoption of smartphones and tablets.

Figure 5 -Share of global adspend by medium (%)



Source: ZenithOptimedia

[11] http://www.agcom.it/Default.aspx?message=visualizzadocument&DocID=12657

http://www.zenithoptimedia.com/wp-content/uploads/2013/12/Adspend-forecasts-December-2013-executive-summary.pdf

3 Main online activities

This section gives an overview of the main online activities of digital consumers in the digital world, illustrating their concerns and needs. Cross cutting regulatory issues (i.e. those which span a number of online activities) and attempts to regulate new activities and market players are addressed in more detail in the following sections.

3.1 Search

Consumers very often start by searching the Internet. As the chapter above mentioned, search is mainly done (90 %) through Google search. Users may have the following concerns when using search engines:

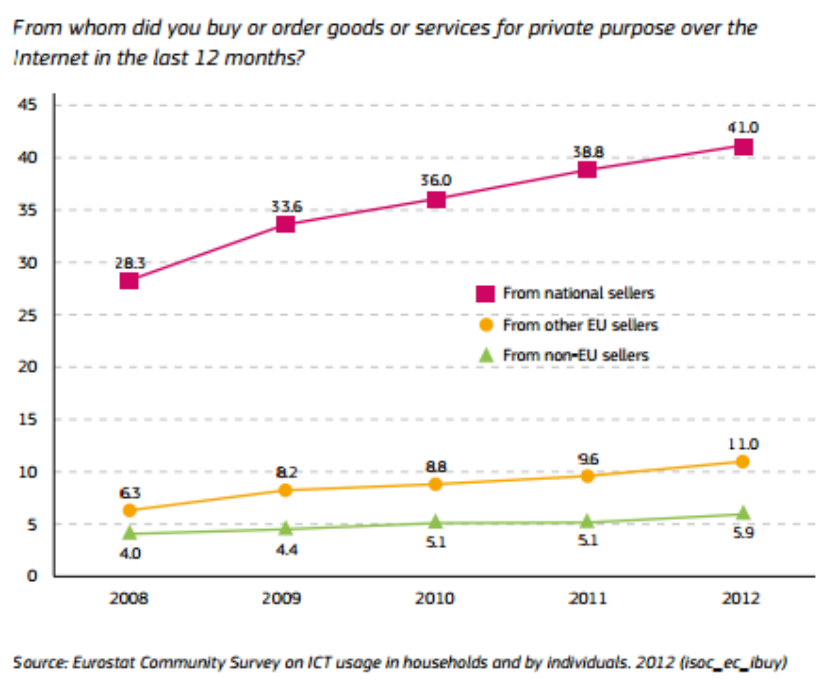
- how will their search data be used? Will it be sold for commercial purposes, or used for law enforcement?
- have the search results been manipulated in some way?
- will they be exposed to illegal or damaging search results? If so, what should they do?

Because of the scarcity of operators, digital consumers are concerned about the way they operate on the market and expect a high level of protection and transparency.

3.2 Shopping online

Consumers are increasingly buying goods online. According to figures for the EU, there is also a growing gap between domestic and cross-border e-commerce. Consumers are more inclined to buy from domestic websites than from websites that are located in another country.

Figure 6 - Percentage of the population who ordered goods or services over the Internet from national sellers/ from sellers from other EU countries/from sellers from the rest of the world (non-EU) in the last 12 months (EU 27)



The proportion of online cross-border shoppers has however grown in all countries since 2008 and according to a report by the European Commission[13], the largest increases are observed in Malta (21 percentage points), Luxembourg (17), Belgium (16) and Finland (15).

Consumers face particular issues when they shop from websites that are located in other countries

The particular concerns are as follows:

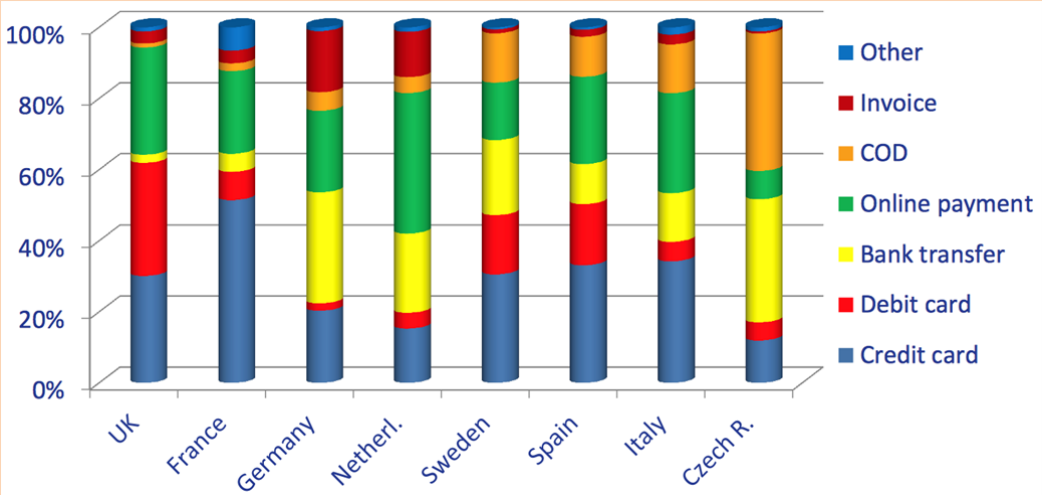
- Consumers do not know who is operating on online store or how to contact the website for more information, for instance on the ordering process.
- If things go wrong (e.g. the ordered goods do not arrive, or the customer is billed twice) consumers very often do not know where to go for redress.
- When making purchases online, consumers are usually asked to tick a box to confirm they accept the terms and conditions. The conditions are generally very long and consumers have no choice in accepting them if they want to make the purchase.
- Will they receive their ordered goods on time?

[13] The Consumer Conditions scoreboard – Consumers at home in the single market – sWd(2013) 291, http://ec.europa.eu/consumers/consumer_research/editions/docs/9th_edition_scoreboard_en.pdf

3.4 Making payments

The preferred payment methods for online purchases vary considerably among countries. In the UK, credit and debit cards and the PayPal online payments platform account for nearly all of the market. In other countries, bank transfer and payment by cash on delivery (COD) are also important payment methods.

Figure 7 - Online payment methods by country in 2011



Source: EMOTA[14]

New methods of payment are being developed, including mobile phone payments/m-wallets (payments through SMS, payments charged on consumer mobile operator's bills, etc). The growth in use of mobile devices to make payments is expected to accelerate, especially in developing countries where many consumers do not have bank accounts and do not have access to credit cards.

The digital consumer needs assurance that these new methods of payment will be sufficiently trustworthy.

When consumers get to the stage of paying for their online purchases, they often find that there is a surcharge for paying by credit or debit card rather than by other means such as the Paypal online payment platform. For example, surcharges are common for purchases of airline tickets.

Consumers may be worried about the risk of their bank or credit card details being stolen and used to make unauthorised transactions.

3.4 Music and video

Consumers may find that access from their country to websites offering legal streaming or download services for music, video or television is blocked or that the catalogue of content is restricted. Geo-blocking is done based on the IP address of the visitor.

[14] http://media.wix.com/ugd/b18286_390bb25f5c1340fbbc9df4945b56ad16.pdf

For example:

- The availability of Netflix outside of the US is restricted to the following countries: Canada, Mexico, throughout South America, United Kingdom, Ireland, Netherlands and Nordic countries[15].
- Across Europe, some of the live streaming and catch-up services of the main national commercial television channels and public service channels are either blocked or limited outside of their home country (e.g. the international (outside UK) version of BBC iPlayer gives access to a much narrower catalogue of content than the domestic version.

In many countries, there are only a limited number of legal services available and consumers tend to access music and video content through illegal services that are available on the Internet, either through P2P, download or streaming services. To by-pass geo-blocking, users are inclined to use proxy services which allow users to mask their home country location and to access the services that they could otherwise not access.

Video download and streaming services are very 'bandwidth hungry' and digital consumers will be want to be assured that their access to services is not blocked or slowed down by their broadband access provider – provided that the content is legal.

3.5 Gaming and using apps

Games marketed as “free to download” are not always free to play, as the players may need to pay for special content or features through in-app purchases.

Consumers need protection against unexpected costs from in-app purchases. Further, they may not be fully aware of the amount of money they are spending because their credit cards are charged by default.

Children are particularly vulnerable to marketing of free to download games.

3.6 Using social media

The use of social media entails many new types of concern, including in relation to the protection of minors.

The main problems are:

- Children are less aware than adults of the risks of sharing their personal information.
- Children seeing age-inappropriate content, such as sexual or violent content.
- Cyber bullying and exposure to negative user generated content (such as posts, comments, pictures or videos on social networks such as Facebook or online sharing platforms such as YouTube).
- Inappropriate contact from adults with a sexual interest in children.

