



GSR

2009

Discussion Paper

Comments are welcome and should be sent by 20 November 2009 to GSR09@itu.int



Work in progress, for discussion purposes

Please send your comments on this paper at: gsr@itu.int before 20 November 2009.

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

Consumer Protection: meeting the expectations of the connected consumer

Author: Rosalind Stevens, Senior Telecomms Expert

1. INTRODUCTION

Throughout the world, access to the Internet is increasingly considered as an “essential service”. Whether this be through access to high-speed broadband or a dial-up Internet connection, via a fixed or cellular mobile phone line, the need to be connected and “always on” impacts on the way in which business is transacted and the way in which consumers react. Being connected has become synonymous with access to markets, to information, to social networks and to education.

Rapid technological change and its impact on consumer behavior is taking place within an increasingly liberalized market place in which the global drive to compete brings new challenges to both existing and nascent regulatory authorities.

In order to ensure that consumers benefit fully from the services the Internet has to offer, regulators need to ensure that networks are efficient and reliable, widely accessible (including in remote rural areas) and affordable. In order to encourage private investment in the infrastructure needed to meet those objectives, regulators need to create an environment in which communications investment is commercially viable, whilst at the same time promoting competition to increase choice and drive down prices. The challenge for regulation is to promote favorable market conditions in which competition can flourish and foster innovation, whilst at the same time ensuring that consumers’ interests are protected.

If competition is to benefit consumers, they must be able to exercise choice.¹ The assumed regulatory “best practice” to date has been to focus on the consumer detriment that arises where there are information asymmetries in favor of the supplier. By ensuring consumers are well informed, the market will work effectively through increased competition between suppliers, both in terms of price, quality and choice of products on offer. In short, the assumption is that competition, when managed appropriately, benefits consumers. In other words, when competition works well, regulation is not needed.

This approach is rooted in the traditional, neo-classical economic theory of “rational” consumer behavior, whereby consumers have a set of preferences. By exercising those preferences (which are assumed to be stable) and making rational choices consumers are able to maximize both their own self-interest and wider consumer welfare.

From a consumer perspective, more competition may lead to a bombardment of marketing material, masquerading as information. This is especially the case where access to high-speed broadband connections makes them an advertising target easily accessible day and night. This may leave consumers feeling overwhelmed and struggling to differentiate between the choice of products and services on offer. Consumers can suffer from “information overload”.

If consumers become overloaded, or cannot rely on the truthfulness or accuracy of information, they may become “paralyzed”. Thus they are reluctant to switch between services and/or suppliers for fear of making the “wrong choice”. Or, they may choose service bundles and long-term contracts that they do not need. Or, they may be enticed by special offers like a free handset or modem, and later find themselves “locked in” to contracts that offer poor value for money. Overall consumers may be dissatisfied because they feel that they have “failed” in some way by not getting the best deal and/or the latest technology/service on offer.²

In the ‘always-on’ environment, citizens and consumers may also be unaware of how to protect themselves and their families from harmful or offensive content. In some cases this may make them reluctant to engage fully in the on-line environment.

This paper considers the changing needs and expectations of ICT consumers (section 2). There are a number of ways in which regulators might meet those needs and expectations. Regulators might provide price (section 4.1) and quality of service (section 4.2) information. They might also try and educate consumers (section 4). They might play a role in handling complaints (section 4.4). Regulators also need to consider the best way to address trust and security issues (section 5). Last, it considers whether there are regulatory gaps that should be addressed (section 6).

2. CONSUMER NEEDS AND EXPECTATIONS

In order to ascertain the most appropriate level of regulatory intervention, ICT regulators to understand consumers’ needs and expectations. Those expectations may vary according to the availability, accessibility and affordability of services. Where there is no universal access to basic telecommunications infrastructure, for example, the need for affordable, reliable services is likely to be far more important than having a choice of supplier. Nevertheless consumers expectations are likely to be disappointed if the quality of service is poor, for example if there are delays and jitter on the line.

Consumers may purchase a bundle of services without fully understanding what is being offered. The broadband service may work well for voice calls and emails but may struggle when downloading live television or video on demand services. Gaming enthusiasts using games consoles with versatile plug and play technologies³ to play interactive games through their PC can also download and share games with friends, family and other users remotely. They can also use the box to surf the Internet and download news, weather and email services and even TV catch-up services. However this might attract unexpected and unwelcome additional charges from their broadband provider if they exceed their contracted download limits.

The high levels of traffic these activities generate may result in degradation of some or all aspects of the service. This is unlikely to be acceptable to consumers who expect to be able to access and distribute content and run any applications or services of their choice. Indeed irrespective of their different needs, ICT consumers are likely to expect that their Internet service should provide a fast enough transmission speed to be able to support full use of common Internet features such as access to online services and applications, including multi-media, web 2.0 functionalities and file transfers. Consumers are also likely to expect that this level of service is available at a reasonable price. Inevitably there will need to be some sort of “trade off” between the quality of service provided and the price of package.

From a regulatory perspective, it may be difficult to distinguish between those elements of the service that can be regulated such as the fixed line service, from those that can not, such as the gaming consoles and the content that the gamers are sharing. This presents new challenges to regulators. A suitable response may require a combination of consumer education initiatives and non-ICT specific regulatory intervention. This could include the application of competition law powers, reliance on general consumer protection law, and data protection legislation. Such an approach may be more effective than constantly trying to play “catch up” with technological innovation.

Regulators also need to identify and address the needs of vulnerable consumers, including children, who may not be adequately equipped to defend their own interests on the basis of information alone. As more public services are delivered over the Internet (e-government, e-health, e-education, etc.), it becomes increasingly important to ensure that the networks and connections that underlie these applications are secure and reliable.

Consumers are exposed because their personal data, including sensitive personal information, is being shared across the networks, including for advertising purposes. The emphasis on “traditional” advertising through the media had shifted towards more direct personalized marketing through the Internet or contextual advertizing through SMS or MMS. The Internet search engine, Google, recently launched a system that provides advertising to web users based on their previous online activities. The system uses “cookies” to track users as they visit different websites that show advertisements through the Google Ad Sense programme. Whilst some consumers have welcomed tailored marketing, others may feel it invades their personal privacy.

Increasingly there are demands on telecommunication and ICT regulators to define personal privacy in the on-line space and to find ways to protect consumers from potential threats. Regulators may also be required to develop a security framework in which service providers are required to operate and/or act as enforcement agency for various measures.

3 CONSUMER PROTECTION FRAMEWORK

The ICT sector is a conduit for economic development, innovation and competitive growth. Confident, informed and empowered consumers help drive growth and innovation. ICT regulators therefore recognize the value of consumer protection measures for improving consumer confidence and stimulating demand. Consumers want assurance that their rights are protected in relation to privacy and data security, that they can rely on the quality and availability of services, and that they can trust the information they receive about the services on offer. In short, consumer protection can be part of a proactive, dynamic approach by regulators.⁴

A growing number of countries have developed specific consumer protection regulations/legislation for ICT customers (Table 1). In some cases the ICT regulator has primary responsibility for enforcement, in others responsibility is shared with, or assigned to a designated consumer protection agency. This section provides examples of different approaches adopted.