In adulthood, problems can also arise, in particular with the protection of their personal data:

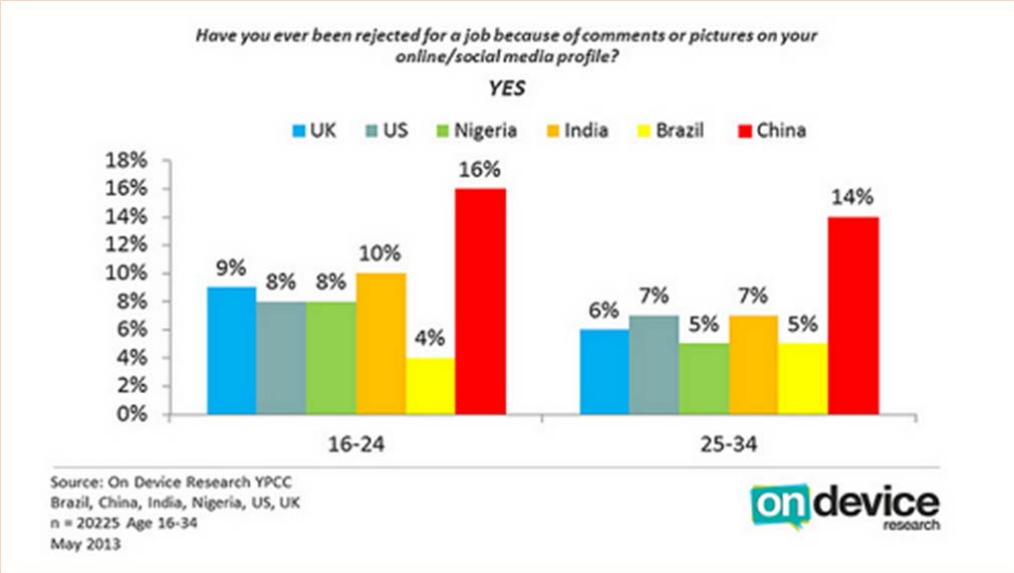
- Consumers are not always aware of the privacy issues that using social media involve.
- Consumers may face problems when they try to transfer their personal data from one social network to another. They are locked-in with a single operator.

[15] http://ir.netflix.com/faq.cfm

A recent study[16] has highlighted that one in ten young people have been rejected for a job because of comments or pictures on their social media profile. The report also reveals that a majority (two-thirds) are not concerned that their use of social media now, can harm their future career prospects and are not deterred from using it.

The report concludes that better education of the impact of social media is needed, to ensure young people are not making it even harder for them to get on the career ladder. This illustrates that it is important to enable digital consumers to erase their profiles from social media.

Figure 8 - Percentage of applicants that have been rejected for a job because of their social media/online profile



3.7 Using cloud services.

Demand for storage is increasing because of the sheer volume data that businesses and individuals are collecting, and the use of the cloud is now part of everyday life in developed countries[17]. It has numerous advantages in that users can store their files, software, photos, video, music etc. on the cloud and access their content when they need it on their smart phones, laptops or tablets from whatever location.

Consumers already use a range of cloud services, including web-based email (e.g. Gmail), social media (e.g. Facebook), software as a service (e.g. Office 365), and cloud storage (e.g. dropbox).

With cloud services, some of the particular concerns of digital consumers are as follows:

- Will the data (music, video, photos) be safe on the cloud?
- Will they be able to transfer the data from one cloud provider to another? (data portability)
- What will happen if the service becomes unavailable?

[16] http://ondeviceresearch.com/blog/facebook-costing-16-34s-jobs-in-tough-economic-climate#sthash.MLn5EZhF.Vp50W4rO.dpbs

[17] GSR 2012 Discussion Paper, The Cloud: Data Protection and Privacy Whose cloud is it Anyway?

- Is the cloud provider subject to any rules and regulations?

In the following section, we will attempt to answer some these questions.

4 Cross-cutting regulatory questions and the role of policy makers, regulators and market operators

4.1 Privacy

When accessing some of the online services referred to above, consumers may not feel in control of their privacy online. In particular, they may not know what personal information is being collected about them, who is collecting their personal data and who it is passed on to, what purpose(s) their data is being used for. In this context, consumers very often have no choice other than to accept the complex privacy terms or not to use the service at all.

The increasing monetisation of personal data has led some operators to massively collect individuals' personal data for different purposes such as behavioural advertising. In this regard, consumers sometimes do not understand that there is a trade-off between free to use services and the tracking and behavioural advertising that often finance those services. When accessing these services, consumers are often literally tracked without giving their consent, for the purpose of targeting personalised advertising to them. This issue has been put at the centre of the work programme of Consumers International[18].

Furthermore, consumers may face difficulties when they try to transfer their personal data from one operator (e.g. social network, cloud services provider) to another. Indeed, if they want to switch to another operator, they will in most cases have to re-enter all their personal data and information with the new operator. Given these difficulties, consumers may find too burdensome to shift to another operator. This situation also prevents new operators from accessing the market, thereby impeding effective competition.

Also, in some jurisdictions, competent authorities have enacted data retention laws obliging certain operators such as ISPs to retain for a period, certain types of personal data (in particular so-called traffic data, such as IP addresses, email addresses of senders and recipients) for law enforcement purposes. Consumers may not know that their personal data are retained or the conditions (e.g. duration, type of retained data, location of the retained data) under which the data retention takes place.

As reflected in the multistakeholder statement[19] following NETmundial, the Snowden revelations on mass surveillance activities by intelligence agencies have put data protection at the centre of the international debate on internet governance and have considerably increased consumers' awareness regarding privacy issues.

Regulatory landscape and trends

Privacy laws are being revised in some countries with the purpose of strengthening individuals' privacy rights.

In the EU, whose current data protection rules date from 1995,[20] a new proposal[21] includes a number of measures to reinforce online privacy rights. For instance, individuals' consent for the processing of personal data would have to be given explicitly (either by a statement or by a clear affirmative action), rather than assumed.

---

18 http://www.consumersinternational.org/media/1113711/ci%20programme%20of%20work%20on%20privacy.pdf

19 http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

20 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

21 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

The new proposal also provides individuals with a right to data portability, whereby they would have the possibility to request from the operator a copy of their personal data or information[22] and to transmit them directly from one operator to another.

Also in the European Union, data retention laws are particularly vulnerable at the moment. They are being challenged before constitutional courts following the decision of the Court of Justice of the European Union to strike the data retention directive[23] as it did not respect EU citizens' fundamental right to the protection of their personal data[24].

Australia has recently adopted new data protection rules[25] that will strengthen consumers' rights by including measures aimed at improving consumers' access to companies' privacy policies, generally prohibiting the disclosure of individuals' data for the purpose of direct marketing, and establishing timely and effective complaints handling mechanisms.

In April 2014, Brazil, whose government is very much concerned about the issue of mass surveillance, adopted a new internet law, also known as 'Marco Civil'[26]. The law enshrines the right of internet users to privacy of their internet communications, and requires ISPs not to give third parties access to their registry of end users´ connections and applications, unless the end users have given their explicit consent, or in the cases foreseen by law.

Privacy rules vary considerably from one country to another and some countries completely lack privacy laws. The different levels of data protection throughout the world may bring some legal issues when consumers whose privacy rights have been violated seek redress in third countries, or when personal data are transferred from one jurisdiction to another. Indeed, cross-border personal data flows, which are an integral element of today's e-commerce, are continuously increasing, thereby elevating privacy risks. In this context, international cooperation is crucial. For instance, the EU and the US, whose respective privacy policy frameworks differ enormously, have developed a Safe Harbour Framework containing a number of privacy principles[27] to which US based companies may adhere. Under this voluntary scheme, Safe Harbour companies such as Google or Facebook can transfer EU citizens' personal data to the US. However, the Snowden revelations on alleged back-doors from US companies to the US intelligence agency have put this framework under scrutiny.

The global dimension of privacy issues has led some international organisations to take some initiatives regarding privacy. In 2013, the OECD adopted revised guidelines governing the protection of privacy and transborder flows of personal data[28]. The guidelines, which aim to harmonise OECD countries' privacy laws, include a number of principles such as purpose specification (i.e. the purposes of the data collection have to be specified), use limitation (i.e. data should not be disclosed or used for non-specified purposes

---

[22] Some operators already offer to the users the possibility to obtain a copy of their data : seehttps://www.facebook.com/help/131112897028467 and https://support.google.com/takeout/answer/2508459?hl=en&ref_topic=2508503

[23] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[24] http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=406224

[25] http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform

[26] http://www.senado.gov.br/atividade/materia/getPDF.asp?t=147571&tp=1

[27] http://export.gov/safeharbor/eu/eg_main_018475.asp

[28] http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

without the individual's consent or when authorised by law), and security safeguards. Similar harmonisation intents have taken place in other international fora (e.g. APEC's privacy framework)[29].

Although these agreements and soft-law approaches may help in offering solutions to consumers' privacy concerns, more and more voices are advocating the adoption of a global instrument providing for strong privacy and data protection principles. In 2009, data protection authorities from different countries all around the world called for the establishment of a new international framework for privacy protection, with the participation of civil society[30].