Table 1: Countries with specific telecommunication consumer protection regulation/legislation

Africa	Angola, Burkina Faso, Cape Verde, Equatorial Guinea, Gambia, Malawi, Nigeria, Rwanda, St Tome and Principe, Senegal, South Africa, Tanzania, Zambia
Americas	Brazil, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guyana, Jamaica, Nicaragua, Panama, Paraguay, Peru, St Vincent and the Grenadines, United States
Arab States	Algeria, Egypt, Mauritania, Oman, Saudi Arabia, Tunisia, United Arab Emirates
Asia and Pacific	Australia, Bangladesh, China, Iran, Kiribati, Korea (Rep.), Nepal, Pakistan, Samoa, Singapore, Sri Lanka, Thailand
Europe and CIS countries	Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Ireland, Kyrgyzstan, Liechtenstein, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Poland, Portugal, Romania, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom

Source: ITU World Telecommunication Regulatory Database, www.itu.int/icteye

In Australia, a robust protection framework protects consumers. This is underpinned by a statutory communications and media regulation body, the Australian Communications and Media Authority (ACMA), by general consumer protection law and a by a telecoms interest group. ACMA's duties and responsibilities are far-reaching. They include the investigation of complaints about online content and gambling services;⁵ encouraging development of codes of practice for Internet service providers and online content service providers and monitoring compliance; and informing the community about Internet safety risks, particularly those relating to children. The Australian Telecommunications User Group, ATUG,⁶ a non-profit organization, aims to ensure that Australian telecommunications users have access to a wide range of high quality, low price communications services. Separately, the Consumer Telecommunications Network (CTN)⁷, a national coalition of

consumer and community organizations, is concerned with access and equity for residential ICT users.

Consumer protection in Australia is likely to be further strengthened through a proposed new single consumer law based on the consumer protection provisions of the Trade Practices Act 1974. The new law would include a national prohibition on unfair contract terms, and new civil penalties for breaches of the law. It would also give regulators new powers of enforcement, including substantiation notices, infringement notices and public warnings.⁸

In Kenya, general consumer rights that were previously enshrined across different pieces of legislation are now consolidated within the Consumer Protection Bill 2007. The Bill provides for specific rights in relation to the supply of telecommunications services and products, which should strengthen the consumer protection framework. In addition to setting consumers' rights, the Bill sets consumers' responsibilities, making consumers a fully-fledged stakeholder in this area and shifting the focus away from consumers' passive attitude towards a more pro-active, informed one.

Some African regulators have also established specific divisions that concentrate on consumer protection issues. The Consumer Affairs Bureau of the Nigerian Communications Commission (NCC)⁹ has a strong emphasis on consumer empowerment. Its objective is to create a visible and credible consumer voice, inter alia, by providing a one-stop shop for consumer information. The Bureau produces fact-sheets and brochures and organizes public and local communities out-reach programs. It is not solely an information provider however. The Bureau plays an important monitoring role, which helps to detect unscrupulous industry practices and protect consumers from them. The Bureau's help-desk responds to consumers' enquiries, investigates complaints and where possible tries to resolve them. This is an important part of a consumer protection framework, as explained in section 4.4 below.

It is not always the ICT regulator that has sole responsibility for protecting ICT consumers. In the United States, the Federal Trade Commission (FTC) is a law enforcement agency with both consumer protection and competition responsibilities that cut across a broad range of sectors of the economy. The FTC's responsibilities include administering consumer protection legislation; including telemarketing sales and pay per call rules. It helps to promote consumers' interests by sharing its expertise with both US federal and state and international government agencies. The FTC's Bureau of Consumer Protection is responsible for fraud prevention, deception, and unfair business practices across the marketplace. The Bureau undertakes research, arranges public hearings, workshops and conferences. It also develops plain-language consumer education programmes. The consumer section of its website stresses the importance of education as the "first line of defense against fraud or deception."¹⁰ Consumers are encouraged to contact the Bureau for their information needs or to file a complaint if they have been the subjects of fraud or identity theft.

In some instances, independent consumer organizations with responsibilities for a wide variety of products and services may play a powerful consumer protection role. Although such bodies often have limited resources to enable them to specialize in any one sector, including communications, in some instances lobbying on a single issue can prove effective. The League for the Defense of the Consumer in Benin (LDCB)¹¹ campaigns for consumers on a very broad range of issues ranging from the

quality of food to mobile phone tariffs. It highlights consumer protection matters in the press, through public forums, and through regulators. Its lobbying has proven very successful in achieving reductions in mobile phone tariffs. Following recognition of the importance of affordable access to the Internet through GSM networks and in the absence of price control regulation, the Benin government agreed a protocol with GSM operators for a 20-30% reduction in mobile phone charges. The LDCB organized a press conference where it put the operators on notice of the consequences of non-adherence to the protocol within the stipulated time frame. LDCB undertook research to establish whether the operators had implemented the reductions. It compared tariffs between operators and publicized its results at another press conference. Although it has not succeeded in achieving all of the reductions it wanted, the initiative demonstrates the potential for consumer focused campaigns to improve consumer awareness of their rights.

Less common are consumers that are pro-active in organizing themselves. In Uganda, telecommunications users recently established a consumer protection association. This arose because of a specific problem of consumers being bombarded with commercial text messages. When consumers tried to unsubscribe to the messages they were charged for the messages. Following unsuccessful attempts to challenge the ICT providers, a group of consumers, and acting with members of the National ICT for Development I-Network, formed the Ugandan ICT Consumer Protection Association¹² (UCIPA). UCIPA membership is open to all ICT consumers and stakeholders, but it is very much consumer driven. Although it is early days to assess its impact, UCIPA wants to develop a collective voice for ICT consumer's concerns, such as billing, pricing and quality of service issues.

Given that ICT services extend beyond national boundaries, it is worth considering whether consumer protection needs may be better served through regionally coordinated regulatory initiatives. The Central African Economic and Monetary Community's (CEMAC)¹³ Consumer Protection Directive¹⁴ (Box 1) covers a wide range of typical problems facing ICT consumers, including in relation to the security and protection of their personal data.

Box 1: Summary of CEMAC's Consumer Protection Directive provisions

Right to privacy

- Confidentiality of electronic communications.
- Right not to have automatic callbacks.
- Prohibition of unsolicited marketing material.
- Right not to be listed in a telephone directory and/or for a consumer's telephone number to be given to a third party.

Right of access to information

- Access to transparent, up-to-date information about prices, services and terms of trade.
- Provision of a customer contract with as a minimum, details of the name and address of the service provider, the services offered, their quality and installation, service support, price and tariff structure,

the duration of the contract and arrangements for contract renewal and/or termination; compensation schemes; arrangements for recovery of debt; arrangements for handling complaints/disputes; circumstances under which the contract may be terminated.

Billing arrangements

- Tariffs should correspond to the service demanded by the consumer, who should not be made to pay for ancillary services that they do not need. Consumers have a right to a non-itemized bill and where itemized bills are provided these should be in accordance with the consumer's right to privacy.
- Measures taken in relation to non-payment of bills should be proportionate and non-discriminatory; with the consumer given notice of termination of/interruption to service. Prior to disconnection consumers have the right to a reduced service that allows them to make emergency calls.

Quality and availability of service

- ICT providers must provide quality of service and must publish information about initial supply times, fault rates and repair times. They must provide means of redress in case of failure or interruption to service. Operators must put technical and organizational measures in place to guarantee the integrity of their networks and services and that there is guaranteed access to emergency calls.

Dispute handling

- Consumers have the right of access to out-of-court procedures for the settlement of disputes, which must be simple, transparent, free-of-charge to consumers and allow for a fair and speedy settlement.

Handling of personal data

- User data should be deleted or anonymized after transmission (except where governments require providers to retain details for security purposes (when it must be retained for a maximum of 2 years). Data retained for billing purposes must only be stored for the time necessary to allow for disputes to be resolved. Data may be used for commercial purposes but only with the consumer's prior consent, which may be withdrawn at any time.

Cyber security

- Governments must put in place a policy and technical measures to safeguard the security of electronic communications through national legislation and better cooperation regionally and international.

Source: CEMAC

Another new regional initiative, the African Network of Consumer Associations of Information and Communication Technologies (ANCA-ICT)¹⁵ was set up with the overarching goal of advancing the interests of telecommunication consumers across the continent. The main aims of the group are to put pressure on providers to reduce prices, to help the optimization of resources and to contribute to promoting the quality of investment for an information society for all.