Role of data protection authorities

Data protection authorities are increasing their efforts in protecting consumers' privacy rights by:

- conducting investigations and possibly fining major companies for not respecting privacy rules. For instance:
  - In May 2014, the Court of Justice of the European Union adopted a landmark decision obliging operators of search engines to remove from their search results links to other websites that contain personal data – at the request of the concerned individual and under certain conditions[31]. The Court ruling confirmed the decision of the Spanish data protection authority, who requested Google to remove the links directing to another website containing an individual's personal data. It implies that search engines are bound by the so-called right to be forgotten.
  - Several regulators from different countries around the globe (e.g. Macao China, United States, Republic of Korea, Germany) have fined Google for its collection of personal data without user's consent for the provision of its 'street view' services. According to the Korea Communications Commission, "the information collected included not only personal data such as online IDs, passwords and residential registration numbers but also around 600,000 Mac addresses that are highly likely to identify the user if used in combination with other information"[32].

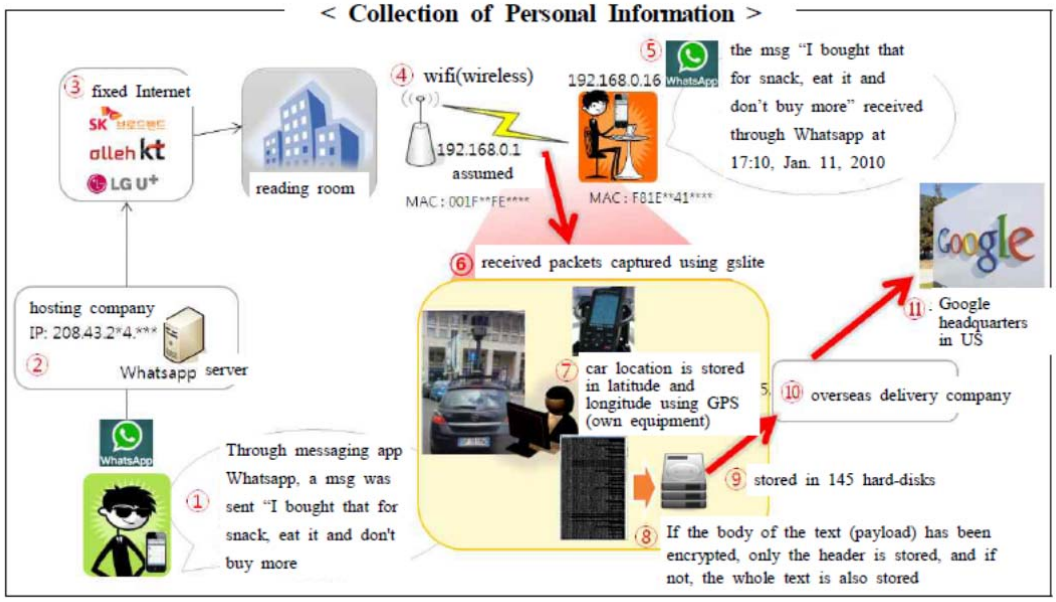
[29] http://publications.apec.org/publication-detail.php?pub_id=390

[30] http://privacyconference2012.org/wps/wcm/connect/2912ce004adc64f09e809ea0fea628d8/2009_M1.2.pdf?MOD=AJPERES

[31] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

[32] http://eng.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=37564

Figure 9 – Google's collection of personal data for its "street view" services



Source: Korea Communications Commission

- issuing guidance in order to help different data controllers or processors in protecting consumers' personal data. Some examples:
  - The body representing European data protection authorities have recently issued recommendations on anonymisation techniques[33]. Anonymisation techniques are gaining importance in the context of Big Data. They consist in processing personal data to prevent the individuals' identification and allows operators to make information derived from the personal data they hold publicly available for different purposes (e.g. scientific research), whilst protecting consumers' personal data. As stated in the ITU-T Technology Watch Report[34], "some telecommunications operators have started exploiting aggregated customer data as a source of income by providing analytics on anonymised datasets to third parties". Anonymisation processes entail certain risks that personal data are disclosed and guidance can therefore be of utmost help for operators.
  - In 2014, representatives of the body representing European data protection authorities and of APEC economies agreed on a checklist aimed at facilitating personal data transfers for

[33] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[34] http://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000220001PDFE.pdf

international businesses operating in both the EU and APEC economies, while respecting consumers' privacy rights[35].

Industry-driven initiatives

Conversely to regulation, standardisation and self-regulation can serve at exploring the economic or social benefits of personal data, whilst respecting consumers' privacy rights, as shown in the following examples.

Regarding behavioural advertising, although some countries' laws provide that tracking can only take place with the consumer's explicit consent, they do not go as far as to indicate the technical means by which consent can be given. In this context, standardisation initiatives can hugely help consumers. All of the major web browsers have a "do not track" (DNT) preference setting. The purpose of the DNT standard is to determine how a website or advertiser should reply to a notification expressed by an internet user (normally through a browser setting) that they do not wish to be tracked online. With this setting enabled, each time the browser fetches content from a website, it adds a request for the user not to be tracked – but it is up to the website and their third-party content providers (including advertisers) to honour this request. At present there is no agreed standard to implement DNT. The World Wide Web Consortium (W3C) has been working on a voluntary DNT standard since 2011, but reaching agreement between advertisers, website owners, browser producers, and consumer privacy advocates is proving challenging[36].

In the US, under the auspices of the Department of Commerce, different stakeholders have developed a code of conduct that brings transparency as regards the way providers of applications for mobile devices handle personal data[37]. It contains requirements for a short notice that would be presented to consumers after downloading an app. This notice should indicate what data the app collects, the means of accessing its privacy policy, and with whom it would intent to share the data[38].

Conclusions

The processing of personal data is an intrinsic part of consumers' day-to-day online activities. Most of consumers' online activities involve the processing of personal data (e.g. the mere access to a website, an online payment). Adequate protection of consumer's personal data is of key importance to the development of online activities.

Although some countries are strengthening their privacy laws, the coexistence of diverging legislative frameworks around the world does not help in building consumers' trust in cross-border e-commerce.

Industry initiatives are proving difficult to achieve as they require a high level of agreement among very different stakeholders. Regulators have a definite role to play to strengthen industry-led solutions such as anonymisation and privacy by design.

Recommendations

At the level of policymakers

---

35 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

36 http://www.w3.org/TR/tracking-dnt/

37 http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

38 http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf

Strong privacy regulations can help to make consumers feel more confident that their personal data is protected online. They should contain fundamental data protection principles (e.g. purpose limitation) and should provide individuals with rights (e.g. right to access the collected data, right to erase) and adequate safeguards. The latter are particularly relevant in the context of data retention.

The global dimension of online privacy requires concerted action in international fora and the adoption of international binding instruments.

At the level of the regulators

Regulators have a strong role to play in order to ensure that the rules on data protection are respected by market players.

Regulators also need to develop strong cooperation and partnerships with regulators in other countries and regions of the world, in an effort to develop common approaches.

Regulators need to provide guidance for the industry on the interpretation of the legal norms and help industry develop best practices.

Regulators can foster industry-wide codes of practice and be involved in standardisation initiatives.

At the level of the industry

Self-regulation (e.g. codes of conduct) and standardisation initiatives require the involvement of all the parties concerned (industry, governments, civil society, consumers, etc.).

4.2 Security

For all of his activities, the digital consumer will be concerned about the security of his data. For instance:

- What happens if his data is lost by internet companies, online retailers or governments and re-used for fraudulent purposes?
- Who is responsible to ensure the security of data?
- Is there a competent authority to deal with these issues?

Recent cyber attack incidents leading to severe security breaches have shown that these are real questions. Despite this, these simple questions are not easy to answer.

Regulatory landscape

Many countries[39] have in place legislation to criminalise new forms of attacks against information systems such as the illegal interception of computer data, or the spread of malicious software into networks and computers. These laws are useful but do not force operators to protect their systems in the first place, and do not provide particular protection for the digital consumer.

In the European Union at least, there is at the moment no obligation for companies other than telecommunications operators to notify security breaches to customers or to national regulators. The

[39] For instance, in the EU, the relevant directive is Council DIRECTIVE 2013/40/EU of August 12, 2013 on attacks against information systems and repealing Council Framework Decision 2005/222/JHA

European Union is attempting[40] to adopt a new directive which would oblige certain operators ('key internet enablers') to do so but negotiations are difficult.

The proposal would also oblige member states to set up national competent authorities responsible for network and information security and would oblige certain market operators[41] to have in place methods to deal with security risks.

In relation to the role of regulators, the proposal specifies that competent authorities would have the power to require market operators (and public administrations[42]) to:

- provide information needed to assess the security of their network and information security systems , including documented security policies; and
- undergo a security audit carried out by a qualified independent body or national authority and make the results available to the competent authority.

The proposed data protection regulation (mentioned above) is also proposing to extend the obligation to notify competent authorities and affected individuals in case of personal data breaches.

ITU is working with Member States, regions, and in partnership with IMPACT, to deploy capabilities to build capacity at national and regional level, in addition to establishing National Computer Incident Response Teams (CIRTs).

ITU, in collaboration with IMPACT, is helping countries to establish their National Computer Incident Response Team (CIRT), which serves as a national focus point for coordinating cybersecurity incident response to cyber attacks in the country. The objective of the CIRT Assessment is to define the readiness to implement a national CIRT.

ITU-IMPACT has to date completed CIRT assessments for over 50 countries.

Source: ITU: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx

At the regional level, ENISA[43], the European Union Agency for Network and Information Security has been set up to enhance the capability of the EU and its member states and businesses to prevent, address and respond to network and information security problems.

Industry argues that regulatory approaches could hinder private sector innovation and industry should be in charge with ensuring the protection of their systems. Cyber security standards are being developed[44] and this is sufficient, they argue.

---

[40] http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and

[41] The Commission's initial proposal refers to market operators "which enable the provision of other information society services" (an non exhaustive list of operators is included in an annex which lists as an example social networks and search engines), and operators of critical infrastructures that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health. Software and hardware companies would be excluded.

[42] The European Parliament has amended the Commission's draft and has proposed to remove public administrations from the scope of the proposal.

[43] http://www.enisa.europa.eu/about-enisa/activities

[44] See in particular ISO 27001 and 27002, http://www.17799.com/

Conclusions

The digital consumer needs to be assured that his data will be kept secure. There are very few policy responses dealing in a comprehensive manner with the concerns of digital consumers relating to the security of networks and data.

Recommendations

At the level of policymakers

It is difficult to conclude about a possible policy responses given the fact comprehensive strategies are not yet adopted on this question.

Despite this fact, we see that consumers do need at the very least to be informed of data and security breaches. Regulators should also be informed. At the very least, the policy framework should include these elements.

At the level of the regulators

Regulators should be established to deal with issues relating to information and network security. Their tasks can be to:

- provide information on security standards
- audit the security standards of operators
- explain to digital consumers what to do in case of cyber-security attacks
- provide information on new types of viruses, malware etc.

At the level of the industry

Industry should continue to work on the protection of the security of their networks and information systems as a matter of priority.

Even in the absence of a regulatory obligation, industry should be transparent about cyber attacks and inform affected users immediately when their data could be compromised.

4.3 Illegal and harmful content

Digital consumers may come across illegal and harmful content on the internet, for instance in search results or on social media.

Minors need more protection than adults and parents and carers need to make sure that children will not be exposed to violent or other forms of unwanted content. Many operators (ISPs, mobile operators, social networks, search engines) have committed through codes of conduct or on their own initiative to address the problem of harmful content. ISPs and mobile operators usually offer parental controls that need to be activated by subscribers. The main search engines also offer 'safe search' tools to prevent inappropriate content (text, images and videos) to appear in search results.

Despite these initiatives, parents are sometimes not sufficiently digitally literate to know what to do. There is therefore a need for governments, regulatory authorities and market operators to provide information on the available tools and on how to use them.

Digital consumers need to know what to do when faced with illegal and harmful content.

- Who should they report the content to?
- How can the content be removed?
- Where can they seek redress?
- What happens if the content is on a website that is located in another jurisdiction?

These concerns illustrate that the respective roles of courts, police forces, market operators, regulators and victims need to be clearly defined.

Almost all countries have mechanisms in place to deal with illegal content on the internet but it is a complex area of policy since a balance needs to be achieved between freedom of expression on the one hand and the need to fight illegal activities on the internet. Difficulties also occur because:

- What is illegal in one country may not be illegal in another country.
- ISPs, search engine providers and SNS do not want to monitor the internet to detect illegal and harmful content.
- Law enforcement authorities need to be able to detect and take action against illegal acts and this very often requires the collaboration of ISPs, search engines and social networks.

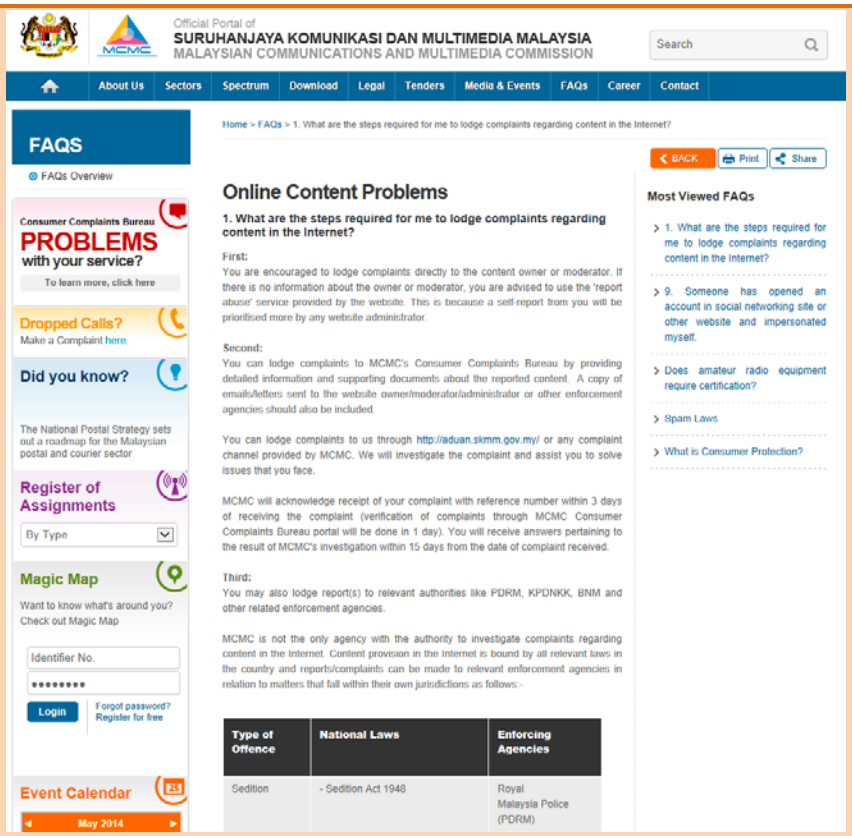
Around the world, laws are being adopted to try to deal with these issues, general laws and also specific rules to deal with special concerns (e.g. fighting online piracy, online child pornography, illegal gambling, etc.).

Self-regulatory frameworks on notice and take down or notice and take-action have also developed to frame the role of internet intermediaries and to ensure that content can easily be removed from websites when it is obviously illegal. In some areas (e.g. fighting online piracy, as explained above) regulators can be involved in the process.

Hotlines exist in many countries for victims to report illegal content. INHOPE[45] is the global network of internet hotlines to respond to reports of illegal content on the internet and to fight sexual abuse material.

Some regulatory authorities around the world are providing information on what to do when facing problem.

[45] http://www.inhope.org/Libraries/Infographics/INHOPE-2013-Inforgraphic.sflb.ashx



Source: website of the Malaysian Communications and Multimedia Commission

Conclusions

The digital consumer deserves at the very least to know what to expect when faced with illegal or harmful content on the internet. Minors are particularly vulnerable and need a higher level of protection than adults.

Many countries are adopting general and specific legislation to deal with illegal and harmful content on the internet. But digital consumers often do not know what to do when they are confronted with illegal and harmful content or conduct on the internet.

Recommendations

At the level of policymakers

Clear rules need to be adopted on the respective duties of internet players (ISPs, search engines, social networks), law enforcement, courts, regulatory authorities and hotlines in the fight against illegal and harmful content on the internet. These laws need to take into account the fact that content will often be located on websites in other jurisdictions.

At the level of the regulators

Regulators have a strong role to play to ensure that digital users receive the information they need. They can act to make sure that internet intermediaries deliver this information directly, but they can also promote this information on their websites.

Regulators can foster industry-wide codes of practice and be involved in standardisation initiatives.

Regulators need to develop strong cooperation and partnerships with regulators in other countries and regions of the world, in an effort to develop common approaches.

At the level of the industry

Industry should provide clear information on:

- the available filters
- how to report illegal or harmful content, and explain the follow up that will be given
- the hotlines that may be established in the country
- the possible involvement of regulators (e.g. AGCOM in Italy on the fight against online piracy as explained below and/or the police.

4.4 Copyright

As illustrated above, the main problems are the lack of availability of creative content in some regions and the increasing amount of online piracy.

The fact that broadband subscriptions continue increasing all over the world (e.g. according to the IFPI Digital Music Report 2014[46], whilst mobile broadband penetration in Sub-Saharan Africa only increased 2% in 2011, it increased 11% in 2013), presents new opportunities for both businesses and consumers, but also creates "a hugely disruptive challenge to the creative industries, especially in the area of digital copyright"[47].

Consumers' organisations generally perceive that efforts are being put by governments and international organisations in protecting the different rightholders (creators, music publishers, audiovisual producers) and fighting against piracy, rather than in taking the necessary initiatives to provide consumers with more access to creative content.

Regulatory landscape and trends

In some cases, the reason for the restrictions described above is the fact that the exercise of intellectual property rights is territorial in nature.

Rightholders, who have the exclusive right to authorise or prohibit the reproduction and the communication of their works, including online, normally exercise their rights on a territorial basis, country by country.