Consumer protection for ICT consumers may be complemented and/or strengthened by a strong general consumer protection framework¹⁶. In Europe, in addition to the comprehensive framework of specific measures for users of electronic communications services, the EU has developed an overarching consumer policy strategy. The aim of the strategy is to address common problems that individuals

(and/or individual regulators) lack the capacity to tackle on their own. The measures seek to ensure that markets are fair and transparent, that consumers are equipped to make rational choices and that consumers take responsibility to promote their own interests. The strategy is based on the assumption that empowered consumers are consumers whose welfare is maximized, provided that the consumer protection framework is effective. It specifically recognizes the potential for e-commerce to improve choice, make prices more competitive and develop markets and services more tailored to individual needs. On the other hand, it recognizes the challenges that e-commerce presents to the traditional modes of regulation and self-regulation. In brief, existing consumer rights may not be fit-for-purpose in the digital age¹⁷ and measures may not be effective if implemented at a national level.

3.1 CO- AND SELF-REGULATION

Notwithstanding the importance of a robust consumer protection framework for stimulating ICT growth, regulatory measures are not without cost. Irrespective of how they are financed the cost will ultimately be borne by ICT consumers, either through the costs of funding the regulator and/or through the transfer of the costs of compliance from the provider to the consumer through the price mechanism. Of course, where regulation is effective, consumers will be net beneficiaries of regulatory intervention. Nevertheless it is essential that consumer protection measures are proportionate to the actual or potential harm consumers face. As such regulators may wish to explore the potential for devolving some responsibility to the providers. Reliance on complete self-regulation is only likely to be effective where ICT providers share the same objectives as the wider consumer and social protection agenda. More commonly, regulators will tend to favor a co-regulatory approach to consumer protection.

In Bahrain, for example, the Telecomm Regulatory Authority (TRA), Business Users Advisory Group (BAG) and the Consumer Rights Group (CRG), have been working together to identify solutions to actual or potential problems consumers face. Rather than imposing potentially unnecessary regulation on providers, the TRA's initial approach has been to publish draft Consumer Protection Guidelines for consultation. The Guidelines, inter alia, clarify how licensed operators should behave in order to respect and protect consumers' rights; thereby encouraging best practice and promoting the provision of high quality services. The objective is to enhance consumer awareness of their rights. In turn this should deter providers from abusing those rights. TRA has made clear its intention to use its backstop powers to regulate behavior if providers do not adhere to the Guidelines. By setting out clearly what is expected, by actively monitoring progress, by being prepared to intervene where necessary, the Guidelines should satisfy the dual purpose of promoting effective competition and ensuring that consumers are treated fairly.

In Papua New Guinea (PNG), where there are low levels of access and high charges for Internet use, the Independent Consumer and Competition Commission (ICCC) has developed Code of Practice for Internet Service Providers¹⁸. The regulator recognizes the importance of improving consumer confidence in order to stimulate demand and promote growth. The Commission has the powers to develop and enforce codes but chose to consult widely with stakeholders before doing so. Broadly, the Code is a framework for best practice in relation to the provision of information, protection of data, and

complaints handling for consumers. It is also designed to improve consumer relations with the ICT providers. A further requirement of the Code is that operators must co-operate and assist law enforcement agencies and government regulatory agencies to prevent the use of the Internet for criminal activity. This includes a requirement to close down or block access to sites being used for criminal purposes and/or to propagate consumer viruses.

In Malaysia, one of the first countries to introduce specific laws covering the Internet, the focus has nevertheless been on self regulation of the industry. This is due to a desire not to fetter the pace and potential of convergence. The NRA, the Communications and Multimedia Commission has established an independent body, the Communications and Multimedia Forum, to develop consumer codes of practice. The content of the codes is based on input from industry and consumers. Taking a pro-active approach to promote consumer awareness, the Codes were presented in a series of road-shows throughout the country. Unfortunately the codes generated little public interest.¹⁹

Co- and self-regulatory initiatives are more likely to be successful where underpinned by consumer support and the regulator's ability (and willingness) to intervene where necessary. ACMA has recently developed an industry code on mobile premium services (Box 2). The Code is part of ACMA's strategy and new regulatory package for protecting consumers of premium short message services (SMS). Adherence to the code is obligatory and ACMA intends to closely monitor it.

Regulators must nevertheless maintain a pragmatic approach. There may be technical barriers, such as limited availability of international bandwidth, that render compliance with codes of practice physically impossible. Mobile phone operators may not be able to control minors' use of their services, even if they have special measures in place. What is important is that providers do not "over-promise" on what they can deliver and it is here that consumer education should take central stage within the consumer protection framework.

Box 2: Australia's industry code on mobile premium services

The code sets out detailed rules covering a range of important matters including procedures to be followed for subscribing to premium SMS services²⁰; the banning of advertisements targeted at children under 15; strict rules about how advertisements (and charges) are displayed; and improved complaints handling obligations of companies supplying premium SMS services."

One of the elements included in the package provides for "Additional protections for minors"

A ban on advertisements for premium SMS services targeted at children aged under 15.

Advertising which may encourage minors to use the service to carry a warning for people under 18 years to ask the account holder before using the service.

Content suppliers to consider a special set of factors when investigating complaints involving minors' use of mobile premium services."

Source: ACMA Australia, at: www.acma.gov.au/WEB/STANDARD/pc=PC_311730; see also www.commsalliance.com.au/_data/page/20547/C637_2009.pdf

4 CONSUMER EDUCATION

In order to ensure that consumers' needs and expectations are met, regulators need to be confident that consumers are aware of their rights (and responsibilities) and have the right information to make rational choices. The key factors for consumers to consider are price, quality-of-service and the trade-off between the two. Information must be easy to understand, easy to access and easy to compare if consumers. The regulator's role is to ensure that the right information is available, that it is accurate and that it is reliable.

4.1 PRICE INFORMATION

One of the key factors that continue to determine either the choice of provider (where choice is available) or the decision to use an Internet service is price. This may be a value for money decision or simply a question of affordability. In order to compare prices, consumers need access to reliable, comparable information. However, although ICT providers may publish details of enticing price offers they are naturally reluctant to publicize their competitors' offerings. A typical marketing campaign may fanfare the benefits of replacing many individual bills for fixed line, mobile, Internet/broadband, and TV services with a combined tariff. At first glance this may appear to offer substantial savings. Enticing opening offers may disguise a package that costs more than the sum of the parts. The bundled service offers may only be available to new customers. They may expire after an introductory period, after which time tariffs may rise considerably. Many offers are tied to longer contract periods such that over time the cost may be much higher than comparative offerings. It is not unusual for offers to exclude additional charges for equipment, such as rental costs for TV set cable boxes, the purchase of dongles and wireless routers and so on. Certain promotions may only be available on-line and not in the showroom.

Regulators can ensure that ICT providers have transparent pricing structures that enable consumers to compare the deals on offer. Regulators can do this either through a statutory obligation or a "voluntary agreement" between the regulator and the ICT providers, supported by backstop powers if the industry fails to comply. Such initiatives may be regional or national, dependent on the structure of the ICT market.

For example, within the European Union (EU), an overarching regulatory framework includes measures to improve transparency of price information and the consumer contract. The Framework requires that consumers must have easy access to comparable price information, either free of charge or at a reasonable price. Consumers must also be told about any additional charges for their service e.g., whether access to a free phone number will attract a charge and what they might expect to pay if they terminate their contract early.²¹ The format of the information and the way in which it is provided is for individual NRAs to decide. Individual regulators therefore have the autonomy to adopt an approach they feel it best suited to consumers needs.