Consequently, providers of online content such as music or video need to clear rights in each country from which they allow access to their services. For example, currently, for an online provider of movies, to serve the US market with a population of 316m involves clearing rights only once, whereas to serve the EU market as a whole with a population of 503m could involve clearing the rights 28 times. The situation becomes even more complicated as very often more than one party have rights on a single copyright work. It goes without saying that sometimes it is not easy for internet providers to know from whom they need to obtain rights' clearance. For instance, an online music store that wants to offer a song will have to

[46] http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf

[47] In this regard, see ITU GSR11 Discussion paper http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/documents/05-Intellectual-property-E.pdf

clear authors' rights (via collecting societies), and the record producer's and performers' rights (via the record producer).

This may inevitably result in market fragmentation, and it is said to impede the emergence of new services. From the consumer perspective, this obviously leads to a lack of availability of legal content. Furthermore, the online provider's higher licensing costs will surely somehow be passed on to the consumer.

The territoriality principle, as well as the copyright framework, is enshrined in international treaties such as the Berne Convention and the World Trade Organisation's Agreement on Trade-Related Aspects of Intellectual Property Rights. A reform of the copyright system is probably needed but is proving difficult to achieve. Some also advocate a complete overhaul of the copyright system but this is unlikely to happen in the foreseeable future as it would require changes to international treaties[48] on which the copyright system is based.

The World International Property Organisation is the main actor regarding copyright in the international sphere. However, WIPO's on-going work in the Standing Committee on Copyright and Related Rights, which gathers representatives from 187 countries, is limited to concrete aspects of copyright, such as harmonizing exceptions and limitations to copyright (e.g. Treaty facilitating access to published works for the visually impaired and facilitating the cross-border exchange of accessible format copies[49]). Also, WIPO is witnessing the confrontation between developed countries, which rely on a strong content industry and do not want to reduce copyright protection, and developing countries, which advocate for more flexible copyright rules as a means to gain more access to creative content and knowledge.

In 2011, the OECD, following a high level meeting, issued a communiqué stating that although the "effective protection of intellectual property rights plays a vital role in spurring innovation and furthers the development of the Internet economy", "Internet policy making principles need to take into account the unique social, technical and economic aspects of the Internet environment"[50]. However, OECD's more concrete actions in the field of copyright have rather focused on piracy of digital content[51].

In the EU, several sectoral initiatives have been taken in order to overcome the rigidity of copyright rules. For instance, the EU has adopted a directive that aims to facilitate the multi-territorial licensing of authors' rights in musical works for online uses. The directive promotes that national authors' collecting societies aggregate their repertoires. The aim is to make it easier for online music services to obtain licences for a multitude of countries and to offer a large catalogue of music to consumers.[52]

Role of regulators

While little can be done to change the licensing of rights on a country-by-country basis, competition law authorities can have a role to play in how right holders grant licences and their action can ultimately improve consumers' access to online content.

---

[48] http://www.wipo.int/treaties/en/

[49] http://www.wipo.int/treaties/en/text.jsp?file_id=301016

[50] http://www.oecd.org/internet/innovation/48289796.pdf

[51] http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/piracy-of-digital-content_9789264065437-en#page1

[52] http://europa.eu/rapid/press-release_MEMO-14-80_en.htm

For instance, a system of licences for sports events granting absolute territorial exclusivity to licensees (broadcasters in this case) has been found contrary to competition law by the Court of Justice of the European Union.[53]

More recently, the European Commission launched in 2014 an investigation regarding alleged restrictions between several US rightholders (film studios such as Warner Bros., Sony Pictures, Paramount Pictures) and EU users (pay-TV broadcasters such as Sky Italia (Italy) and Canal Plus (France))[54]. Such alleged restrictions would be included in licensing agreements between the US and the EU companies and would prevent the latter to offer their services across borders, "for example by refusing potential subscribers from other Member States or blocking cross-border access to their services".

At the level of copyright enforcement, telecommunications operators and regulators are increasingly involved in copyright issues, mainly as regards the fight against piracy. For instance, France has set up a special administrative authority, HADOPI[55], to fight online piracy, to promote legal offers and to raise awareness about the consequences of internet piracy. HADOPI has developed powers in relation to individual downloaders, through a so-called graduated response system[56].

Another example can be found in Italy, where a special role has been given to AGCOM, the converged regulator.

New rules on protecting copyright online (in force since March 31, 2014) entrust AGCOM to order selective removal of works (or links/trackers to works) or disabling of website access by ISPs.

The regulation establishes a committee composed of representatives from the different sectors (consumers, rightholders, ISPs, public institutions) to develop and protect the legal offer of digital works and to discuss possible self-regulatory solutions with the aim of supporting the development of digital works.

The take-down procedure starts with the notification of a claim (in a form on AGCOM website) asking AGCOM for the removal of illicit content. AGCOM informs the claimant within 7 days about the start of the procedure or reasoned dismissal of the claim.

The notification about the start of the procedure (sent to the claimant, service providers and website manager, and uploader, if identified) should at least contain a detailed description of the digital works involved; the indication of the copyright law provision allegedly infringed; a brief description of the facts and of the preliminary outcomes of AGCOM investigation; the notice that the receiver of the notice may remove the disputed contents on a voluntary basis.

The parties may file counterclaims within 5 days. In case the recipient makes the necessary adjustments to remove the illicit content or if the claimant brings an action before a court, the procedure will be closed.

The procedure should be closed within 35 days. If AGCOM concludes that a breach has been committed, it will order the service provider to either remove the illicit content or disable access to it (i.e. web-

[53] http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-10/cp110102en.pdf

[54] http://europa.eu/rapid/press-release_IP-14-15_en.htm

[55] http://www.hadopi.fr/

[56] http://www.hadopi.fr/en/new-freedoms-new-responsibilities/graduated-response

blocking). The decision has to be proportionate to the gravity of the violation. Compliance with AGCOM decision must be ensured within 3 days. AGCOM decision can be challenged before an administrative court.

New rules are without prejudice of self-regulatory instruments on notice and take-down procedures put in place by interested parties.

Source: Cullen International

Industry driven initiatives

Some industry initiatives aim at facilitating the licensing of rights in musical works for online purposes. For example in 2000, collecting societies from all over the world signed the Santiago Agreement. This agreement contained reciprocal agreements allowing that a single collecting society granted multi-territorial licences covering the repertoire of the other collecting societies. For providers of online music services, the agreement put in place a one-stop-shop mechanism by which they uniquely had to negotiate with the collecting society of the country where the provider was based. The Santiago Agreement was withdrawn following European Commission's competition concerns[57]. Indeed, the agreement contained membership clauses, which restricted authors' ability to affiliate to the collecting society of their choice; and exclusivity clauses, which provided collecting society with absolute territorial protection regarding other collecting societies. These clauses obliged internet providers to obtain the necessary licences from the collecting society of the country where they wanted to offer their services.

In order to favour multi-territorial licensing solutions for online music, different rightholders are working on a global repertoire database[58]. This initiative may help online music providers to identify who owns and controls musical works, thereby facilitating their licensing tasks. This may result in consumers having more access to more music works in more territories.

In the audiovisual sector, the film producer MIRAMAX and Netflix have signed a licensing agreement covering a number of countries in Latin America and allowing licensing to occur on a regional basis[59].

In order to share content (e.g. videos, songs) and knowledge (e.g. academic works, e-books) whilst respecting copyright, creative common licences are spreading all over the world[60]. Creative common licences are a flexible solution to conciliate the rigid copyright rules with the creator's expectations to reach a wider audience. They normally contain a permission to publicly share and use a given work under certain conditions designed by the creator himself. These licences are also being increasingly used by public institutions and international organisations[61].

Conclusions

Although new online services continue spreading throughout the world, the online market of online content is fragmented and consumers are often discriminated by reason of their physical location.

---

[57] http://ec.europa.eu/competition/antitrust/cases/dec_docs/38698/38698_4567_1.pdf

[58] http://www.globalrepertoiredatabase.com/

[59] http://ir.netflix.com/faq.cfm

[60] http://creativecommons.org/about

[61] http://www.wipo.int/pressroom/en/articles/2013/article_0026.html

The focus should be put in improving licensing practices, i.e multi-territorial licensing. The territoriality principle does not prevent rightholders from granting multi-territorial licences.

The challenge is to conciliate the righholders' right to be properly remunerated with the consumers' expectations to enjoy an attractive legal offer of online content wherever they are.

As commissioner Viviane Reding said in relation to European consumers, "consumer rights online should not depend on where a company or website is based. National borders should no longer complicate (...) consumers' lives when they go online to buy a book or download a song"[62].

Recommendations

At the level of policymakers

The debate on the adequacy of the existing copyright rules to the online environment has to be brought in regional and international fora, as it is happening in the EU.

Educational campaigns should be promoted in order to educate consumers to the respect of intellectual property rights.

At the level of regulators

Competition authorities play a key role in ensuring that certain rightholders do not put barriers to cross-border online services.

Regulators could become more involved in copyright enforcement. They are the appropriate actors to build bridges between rightholders, intermediaries and consumers (e.g. they can coordinate multistakeholder, fast and efficient mechanisms to take down illegal content).

At the level of the industry

Rightholders should explore new licensing solutions, especially for audiovisual content.

Online service providers should not add additional barriers to e-commerce, i.e. if they acquire multi-territorial licences they should develop multi-territorial online stores for consumers (in the EU, a single online music store instead of 28).

4.5 Net neutrality

Net neutrality in its simplest definition means that digital consumers should not find that their access to, and use of, specific apps, content or services is blocked or slowed down by their broadband access provider – provided that the content is legal.

Net neutrality is therefore an issue relevant to many of the services used by digital consumers discussed in this paper.

Regulatory responses

There have been three types of regulatory responses:

- requiring broadband access providers to be transparent about their traffic management practices;
- imposing a legal requirement for net neutrality;

[62] http://europa.eu/rapid/press-release_IP-09-702_en.htm

- the 'do nothing' approach.

At the European Union level, broadband access providers are required to explain clearly and simply on their websites and in their contracts:

- any conditions limiting access to, and use of, apps, content or services;
- the traffic management practices they apply and the impact on service quality.

The EU is proposing to go beyond such transparency requirements and to impose a EU-wide net neutrality rule: blocking or slowing down access to apps, content or services by ISPs for anti-competitive reasons would be prohibited.[63] Traffic management would still be allowed for legitimate reasons, such as managing peak loads, provided it is applied in a non-discriminatory way. It is expected that the proposal will be adopted at the end of 2014 or start of 2015.

Laws requiring net neutrality have already been adopted in two European countries – the Netherlands[64] and Slovenia[65].

In the US, the Federal Communications Commission (FCC) on May 15, 2014 opened a public consultation on proposals to replace the net neutrality rules contained in its 2010 Open Internet Order that were (partly) revoked by a court decision in January 2014[66].

In Latin America, laws requiring net neutrality have been adopted in Chile[67] and Colombia[68].

Recently the net neutrality question has shifted focus from blocking/slowing down access to whether broadband providers should be allowed to charge content companies for preferential treatment to reach customers at higher speeds or quality (so called “fast lanes”).

In February 2014 Netflix and the US cable operator Comcast struck a landmark deal in which Netflix would pay an undisclosed fee for faster access to Comcast customers[69].

Here clear rules have yet to be established.

In the US, the revised Open Internet proposals adopted by the FCC on May 15,2014 address the question of fast lanes and the conditions under which they would be acceptable. The FCC has put forward a proposal to allow ISPs to charge companies to reach customers at faster speeds but only if they meet a new standard of “commercial reasonableness” that will be judged by the FCC on a case-by-case basis.

The EU is proposing that in addition to regular, best-effort internet access, broadband access providers are allowed to offer “specialised services” requiring a defined quality of service or dedicated capacity as long as those services do not impair the quality of internet access services. Under the proposed EU

[63] http://ec.europa.eu/digital-agenda/en/connected-continent-legislative-package

[64] Article 7.4(a) of Telecommunications Law. http://www.government.nl/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act.html

[65] Article 203 of Electronic Communications Act. http://www.scribd.com/doc/144614369/Slovenia-Net-Neutrality-law-2012

[66] http://www.fcc.gov/document/fcc-launches-broad-rulemaking-protect-and-promote-open-internet

[67] http://www.leychile.cl/Navegar?idNorma=1016570&buscar=NEUTRALIDAD+DE+RED

[68] https://www.dnp.gov.co/LinkClick.aspx?fileticket=tYD8BLf-2-g%3D&tabid=1238

[69] http://www.ft.com/intl/cms/s/0/60a27b18-9cc4-11e3-b535-00144feab7de.html#axzz31gCtDVc4

definition, specialised services operate in closed networks, e.g. IPTV, and are not used as a substitute to full internet access services.[70]

Recommendations

At the level of policy makers

Policy makers should define a clear set of rules on net neutrality covering both regular internet access and paid-for fast lanes.

At the level of regulators

Regulators should monitor the enforcement of these rules and provide guidance on their implementation. For example, regulators can define what is the minimum quality of service acceptable for regular internet access and what are fair and reasonable conditions for selling fast lane access.

At the level of the industry

Broadband access providers should act transparently both towards broadband users and content companies. Users should be able to easily understand the traffic management policies that apply to the broadband subscription they buy.

Fast lanes should be offered in an open and transparent way to all content companies that may be interested in using them, including at fair and non-discriminatory prices and other terms and conditions.

4.6 Payments

We identified above that consumers need to be confident that new methods of payment will be trustworthy.

This is an area for policy makers and regulators, as some of these new methods of payments are not offered by the usual 'regulated' entities but by new entrants, which do not necessarily abide by the same set of rules and regulations.

EU policy makers are seeking to make sure that operators providing these services are supervised by national competent authorities and provide the same guarantees as payment services offered by banks and credit card companies[71].

The OECD Committee on Consumer Policy very recently issued[72] policy guidance to boost consumer protection when using mobile and on-line payment systems and to identify ways in which policy makers and businesses can work together to strengthen consumer protection while also ensuring innovation in the marketplace.

For instance to ensure the security of payments, the OECD policy guidance specifies that:

- Payment providers should put in place appropriate safeguards to protect the security of their systems, and should encourage the adoption of such measures by all entities having access to consumer data related to payments

[70] http://ec.europa.eu/digital-agenda/en/connected-continent-legislative-package

[71] http://europa.eu/rapid/press-release_MEMO-13-719_en.htm?locale=en

72 March 28, 2014, http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/cp(2011)24/final&doclanguage=en

- In addition to notifying consumers, payment providers should provide them with timely and effective redress mechanisms when their data is compromised and/or they suffer financial losses caused by security breaches
- Stakeholders should work together to raise consumer awareness about payment security issues, and about the actions that consumers can take to protect themselves in such transactions.

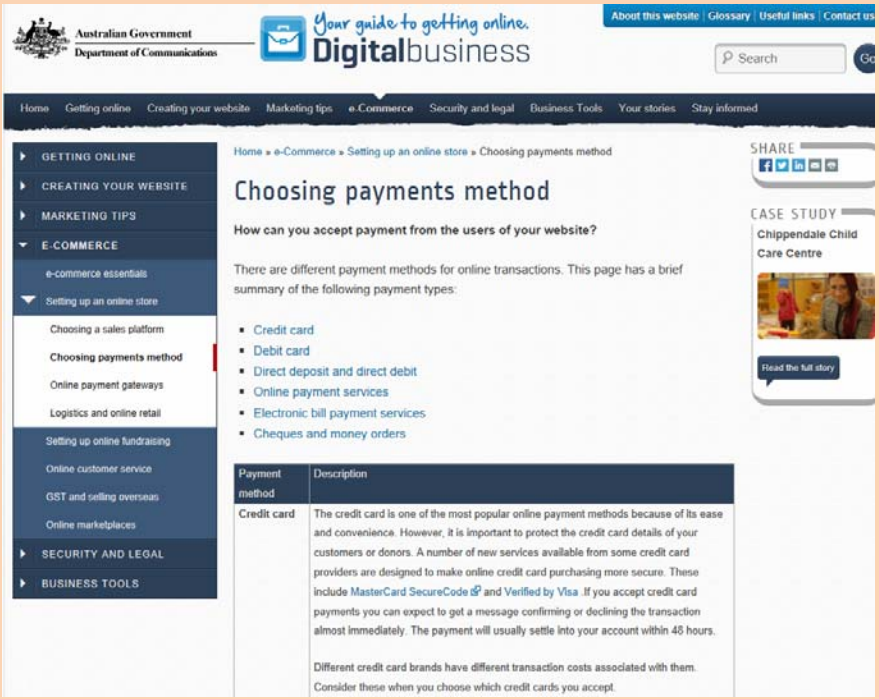
Regarding surcharges for card payments, competition authorities around the world (Australia, EU, US) have taken action to lower the interchange fees set by the two leading card schemes Visa and MasterCard.

The EU is adopting legislation that would cap the level of interchange fees across the 28-nation bloc. It would also prohibit retailers from applying surcharges to such card payments (because the interchange fees would have been significantly lowered by the cap)[73].

Note also that Australia's Government Department of Communications is providing information of the different methods of payment on its website.

[73] http://europa.eu/rapid/press-release_MEMO-13-719_en.htm

Australian's Government Department of Communications lists on its website[74] the different payment methods for online transactions, with tips for online retailers on what to look out for, including on the need to protect the payment details of customers as they are sensitive pieces of information.



4.7 Consumer rights and trust

The policy responses

A strong set of consumer rights can help to protect digital consumers when they buy goods and services online.