In the United Kingdom, Ofcom, the NRA oversees a price accreditation scheme for third party price comparator sites covering fixed line, mobile, broadband and digital television services. The aim of the scheme is to increase consumer confidence about how to find the best price for the service they

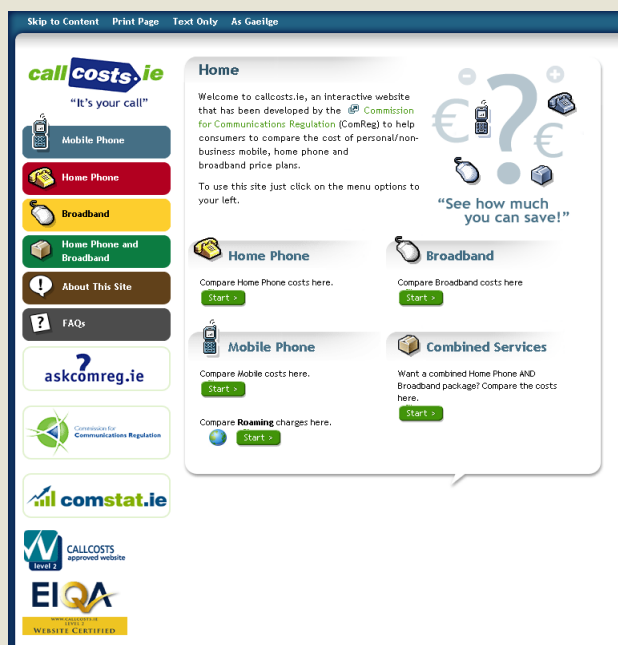
wish to purchase. The companies that have been approved have the right to display Ofcom's Price Accreditation Scheme logo on their websites and in any publicity campaigns.

To date, Ofcom has accredited three separate sites, which between them provide a wide array of "leading market deals" for home broadband, mobile broadband, digital TV, home phone, bundled packages. Each site explains the many caveats attached to the offers such as "available to existing subscribers only". The sites feature sophisticated search engines. These may be tailored according to consumer postcode, phone number, type of deal required and so on. One site provides detailed information about mobile price tariffs, including an online billing assessment.

Although there are many other commercial comparator sites in the UK that provide similar information, the added value of the accredited sites from a consumer perspective is the assurance that the calculations are accessible, accurate, up to date, transparent and comprehensive. Consumers know that the providers involved are willing to undergo both initial and annual audit spot check to verify the accuracy of the information provided.²²

Elsewhere within the European Union, a slightly different approach has been taken. The Irish Commission for Communications Regulation (ComReg) has developed its own interactive websites (Figure 1). Comreg's site also helps consumers compare the cost of personal, non-business mobile, home phone and broadband price plans. ComReg has designed the site to cater for typical features in the market. The tariff information provided is supplied by operators who have the option to test their tariffs against the market before publishing them live on the site. The Comreg site is accredited externally by an independent certification body.

Figure 1: Example of an interactive call cost comparator site from Ireland



Source: <http://www.callcosts.ie/home/default.asp>

Taking this sort of approach, regulators are able to fulfill a statutory duty to ensure consumers have access to accurate, comprehensive, and accessible information on prices without having to collect and validate the information themselves (which is a costly, resource intensive exercise). However such initiatives may struggle to keep up with market developments. Take the increasingly popular 3G mobile broadband services. Consumers may struggle to understand complex tariffs that vary according to whether the customer has a pay-as-you-go service or a monthly contract, amount of usage or flat rate, how much information is downloaded, how many voice calls are made, how many SMS text messages are sent and so on.

As part of its wider consumer education role, a regulator may wish to encourage consumers to consider a variety of information sources when making a purchasing decision. This might include specialist articles, web blogs, and interactive consumer feedback sites. In the United States, for example, a consumer web-based campaign, Broadband Census.com, promotes the provision of better information about broadband services, including details of where high speed service are available and where they are not, the extent of competition within a local area, names of carriers offering broadband speeds offered and prices charged. Information is gathered from consumers through an online census. Although such information sources may not have the backing of regulatory accreditation they may nevertheless help consumers gain a wider understanding of the issues they need to consider, over and above price, before contracting to a service.²³

4.2 QUALITY OF SERVICE INFORMATION

Consumers may be prepared to pay more for faster Internet speeds and the ability to access new content and applications but unless they are sufficiently well informed to be able to differentiate between the services offered, there is considerable potential for widespread dissatisfaction. The publication of technical quality of service perspective parameters, such as network latency, packet loss, bandwidth utilization, etc. may be useful for the monitoring purposes by the regulator but they are more likely to confuse than educate the typical consumer.²⁴

According to an OECD report, very few countries regulate or report on broadband quality of service indicators. Regulators in non-OECD countries which do so include the Malaysian Communications and Multimedia Commission (MCMC) and the Telecommunications Regulatory Authority of India (TRAI). The ITU Quality of Service (QoS) indicators and the EU Universal Service Directive QoS parameter requirements have hitherto been concerned with PSTN services.

Those regulators that endeavor to use their statutory powers to provide consumer friendly, comparable information may encounter resistance from some ICT providers, particularly those whose marketing drives rely heavily on price competition. There is little incentive to promote awareness of the availability of independent information that may put a competitor in a more favorable light. The information provided may not be relevant to the consumers it is aimed at, so there is little demand for it. Consequently it becomes difficult for the NRA to justify the cost incurred by industry for its provision. This may weaken the case for continuing regulatory intervention.

This is what happened recently to the UK scheme. Ofcom recently announced that it was withdrawing its Quality of Service Direction requiring fixed voice service providers to publish comparable performance indicators, with immediate effect²⁵. The scheme had initially launched following extensive public consultation, including with consumers. More recent research found that although consumers considered Quality of Service information an important factor for choosing between suppliers, the information they wanted was not the information being provided. They wanted reliable customer satisfaction surveys and a single source of information to help them compare price and quality.²⁶ The demise of the scheme illustrates the constant challenge facing regulators and ICT providers alike in trying to identify, keep abreast of, and satisfy consumers expectations.

This is not a simple task, especially insofar as the provision of Internet services is concerned. Take for example broadband and Internet connection speeds. ComReg, the Irish regulator and the Australian Communications and Media Authority (ACMA) are among some of the most proactive regulators in providing consumer friendly interactive broadband and Internet connection speed calculators.²⁷ Even so, the provision of a speed calculator in itself may not be sufficient to give consumers a true picture of what represents value for money in a broadband package. Technical limitations may also play a part.

Where the broadband service is delivered over traditional copper wires, the further away the subscriber is from the telephone exchange, the slower the service is likely to be. Although some websites publish distances from the exchange as a guide, the distances are calculated “as the crow flies” and not in terms of actual cable length serving the household. Other factors, such as increasing congestion of the network due to popularity of media intensive services such as You Tube, also affect speed. Unless this is pointed out to consumers, they are unlikely to consider it.

Box 3 provides an example of a privately managed site that is designed to help consumers compare mobile broadband deals. The site includes a broadband speed test but also explains that the test can only provide a snapshot of current download and upload speeds, alerting the consumer to the many factors that should be taken into account when comparing offers.

Box 3: Advice to mobile broadband users on how to compare mobile broadband deals (to be used in conjunction with mobile broadband speed calculator)

Each service provider offers a range of packages, so even if you know which provider you want to go with, it's worth going through the various options.

- **Hardware:** Do you just need a dongle for your current laptop, or do you want a shiny new laptop into the bargain? One of your biggest choices will be whether you want a dongle-only or dongle-plus-laptop deal.
- **Price:** Check the red tag for the monthly cost, but also look for text below the tag because many deals come with added bonuses or introductory deals.
- **Setup:** Most deals now have free set-up, but it's worth checking that your super cheap deal doesn't have a set-up cost that takes the shine off.
- **Contract:** As with mobile phones, you can either 'pay-as-you-go' or get a contract from anywhere from 1 to 24 months.
- **Speed:** This is the advertised speed each provider claims you will be able to download data from the Internet at, which is measured in megabits per second (Mb). For most users, it equates to how fast a web page takes to appear, or how fast a song will download.
- **Downloads:** This is the total amount you are allowed to download per month. It can be seen as the equivalent of how many minutes and texts you get with your mobile phone package, but measured in gigabytes (GBs).

While advertised speeds can vary quite dramatically, tests seem to suggest averages around the networks on mobile broadband aren't consistently different enough to warrant it being a serious factor in your choice. As for download limits, it's worth bearing in mind that 1GB could get you 250-1,000 songs, but just one grainy film or a few fuzzy TV episodes; if you want to download a lot of movie files, it's probably worth using your fixed-line home broadband instead, keeping your mobile broadband connection for lighter usage while on the move.

Source: [http://mobile.broadbandgenie.co.uk/3g-broadband?filters\[payg\]=1&filters\[rolling\]=1&filters\[fixed\]=1&order=downloadSpeed#packages](http://mobile.broadbandgenie.co.uk/3g-broadband?filters[payg]=1&filters[rolling]=1&filters[fixed]=1&order=downloadSpeed#packages)

4.3 GENERAL CONSUMER EDUCATION INITIATIVES

In addition to price and quality of service comparator sites, there a number of other interesting ways to educate consumers about ICT services.

In Kenya, the NRA (Communications Commission of Kenya (CCK) is responsible for ensuring that consumers have a good understanding of ICT products and systems. The Kenyan example is interesting because in addition to setting out consumers' rights, it also sets out consumers' responsibilities. Consumers are expected to make reasonable decisions and accept a certain level of responsibility when exercising choice or entering into transactions in the marketplace. Consumers are responsible for paying their bills on time and for reporting faults when they occur so that quality of service can be monitored – and complain when things go wrong. Consumer protection is closely aligned with consumer information. Responsibility for ensuring that consumers have a good understanding of ICT products and system rests with the regulator, the Communications Commission of Kenya (CCK). The CCK does this by publishing consumer factsheets and provides tariff comparators by collecting information from the

providers, monitoring and updating it. It also runs a full consumer education programme (which includes the promotion of safeguards and protection against computer security risks).

In Australia, ACMA undertakes a range of community awareness programs, including collaborating with other agencies to raise consumer awareness of products and services available. ACMA advises consumers not to be tempted by advertising, packaging design or point-of-sale displays, and to carefully consider their actual needs and affordability before making a purchase. It also provides product specific advice to help consumers choose between services on offer.

It is not only the regulator that provides advice on-line. A dedicated section of Australian Competition and Consumer Commission's website provides information about bundled telephone and Internet services, as well as pages providing information about charges based on downloads/uploads.²⁸ What is particularly valuable is the "checklist". Consumers are reminded to check that the bundled package on offer actually meets their needs. They are advised to take the time to compare different packages, to check recent bills to establish typical monthly costs and usage patterns, to ask for offers to be put in writing, to avoid being locked-in to long-term contract that does not suit them, to check for early exit charges and charges for additional services, to check whether local calls are more expensive, and whether there are fees for exceeding the download limit.

In the United States, the Californian Public Utilities Commission, which is not a regulator and has no jurisdiction over ICT providers, is very pro-active in providing information to help consumers get the best out of their telephone service. Its consumer education website, www.calphoneinfo.com, provides useful tips and tricks as well as helpful technical advice. The Commission's activities complement those of the regulator, in providing a framework for consumer protection and freedom of choice in a competitive telecommunication market.

One innovative way of keeping abreast of consumer information needs, providing direct interaction with consumers, is to use one of the latest popular forms of global on-line instant messaging tools, such as Twitter. Box 2 provides a screenshot of a service provided by Ofcom in the UK. The service is free to use. All consumers have to do is to fill in their details on the regulator's website. They can then keep in touch with other consumers and the regulator through the exchange of quick, frequent answers to one simple question. The regulator has the advantage of being able to mediate the exchanges and ensure that accurate information is provided.

Figure 2: NRA "Tweets" on FAQs re Broadband Quality of Service

The screenshot shows the Ofcom website's 'Broadband questions' page. The page header includes the Ofcom logo, a search bar, and navigation links for 'Telecoms', 'TV', 'Radio', and 'Spectrum'. The breadcrumb trail reads: 'Home > Media and Analysts > Homepage features > Broadband'. The date is 28/07/09.

Broadband questions
Over the past week we've been asking you to send in your broadband questions for our team to answer.
 Here is a selection of some of those we've received.

Due to space we haven't been able to use all the questions we've received - but thanks to everyone who took the time to email us or contact us through Twitter.

Q - I signed an 18 month contract with my provider in July 2008 and they said I would get a fast connection speed of up to 8 Mbit/s. Speed tests now reveal my service is usually below 0.5 Mbit/s. Can I get a discount or get out of my contract? - John O Doherty (via email)

If your provider has signed Ofcom's [code of practice on broadband speeds](#) then they may allow you to move without penalty to a lower-speed package if they have one, even though you signed your contract before the code came into effect in December 2008. You could contact your provider and see if they have a lower speed package or will allow you to move. It's also worth asking whether there is anything you can do to speed up your broadband service. Take a look at Ofcom's new video on speeding up your broadband and at our [consumer guide on broadband speeds](#).

Q - How can I improve the signal/speed of my mobile broadband when indoors? - Nathan J Massey, Manchester (via Twitter)

Mobile broadband speeds can vary according to where you are and what time of day it is. You may be able to get a better signal if you try different locations within your house. Your provider may be able to give you advice on how to improve your signal.

Q - Rather than up to XX, why are ISPs not forced to reveal their peak hour planning rules i.e. 20 Kbps per user? Much more useful! - Mike Kiely, London (via Twitter)

Information like this could be useful but might be difficult to understand since it won't tell you what speed you will actually get. Instead, Ofcom's [code of practice](#) requires ISPs to tell customers what their maximum expected speed should be.

Q - Why do countries like Japan and South Korea get much faster speeds than

Source: <http://www.ofcom.org.uk/media/features/broadqanda>

Whatever approach is taken, irrespective of whether the information is provided by the regulator or a third party, consumers need to have sufficient understanding to be able to evaluate the costs and benefits of alternative usage patterns. The information should be easily accessible and available either free of charge or at an affordable price.

4.4 PROVIDING CONSUMERS WITH REDRESS

Access to a fair and transparent complaints process is an essential part of an effective consumer protection framework. Consumer complaints have an important role to play in regulation as they provide a useful barometer on consumer detriment and unfair practice.

There is no definitive model of best practice in dispute resolution. The main options available are litigation, arbitration and mediation. Litigation is unlikely to be the preferred form of redress for individual consumer disputes (particularly where these involve relatively small amounts) due to its cost and the length of time it may take to bring a case to court. Arbitration is often preferred by regulators as a more suitable alternative. The procedure is more relaxed than a court, the process can be a lot quicker and the outcome is usually binding. However from a consumer perspective, there may still be

disadvantages. Arbitration is an adversarial procedure and the onus is on the consumer to present their evidence and put their case – something that not all consumers may be able or willing to do. Typically also, there are costs involved which the consumer may find prohibitive. Mediation, which offers a negotiated solution to disputes without the rules, procedures and costs, may be a useful alternative way of resolving consumer complaints with an operator. However as it tends to be non-binding, even if the consumer wins its case, a satisfactory outcome may still depend on the goodwill of the operator.