These rights include:

- Information on who is operating the website
- Protection against unfair commercial practices, leading consumers into purchasing a good they would not have bought without having been unlawfully led into the transaction
- Clear information on the ordering process
- Price transparency. No hidden extra charges
- Right to cancel a sales contract within a cooling off period, including the right to return goods and obtain a refund

[74] http://www.digitalbusiness.gov.au/e-commerce/setting-up-an-online-store/choosing-your-payments-method/

- Information on when the goods will be delivered and on the cost of delivery and return of the goods
- Information on how digital goods such as music, films or software can be listened to/viewed or downloaded, and whether they can be used on multiple devices
- Easy to use complaint handling and dispute resolution procedures.

Online retailers can guarantee these rights in their standard terms and conditions. Trustmarks (see below) can also serve to inform consumers that these basic core rights are guaranteed.

Laws can also be adopted to guarantee that consumers are always granted these rights. This is what many countries have already done. EU's consumer rights Directive for instance gives a core set of rights to EU citizens when they buy from EU-based online retailers[75].

A step further could also be achieved by adopting standard contracts to which digital consumers and online sellers could decide to adhere to on a voluntary basis and which would govern their entire online relationship. This is what the European Union is trying to do, with the adoption of a regulation[76] on a common European sales law. Negotiations are long and difficult though. The initiative is innovative as the parties to an online sales contract would be able to decide to be exclusively governed by the rules of the European sales law, thereby by-passing national legal regimes and the standard terms and conditions of the online retailer.

Trusmarks

One of the main concerns of digital consumers is that they must feel confident and trust the website from which they are ordering a good or a service. This is very likely to be the case, when they purchase from well-known e-commerce sites such as Amazon, but they may be less sure when making purchases from other sites, particularly if the site is in a foreign country.

Trustmarks can re-assure consumers of their reliability. They show that a website complies with a set of service quality and security requirements.

Trustmark schemes can be run by government bodies, non-profit organisations, industry or trade organisations, or by private businesses.

[75] http://ec.europa.eu/justice/consumer-marketing/rights-contracts/directive/index_en.htm

[76] http://ec.europa.eu/justice/contract/files/common_sales_law/regulation_sales_law_en.pdf

Example of a widely used trustmark on UK websites

SafeBuy certifies that shoppers can trust a website because the retailer adheres to the rules and regulations on distance selling but also more generally, on privacy protection, child protection and security of payment transactions[77].

However, a multitude of trustmarks have appeared, leading to a so-called "trustmark jungle" leaving consumers confused as to which ones they can trust. Furthermore, most trustmarks operate at a national level[78].

The development of internationally recognised trustmarks would help to boost the e-commerce market.

The EU is currently assessing how to reach an EU-wide trust mark scheme and to establish cooperation platforms on the governance of trust mark systems[79].

We see here that regulators could have a role to play to foster the establishment of trustmarks and they could also supervise or approve their operation, thereby increasing the level of trust.

Conclusions and recommendations

- Clear rights and obligations should be given to consumers in the laws.
- Given the increasing number of cross-border transactions, supra-national and regional laws should be adopted to give consumers the same rights when they shop from foreign websites, compared to when they shop domestically.
- Regulators should provide clear information on the rights and obligations of digital consumers
- Regulators have a role to play to foster the development of easily recognisable trustmarks in collaboration with the industry and consumer organisations
- Regulators could take a leading role in the supervision and operation of the trustmark systems

4.8 Delivery

Digital consumers need to be assured that they receive their ordered goods on time and in good order. There is usually no problem for national transactions.

---

[77] https://www.safebuy.org.uk/index.html

[78] http://www.konsumenteuropa.se/en/News/Press-releases/Press-releases-2013/Important-to-be-able-to-trust-a-trust-mark/

[79] http://ec.europa.eu/digital-agenda/en/news/eu-online-trustmarks-—-building-digital-confidence-europe-smart-20110022

The European Commission published a roadmap at the end of 2013[80] which highlights in particular the need for more transparency and information on the available delivery options, for more, better and more affordable delivery solutions and for enhanced complaint handling and redress mechanisms for consumers, which should be jointly ensured by delivery operators, e-retailers and consumer associations.

4.9 Consumer redress and consumer education

Even if a strong set of rights are given to consumers, a key aspect is to make sure that consumers can seek redress when things go wrong.

As illustrated by BEUC, the European consumer protection authority, consumer redress remains an issue, especially in a dispute between a consumer located in country A, and an online retailer established in country B.

BEUC statement about enforcement:

'The lack of effective enforcement is a key problem in consumer protection. At the same time, it is a complex problem to tackle, as effective enforcement depends on multiple factors such as the enforcement structure and traditions at national level, strong public authorities; the economic climate; the strength and experience of consumer organisations; the possibility for easy redress etc.

In addition to national or cross-border instances, more and more infringements are of a genuinely European dimension, for instance when a large company targets consumers in many EU member states with the same or similar unfair practices.

We therefore need more cooperation among various enforcement bodies and organisations as well as to strengthen the powers and sanctions available to them'.

Source: BEUC website[81]

The OECD adopted a recommendation[82] on consumer dispute resolution and redress in 2007, which proposes common principles for member countries on mechanisms for consumers to resolve disputes and obtain redress for economic harm, including when the purchase goods and services across borders.

It provides that member countries should review their existing dispute resolution and redress frameworks to ensure that they provide consumers with access to fair, easy to use, timely, and effective dispute resolution and redress without unnecessary cost or burden.

Member countries should encourage businesses and industry groups to provide consumers with voluntary mechanisms to informally, and at the earliest possible stages, resolve their disputes and obtain redress as appropriate.

In many countries, formal complaint processes have been established through which individuals or groups of individuals can bring problems to the attention of consumer protection authorities. The OECD's

[80] http://europa.eu/rapid/press-release_IP-13-1254_en.htm?locale=en

[81] http://www.beuc.eu/consumer-rights-and-enforcement/enforcement

[82] http://www.oecd.org/internet/consumer/38960101.pdf

Consumer Protection Policy Toolkit[83] refers to concrete examples in Belgium, Chile, Denmark, Finland, France, Korea, Sweden, Switzerland and the United States.

OECD policy guidance on mobile and online payments specifies that:

'Governments, payment providers, merchants and other stakeholders should develop low-cost, easy to use alternative dispute resolution and redress mechanisms which would, inter alia, facilitate resolving claims over payments involving low-value transactions. Such mechanisms could include the development of effective online dispute resolution systems. Alternative dispute resolution and redress mechanisms should not prevent parties from pursuing other forms of redress, as permitted by applicable law'

Source: OECD[84]

Consumer education

Educating consumers about their rights and how to use them is becoming a priority for many governments.

The European Commission regularly publishes for the EU 28 member states a scoreboard[85] showing how the European Union is performing in relation to EU consumers and warning of potential problems.

The July 2013 edition of the Consumer Conditions Scoreboard highlights that a significant number of European consumers do not know their rights and how to use them. 'Only 12%of respondents were able to answer correctly four questions testing their basic consumer knowledge'.

This reveals the need to launch information and education campaigns, and this is clearly a role for governments and regulators.

Consumers International[86], the world federation of consumer groups, has translated this into a right to consumer education, i.e. a right to acquire knowledge and skills needed to make informed, confident choices about goods and services, while being aware of basic consumer rights and responsibilities and how to act on them.

Conclusions and recommendations

Contrary to other areas, consumer education and redress does not demand a change of laws. Government and/or regulators can do a lot to improve the situation. For instance, they can:

- provide information to citizens on their rights and obligations through education campaigns and by providing clear information on their websites
- receive complaints from consumers by operating online complaint-submission mechanisms
- provide information on the available dispute resolution mechanisms
- approve industry mechanisms to ensure redress

[83] OECD Consumer Protection Policy Toolkit, 2010, http://www.keepeek.com/Digital-Asset-Management/oecd/governance/consumer-policy-toolkit_9789264079663-en#page2

[84] http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/cp(2011)24/final&doclanguage=en

[85] http://ec.europa.eu/consumers/consumer_research/editions/docs/9th_edition_scoreboard_en.pdf

[86] http://www.consumersinternational.org/who-we-are/about-us/

5. Targeted initiatives - specific market players

In this section, we describe some recent interventions that are aimed at addressing the conduct of new market players, which have become particularly important in the e-commerce ecosystem. Some of these are regulatory interventions, while others are driven by the market players themselves or are private-public partnerships.

Search engines

Sector specific rules (e.g. on privacy) apply to many of the activities of search engines, but like most operators in the e-commerce ecosystem, search engines are not 'regulated' to the same extent as other types of operator like telecommunications operators, financial institutions or postal operators. There is no single law that covers the activity of search engines.

In the absence of specific ex ante regulation, competition law is quite often the only remedy available against search engine providers that may be abusing a dominant market position. The FTC and the European Commission have recently carried out investigations relating to some of Google's practices but arrived at different conclusions

The European Commission has used its competition law enforcement powers to investigate Google for an alleged abuse of a dominant position in online search and search advertising[87].

One of the main concerns was that Google was discriminating in favour of its own specialised search services on its web page (e.g. specialised search services for flights or hotels). Search engines that focus on narrowly defined categories of content such as flights or hotels are referred to as “vertical” search engines as opposed to general purpose or “horizontal” search engines.