Most ICT regulatory frameworks include some requirement on operators to establish procedures for the handling of consumer complaints and to publish details of those procedures. The level of direct involvement of the regulator in dispute handling varies considerably. In Egypt, the regulator, NTRA, has a dedicated customer service line (with a short code number 155) on which consumers can contact them about the quality of service, reliability and service performance of their service provider although for non-technical complaints, the complainant must contact the service provider first.²⁹

In Saudi Arabia, the regulator, the Communication and Information Technology Commission (CITC), requires service providers to establish a separate division to handle consumer complaints and approves the procedures that are put in place. If the customer and provider are unable to resolve their dispute amicably, the customer may refer the dispute to CITC, in writing, for resolution. The CITC has a period of ten days to consider the complaint and to dismiss it if it decides it is vexatious or frivolous. If it decides the complaint merits investigation, a copy is sent to the service provider who has five days to respond after which the complainant has a further five days in which to reply. The CITC then has a period of 30 days to consider the complaint and reach its conclusions. During this time the provider is not allowed to disconnect the customer's service without the prior permission of the CITC. If the CITC concludes that the provider has breached the Telecommunications Act, it will refer the provider to the Violation Committee that can impose financial sanctions on the operator. The Committee decides the level of the penalty (subject to a maximum threshold) that it considers is proportionate to the gravity of the breach.

In India, the Telecom Regulatory Authority of India (TRAI), which originally had quasi-judicial powers to adjudicate and settle disputes, no longer does so. Following an amendment to the Telecommunication Act in 2000, a separate tribunal was established, the “Telecoms Disputes Settlement and Appeals Tribunal” (TDSAT).³⁰ TDSAT may adjudicate disputes between a licensor and licensee, between two or more service providers, between a service provider and a group of consumers, and hear and dispose of appeals against any decision or order of TRAI. TDSAT’s remit does not extend to the resolution of individual consumer complaints. These are handled by various consumer commissions, including the Consumer Disputes Redressal Forum or the Consumer Disputes Redressal Commission).

Box 4: TDSAT India: Complaints handling

TDSAT has powers to examine evidence and to establish facts and has the same powers as the civil courts in India including: (i) summoning and enforcing the attendance of witnesses which are examined under oath (ii) the right of access and supply of documentation requested (iii) receiving evidence by affidavit; (iv) issuing commissions for the examination of witnesses or documents and reviewing decisions; (v) dismissing an application for default or making a decision ex post and (vi) setting aside any order of dismissal of any application for default or any order passed by it ex parte

Every order issued by TDSAT is deemed to be a decree of the civil court, executable in the same manner as a decree of that court. Willful non-compliance with such orders is punishable by fines.

TDSAT's decisions are subject to appeal before the Supreme Court on the same grounds, usually applicable to appeal appellate decrees, i.e., on a substantial question of law.

Source: TDSAT

Within the EU, it is a statutory requirement under the Universal Services Directive (USD) for NRAs to ensure that transparent, simple, inexpensive and out-of-court procedures are available for dealing with consumer disputes, and to ensure that such disputes are settled fairly and promptly. The recent review of the USD included measures for strengthening out-of-court dispute resolution by ensuring that independent dispute resolution bodies were used, and that procedures conformed to a minimum set of principles, using either existing dispute resolution bodies or by creating new ones.

Where there are systemic problems, caused for example through over zealous marketing or more seriously where there is a rogue trader generating high volumes of complaints, individual, case-by-case dispute resolution may be a costly, time consuming exercise. At best it may only be successful in providing compensation to a few of the consumers affected.

The European Commission has been examining the problems that consumers face in obtaining effective redress and has published a Green Paper on Consumer Collective Redress.³¹ One problem identified is where consumers who have small or scattered claims refrain from bringing an individual court action because the cost of bringing the action is likely to outweigh the amount of damages claimed. The Commission wants to find ways to is seeking views on how best to facilitate redress where a large number of consumers have been harmed e.g., through overcharging through hidden charges, overbilling, misleading advertising, etc. .

Nevertheless whilst collective redress may benefit consumers in some circumstances, the need to maintain an effective means of individual redress is essential for consumer protection.

5 TRUST AND SECURITY ISSUES

As new technologies are developed and access to ICT expands, new threats to the security of networks are emerging. This matters to ICT regulators because unless consumers feel confident that the Internet is reliable, safe and secure they may become reluctant to use it. Consumers may feel they are unable to control security threats themselves, especially as they are increasingly global in nature. Moreover, the impact of security breaches impacts not only on individual consumers but also the wider national and global community. The individual or group of individuals generating an attack may often be physically located outside of national and regional boundaries and regulatory frameworks. Therefore, a global approach is needed to safeguard cyber-security.

Building on earlier work by the United Nations to promote global awareness and promote a global response to cyber-security issues³², the International Telecommunication Union (ITU) has done considerable work in this area. It has launched several projects and initiatives in relation to cyber-security, cybercrime and child online protection. In May 2007, the ITU launched its Global Cyber security Agenda (GCA). Designed as a mechanism and framework for international cooperation and response, the GCA focuses on fostering synergies and building partnerships and collaboration between all relevant parties in the fight against cyber-threats. The agenda has five main work areas: legal measures; technical and procedural measures; organizational structures, capacity building and international cooperation.

The main issues recognised as being security concerns for consumers when using the Internet are:

- Access to personal data
- Spam, scams and fraud
- Inappropriate/harmful content
- Children and the Internet

5.1 ACCESS TO PERSONAL DATA

Of growing global concern to regulators and consumers alike is maintaining the privacy of on-line information. Data protection breaches and reports of losses of personal sensitive data by banks, by health agencies, by government departments, banks and so on seem to make frequent headlines.

On the other hand, an individual's data is a valuable marketing tool that may potentially benefit consumers provided adequate protection exists to prevent misuse of the information. Initiatives such as "opt-in" clauses whereby a consumer's prior consent is required for the receipt of unsolicited marketing material have proven extremely difficult to interpret and enforce. There is similar confusion in relation to "cookies", the small electronic files that are stored on computers during Internet browsing. Cookies can be useful for tracking back and identify individual visitors to a website. Once a consumer has revealed their identity, for example by filling in a form on-line, their browsing behavior can be closely monitored. This helps companies to target their marketing strategies with personalized offers sent by email, which may or may not be welcome.

From a national security perspective, telephone and email data stored by communication network providers for billing purposes may also be used by national law enforcement agencies. This may be without a consumer's knowledge or consent. Network operators may be simply be required by law to retain the information for the purposes of criminal investigations and to support anti-terrorism measures. If aware of the measures, consumers may regard them as a valuable security protection tool or perhaps as an intrusion of their civil liberties.

5.2 SPAM, SCAMS AND FRAUD

Receiving unwanted emails has long been a source of annoyance. A common type of scam experienced by Internet users occurs through unsolicited bulk messages transmitted by email ("spam"). Phishing refers to Spam may also be sent with a fraudulent motive, for instance, to gather credit card or personal banking information ("phishing"). A similar scam, can attack the consumer's computer without the consumer even having to reply to an e-mail ("Pharming"). While the unaware consumer is using the Internet or browsing the web, hackers are downloading crimeware to their computer and is then able to gather their personal information.

According to a recent survey by Microsoft, more than 97% of all emails sent over the Internet are unwanted, many of which have malicious software, referred to as 'malware,' attached to them. The countries most badly affected were Russia and Brazil, followed by Turkey, Serbia and Montenegro. Types of malware vary from country to country. In China malicious web browser modifiers are common whereas in Brazil malware that targets consumers who bank online is more widespread. The report found an increase in the use of fake security software (referred to as 'scare ware') that advises consumers they need to install software protection, when in fact all the software does is to try and steal person details from a PC.³³

The threat from spam is changing in nature. It is now used as the primary means for delivering viruses that can hijack millions of computers (through so-called "zombie botnets"). It can be difficult for service providers to detect (and therefore counteract) spam messages, particularly when "zombie" computers are used to distribute them. Zombie computers are aggregated into large groups of computers known as 'botnets'³⁴ that may be used for the mass distribution of spam and spyware, the hosting of 'phishing' sites and the distributed denial of service (DDOS) attacks on websites. Internet connections become flooded with spam and ultimately are unable to connect to legitimate sites.