In order to avoid a potential fine of up to 10% of its annual worldwide turnover, Google made commitments including relating to the comparable display of specialised search services offered by rivals. Google has accepted to guarantee that whenever it promotes its own specialised search services on its web page, the services of three rivals, selected through an auction, will also be displayed in a way that is clearly visible to users and comparable to the way in which Google displays its own services.

When finally approved, the deal will mean that people who search on Google’s local sites in Europe will see results laid out differently from those in other countries.

In the US, a similar investigation by the Federal Trade Commission of Google’s vertical search business was closed in January 2013 without sanctions. The FTC concluded that Google’s actions to promote its own vertical content on the Google search results page was “a product design change with a legitimate business justification” to improve the overall quality of Google’s search product, rather than to intentionally harm competitors[88].

[87] http://europa.eu/rapid/press-release_IP-14-116_en.htm

[88] http://www.ftc.gov/system/files/documents/public_statements/295971/130103googlesearchstmtofcomm.pdf

Online games and in app purchases

Regarding apps, a number of interventions have taken place in recent months to frame the way in which app service providers are offering their services.

In the EU, the network of national consumer protection enforcement authorities has developed four principles on online games and in-app purchases[89]:

- Games advertised as "free" should not mislead consumers about the true costs involved.
- Games should not contain direct exhortations to children to buy items in a game or to persuade an adult to buy items for them.
- Consumers should be adequately informed about the payment arrangements and purchases should not be debited through default settings without the consumers' explicit consent.
- Traders should provide an email address so that consumers can contact them in case of queries or complaints.

In the US, the Federal Trade Commission has taken action against Apple for unfairly charging consumers for in-app purchases incurred by children without their parents' consent. Apple failed to notify parents that entering their password would approve a purchase and then open a 15-minute window in which unlimited charges could be made without further authentication. Apple was required to change its billing practices by end March 2014 and to pay refunds totalling $32.5m[90].

A lawsuit is open against Google in the US regarding a similar 30-minute window in which in-app purchases can be made without further authentication in games apps purchased from its Play store[91].

Social media

Industry has developed self-regulation in the area of the protection of children. Examples of self-regulatory initiatives in Europe taken under the umbrella of the EU safer internet programme include[92]:

- CEO coalition to make the internet a better place for kids.
- The safer social networking principles for the EU[93].
- European framework for safer mobile use by younger teenagers and children.

The safer social networking principles for the EU highlight highlights the importance of the respective roles of parents, teachers (and other carers), governments and public bodies, law enforcement, civil society and the users themselves. They say that governments and public bodies should:

- Provide children and young people with the knowledge and skills to navigate the internet safely
- Make sure that e-safety curricula are delivered in schools

---

89 http://europa.eu/rapid/press-release_IP-14-187_en.htm

90 http://www.ftc.gov/news-events/press-releases/2014/03/ftc-approves-final-order-case-about-apple-inc-charging-kids-app

91 http://www.theguardian.com/technology/2014/mar/11/google-us-lawsuit-in-app-purchases

92 http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids

93 https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

- Ensure that law enforcement agents are equipped with appropriate training, tools and resources needed to combat criminal activity conducted online
- Work together to ensure that frameworks for cross-border coordination are effective and efficient

Cloud

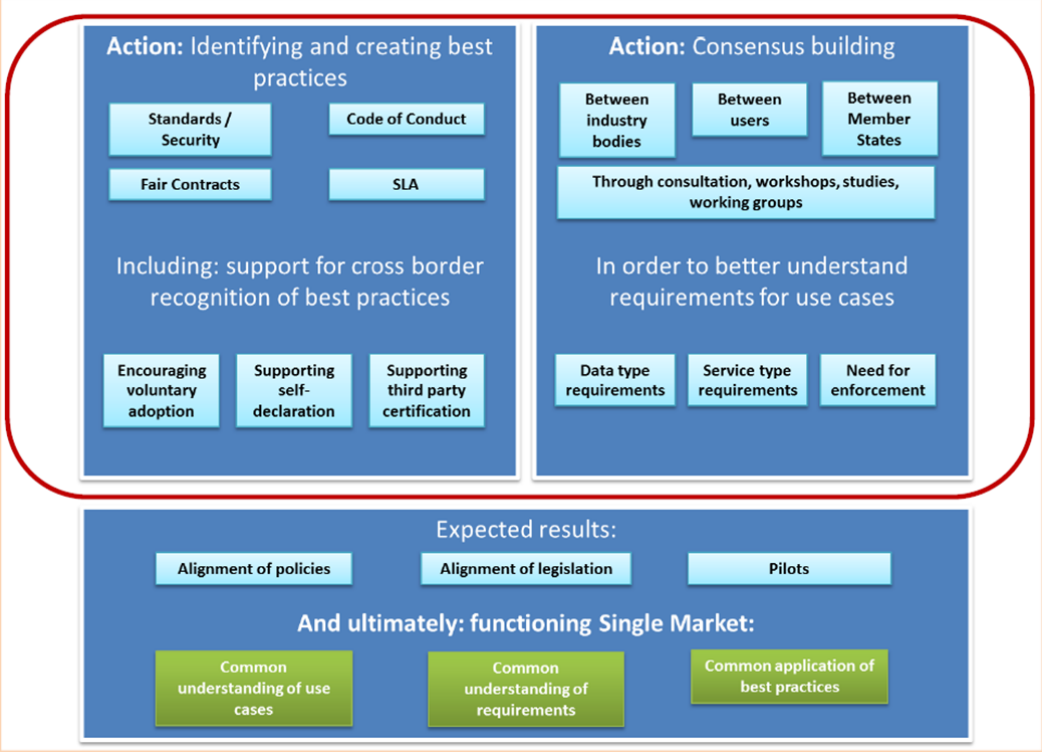
In order to boost trust and confidence in cloud services, industry and public-private partnerships can develop best practices.

The European Cloud Partnership is an example. It brings together industry and the public sector to develop a set of "non-legislative, voluntary measures" for a Trusted Cloud Europe.[94] Best practices are being developed covering legal and operational guidelines as well as technical standards. These include a code of conduct on data protection, model safe and fair contract terms and conditions, and model terms for service level agreements.

Cloud providers could voluntarily adopt the best practices, and would then be able to market their services as complying with the Trusted Cloud Europe framework.

[94] http://europa.eu/rapid/press-release_IP-14-296_en.htm

Figure 10 - Trusted Cloud Europe framework



The following table illustrates the initiatives taken by some countries to promote and frame cloud computing.

Country	*Initiative taken to promote cloud computing*
Germany	Trusted cloud Funding initiative of the Federal Ministry of Education and Research in data protection, data security, privacy, identity and access management in cloud services (also for setting up guidelines)
Spain	Cloud computing Challenges and opportunities adopted by ONTSI (National Observatory for Telecommunications and Information Society) in 2012. Study analysing the economic, social and environmental impact of cloud computing in Spain.
France	Investment by the state in two important cloud computing services : Cloudwatt by Orange and Thalès and Numergy by SFR and Bull
Italy	Digital agenda for Italy includes references on how to develop cloud computing in Italy DigitPA recommendations on the use of cloud computing in the public administration
United Kingdom	G-Cloud Programme Cross government initiative led by Ministry of Justice introducing cloud ICT services into public sector (government, local authorities). The 4th version of the G-Cloud went live on October 29, 2013 with

	1,000 businesses offering about 13,000 services to public sector buyers.
Australia	The Australian Computer Society was asked by the government to investigate the case for a voluntary Cloud Protocol. Conclusion (November 2013): no demand from main cloud suppliers to participate, therefore a voluntary code will be ineffective[95].
New Zealand	Voluntary Cloud Computing Code of Practice developed and operated by the Institute of IT Professionals New Zealand. Cloud providers that sign-up to the code have to disclose important details about their cloud products and services upfront. The code lists the information that must be disclosed, e.g. security standards and practices followed, location(s) where data is hosted, how consumers can access data both during service and after the service has ceased, format and costs for data transportability, etc. The disclosures are reviewed by the body that operates the code ("the CloudCode team"), which also resolves disputes. Signatories can use a special logo.

Source: Cullen Research

6. Conclusion

A largely non-regulated eco-system

Contrary to the telecommunications, energy, postal, financial or audiovisual sectors, many of the operators in the online eco-system are unregulated actors. No single regulator or authority in a country is responsible to supervise and enforce a set of binding rules on these operators. Facebook, Google, Amazon, Yahoo need to respect the laws of the country in which they operate but they are not supervised to the same extent as telecommunications operators or financial institutions.

We have covered some of the most burning cross-cutting regulatory questions that should be addressed as a matter of priority to ensure that digital consumers are fully empowered.

Some of these areas may require changes to the legislative framework. We have tried to show that some regulators around the world are picking up on some important new roles and that there is scope for an accrued role to be played by them.

[95] http://www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol and http://www.acs.org.au/__data/assets/pdf_file/0017/27800/ACS-Cloud-Protocol-Consultation-Report.pdf

Annex 1 / Appendix 1 (if needed)