Given the wide-spread publicity given to Internet scams and fraud, regulators might reasonably expect that consumers would by now be taking reasonable steps to try to protect their on-line security. However it seems that this is not the case. A recent report on consumer attitudes and behavior relating to online security³⁵ found that even consumers who were taking preventative measures were mainly relying on informal knowledge and training. Recently there were reports that tens or even hundreds of thousands of log-in details from Hotmail, Yahoo!, Mail, Gmail and other web based e-mail services, assumed to have been obtained through several phishing exercises, had been posted on a code-sharing website. It seems that there is still a considerable way to go before consumers take on board the importance of keeping operating systems, web browsers and applications up to date with the latest

versions. This is not just important to individual consumers. Lack of proper security controls put other Internet users at risk.

5.3 INAPPROPRIATE/HARMFUL CONTENT

The misuse of online communications to spread racist material, hate speech, propaganda glorifying violence and pornography presents an enormous challenge that ICT regulators may not have the powers to tackle, especially at national level.³⁶ That said, it is very difficult to reach global consensus on the type of content that consumers need protection from. Whereas in some countries xenophobic material or insults related to religious symbols may be censored, in others the same content may be protected under freedom of speech legislation.

One issue on which there is international consensus exists is the need to combat child pornography. Even so, there are differences between national approaches. In Germany for example, the exchange of pornographic material is only a criminal offence where it relates to access by minors, whereas in Egypt, for example, the criminal offence applies to all. Enforcement of the law may prove difficult where the server is located outside the national boundary and prevention may only be feasible by limiting access through filter technologies.

5.4 CHILDREN AND THE INTERNET

The growth in access to the Internet, especially broadband, has encouraged the rapid development and adoption of social networks globally. South Africa has become the eight largest user of Facebook; and sites like You Tube, Blogger.com and Facebook already feature in the Top 10 sites in the African countries.³⁷ The enhanced interactivity of social networks encourages participation and creativity. Social networks are used to organize social agendas, to make shopping decisions, to get travel advice and to look for work.

The attraction to young users of online social networking sites and their desire (and ability) to download audio and visual content presents new challenges for consumer protection. Some youngsters post online photos of their friends or family, addresses and phone numbers and even sexual preferences on the sites, without realizing that someone with bad intentions or a future employer may access this data.

The main and most frequent risk to young users on-line, identified by young people themselves, is cyber bullying by peers. Cyber bullying may typically involve offensive or threatening SMS messages, or posting hurtful content on a social network message board for all to see.

Such issues raise the question of the role of the regulator and what if any action can be taken. The first step is to make consumers aware of the issue and actively encourage them to take precautions. Safeguards are more likely to be effective if there is cross-border co-operation, including by the social network providers themselves.

Social networking sites that are aimed at very young children are expected to use high levels of pre-screening of content for chatting and messaging, moderation and minimal collection of personal

information, and in some cases parental control. For teenagers, however, the initial “preferred” approach has been to promote “empowerment” through the provision of information about the risks of on-line networking and helping them to deal with those risks.

The ITU has launched a Child Online Protection (COP) initiative that aims to unite partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere³⁸. The key objectives of the initiative are to:

- Identity the key risks and vulnerabilities to children in cyberspace
- Create awareness of the risks and issues through multiple channels.
- Develop practical tools to help governments, organizations and educators minimize risk.
- Share knowledge and experience while facilitating international strategic partnerships to define and implement concrete initiatives.

The initiative includes sets of guidelines targeted at children, parents, guardians and educators, industry and policy makers³⁹.

More recently, the regulatory focus seems to be shifting towards more direct protection measures. In February 2009, the European Commission announced that it had brokered a deal with 17 leading Internet service providers to help protect under 18s using social networking sites.⁴⁰ The agreement establishes a number of safeguards to help young people while they are using the web:

- ensuring that the full online profiles and contact lists of website users who are registered as under 18s are set to "private" by default;
- guaranteeing that privacy options are prominent and accessible at all times, so that users can easily work out if just their friends or the whole world can see them online;
- providing an easy to use "report abuse" button.

From a consumer and regulatory perspective, it is encouraging that some individual websites have already started to address privacy and illegal activity issues. For example, following a US campaign to regulate social networks,⁴¹ MySpace has identified and removed over 90,000 sex offenders from its site over a two-year period.

6 CONCLUSIONS: IS THERE A REGULATORY GAP TO BE ADDRESSED?

Consumers have increasingly come to regard an Internet service as essential as a fixed voice telephony service. They expect the service provided to be efficient (preferably fast), reliable and affordable. They want a choice of services and a choice of providers,

These expectations in themselves are nothing new. Many regulators already have a consumer framework in place to meet those needs. What has changed is the way in which those communications services are delivered – with a single platform for voice and data services – and the way in which they are received – in an “always on” environment.

Responsibility for meeting the new challenges need not necessarily fall solely upon ICT regulators. The efficacy of regulatory intervention depends equally on consumers being aware of, and taking responsibility for, their choice of provider and their on-line security.

Wherever possible, consumer involvement and should be actively promoted. This could be part of a legislative framework that sets out consumers’ responsibilities, including letting the regulator know when things go wrong (as required by the Kenyan Consumer Protection Bill). It could be through support for consumer organizations when they lobby on a single issue (as in the example of the League for the Defense of the Consumer in Benin). It may be through the setting up and mediation of on-line instant messaging tools (like the Ofcom ‘Tweets’) that allow the regulator to be “always in touch” with its consumers.

Competition will only work well if consumers can exercise choice efficiently by being able to understand and distinguish between the services on offer. Regulators need to tackle information overload. This could be achieved relatively easily through the establishment of an accreditation scheme for price and quality of service sites (such as the Comreg interactive call cost comparator site). With trusted sites available, consumers do not need to visit multiple sites to make a decision. The regulator’s role should be to ensure that the right information is available, that it is accurate and that it is reliable. Regulators do not have to provide the information itself if they do not wish to do so. Indeed regulators may struggle to keep up with market developments if they attempt it.

Consumer complaints have an important role to play in regulation as they provide a useful barometer on consumer detriment and unfair practice. Access to a fair and transparent complaints process, with sanctions for non-compliance, remains an essential part of an effective consumer protection framework. With the Internet generating many small cross-border transactions, regulators also need to consider ways of securing collective redress (as is currently being explored by the European Commission).

Can regulators simply rely on consumer education, co and self-regulation and general consumer protection law to ensure the needs of connected consumers are met? This seems unlikely to be the case. The success of codes of practice relies in part on consumers taking an interest in them, which may prove difficult (as demonstrated by the Malaysian Communications and Multimedia Forum’s road show initiative). It partly relies on the willingness and power of the regulator to enforce the standards agreed

where necessary (as TRA Bahrain intends in relation to its Consumer Protection Guidelines). On the other hand, regulatory intervention needs to be justified in terms of cost in relation to the consumer detriment avoided.

With the expansion of networks and cross-border communications, possibly the most daunting challenge to ICT regulators is how to tackle cyber-security. The fight against scams, especially those propagated through zombie botnets, is not something that regulators or consumers can tackle on their own. It is a challenge that requires global co-operation between systems operators and software providers, law enforcement agencies, policy makers, industry and business organisations and consumers.

What is currently missing is a global inventory of consumer protection measures that provides comprehensive information about consumer levels of awareness and satisfaction with their consumer protection framework. Such an inventory could be used to undertake an objective evaluation of the most effective way for regulators to respond to the challenges of the always-on environment.

¹ A recent report commissioned by the OECD, which set out to examine the available evidence of consumer behavior and analyze the implications for policy and regulation. Exploring the evidence of actual consumer behaviour, the report makes a number of recommendations for policy makers and regulators designed to promote the consumer interest. See: Organisation for Economic Co-operation and Development, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy: Working Party on Communication and Infrastructures and Services Policy, Enhancing Competition in Telecommunications: Protecting and Empowering Consumers, London 24-25 May 2007, DSTI/ICCP/CISP(2007).

² OECD, *ibid*

³ A device specification which facilitates the discovery of a hardware component in a system without the need for a physical device configuration or user intervention.

⁴ For a more in-depth analysis, see Southwood, Russell, 'Consumer Protection in the Digital Age: assessing current and future activities' August 2006, Background paper prepared for ITU Global Seminar on Quality of Service and Consumer Protection.

⁵ http://www.acma.gov.au/WEB/STANDARD/pc=PC_90103

⁶ <http://www.atug.com.au/>

⁷ <http://www.ctn.org.au/content.cfm>

⁸ <http://www.treasury.gov.au/contentitem.asp?NavId=014&ContentID=1484>

⁹ <http://www.ncc.gov.ng/>

¹⁰ <http://www.ftc.gov/bcp/consumer.shtm>

¹¹ http://site.ldcb.org/index.php?option=com_content&task=blogcategory&id=1&Itemid=2

¹² www.ictconsumer.or.ug

¹³ The Economic and Monetary Community of Central Africa (or CEMAC, *Communauté Économique et Monétaire de l'Afrique Centrale*) is an organization of states of [Central Africa](#) established by [Cameroon](#), [Central African Republic](#), [Chad](#), [Congo](#),

Equatorial Guinea and Gabon to promote economic integration among countries that share a common currency, the CFA franc. CEMAC's objectives are the promotion of trade, the institution of a genuine common market, and greater solidarity among peoples and towards under-privileged countries and regions. Currently, CEMAC countries share a common financial, regulatory, and legal structure, and maintain a common external tariff on imports from non-CEMAC countries.

- ¹⁴ Communauté Economique et Monétaire de l'Afrique Centrale, Union Economique de l'Afrique Centrale, Conseil des Ministres, Directive no. /08-UEAC-133-CM-18, Fixant le Cadre juridique de la protection des droits des utilisateurs de réseaux et de services de communications électroniques au sein de la CEMAC.
- ¹⁵ <http://www.networkworld.com/news/2008/11508-african-telecom-consumer-advocacy-groups.html>
- ¹⁶ The Framework comprises (1) the Unfair Commercial Practices Directive(UCP): which outlines "sharp practices" that are prohibited throughout the EU, such as misleading and aggressive marketing. It places general ban on unfair commercial practices, which is designed to ensure that the Directive will stand the test of time even in fast evolving markets. Specific provisions prevent exploitation of vulnerable consumers, such as children. However enforcement of the rules is the responsibility of national consumer protection authorities and the courts. (2) A legal framework to ensure effective co-operation across national borders and agencies: the Regulation on Consumer Protection Cooperation (CPC). The CPC lays down the legal basis for administrative co-operation between Member States aims to ensure that existing legal, institutional and administrative measures are implemented effectively and to ensure that there is effective cooperation on the ground. National authorities may request another Member State authority to act on an infringement, although as yet there is not provision for consumer compensation. (3) The European Consumer Centre (ECC) Network The ECC aims to promote consumer confidence by advising citizens on their rights as consumers and providing easy access to redress in cross-border cases. The network provides training in management, lobbying and consumer law for national consumer organizations and also monitors national policies in relation to consumers.
- ¹⁷ Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee, EU Consumer Policy Strategy 2007-2013, Empowering consumers, enhancing their welfare, effectively protecting them, Brussels 13.3.2007, COM (2007) 99 final
- ¹⁸ Independent Consumer and Competition Commission, Papua New Guinea, Internet Service Providers Code of Practice, Final Report, December 2005
- ¹⁹ see Kiranjit Kaur, Consumer Protection in e-commerce in Malaysia: An Overview in UNEAC Asia Papers, No. 10, 2005
- ²⁰ Mobile Premium Services or 19 SMS Services are information and entertainment services that deliver various forms of content to your mobile phone. These services are created by a content supplier and delivered over your mobile service provider's network. They are called 'Mobile Premium Services' because you buy them using your mobile phone, you receive them on your mobile phone, and you will be charged a premium cost for them. Communications Alliance <http://www.19sms.com.au/>
- ²¹ The current regime comprises the over-arching Framework Directive,²¹ an Authorisation Directive, an Access Directive, and the Universal Services Directive (USD); plus a separate Directive, the Privacy and Electronic Communications Directive, which regulates the processing of personal data and free movement of data across Member States. The USD establishes a common set of end users' rights and obligations on the service providers, including a defined minimum set of services of a specified quality, to which all end users must have access at an affordable price. The framework of measures are commonly linked to broader policy objectives of inclusiveness, innovation, job creation, growth, etc.
- ²² The three price comparators that have been accredited by Ofcom to date are: <http://www.simplifydigital.co.uk/>; <http://www.broadbandchoices.co.uk/>; and <http://www.billmonitor.com/>
- ²³ See for example, Bon a Savoir, No. 6, June 2009 <http://www.bonasavoir.ch/> for a comparisons of 3G mobile broadband tariffs of Swiss operators

-
- ²⁴ For further details, see OECD Working Party on Communications Infrastructure and Services Policy Report, «Enhancing competition in telecommunications: protecting and empowering consumers» DSTI/ICCP/CISP(2007)
- ²⁵ <http://www.ofcom.org.uk/consult/condocs/topcomm/statement/topcommstatement.pdf>
- ²⁶ Provision of quality of service information, Ofcom research document, 30 January 2009.
- ²⁷ [http:// www.broadband Internet.net.au/broadband Internet/downloadspeed/](http://www.broadband Internet.net.au/broadband Internet/downloadspeed/)
- ²⁸ <http://www.accc.gov.au/content/index.phtml/itemId/815439>
- ²⁹ <http://www.tra.gov.eg/english/main.asp>
- ³⁰ <http://tdsat.nic.in/>
- ³¹ http://ec.europa.eu/consumers/redress_cons/collective_redress_en.htm
- ³² Note in particular UN Resolutions (57/239 and 58/199) related to a culture of security.
- ³³ Report published by Microsoft, April 2009
- ³⁴ Botnets is the term used to describe of compromised computers that run programmes that are under external control. The software package is used to control a network of computers remotely without the end user knowing, e.g. after visiting chatrooms online. Each computer will only send a few hundred emails each which makes it difficult for email providers to detect the spam. Hackers can also use the technology to pre-infect PCs around the world ready for the next buyer.
- ³⁵ *Australia in the Digital Economy: Trust and confidence* http://www.acma.gov.au/WEB/STANDARD/pc=PC_311655
- ³⁶ A study by the OSCE suggests a 25% rise in such sites, see Akedniz, «Governance of Hate Speech on the Internet in Europe» in «Governing the Internet Freedom and Regulation in the OSCE Region», http://www.osce.org/publications/frm/2007/0725667_918_en.pdf
- ³⁷ See article in Balancing Act n° 454, Getting ready for the Big Change – Putting the local into African services and applications.
- ³⁸ <http://www.itu.int/osg/csd/cybersecurity/gca/cop>
- ³⁹ <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>
- ⁴⁰ The agreement – which covers networks including Facebook, MySpace and YouTube Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.It, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo!Europe, and Zap.lu.
- ⁴¹ <http://www.guardian.co.uk/technology/2009/feb/04/myspace-social-networking-sex-offenders>