Republic of Lebanon
Telecommunications
Regulatory Authority

April 25, 2014

Subject: Consumer Protection in a Digital World Consultation Contribution – TRA, Lebanon

In reference to the invitation letter Ref.: BDT/IEE/RME/DM/413 dated 17 March 2014, the TRA Lebanon has the pleasure to submit its contribution related to identifying pro-active policy and regulatory measures in the areas of:

- *Redefining consumer protection needs along the value chain, from ICT networks to apps and services;*
- *Identifying priorities and responsibilities of ICT stakeholders (government, industry and consumers) in a digital environment;*
- *Expanding the regulator's mandate and enforcement measures to ensure effective consumer protection in a converged digital environment (in particular in dealing with privacy, data protection, protection against fraud, misuse, etc.)*

Background:

The Telecommunications Regulatory Authority has taken an active role in relation to consumer protection in Lebanon and has ensured the protection of consumers' rights with respect to telecom service providers by resolving telecom complaints, by intervening onsite where appropriate, by encouraging competition and by setting the appropriate regulations to develop the Lebanese telecommunications market in the interest of the consumer. The TRA has issued several documents related to consumer protection including a Consumer Affairs Regulation, a Code of Practice for Value Added Services, a Human Electromagnetic Exposure Limit Regulation and a Quality of Service (QoS) Regulation. The Authority is keen on making sure Lebanese consumers are informed about their rights and it has made awareness a key element to its strategic yearly goals, especially in relation to Child Online Protection.

The TRA is interested to contribute in identifying pro-active policy and regulatory measures in relation to the on-going consultation that focuses on consumer protection in a digital world in the following areas:

Redefining consumer protection needs along the value chain, from ICT networks to apps and services

The TRA is of firm belief that the regulatory framework should turn focus on protecting consumers in relation to applications and services. The rise of ICT and the spread of Internet Protocol (IP)-based Next-Generation Networks (NGNs), convergence in applications, devices and networks, the rise of social networks and the changing needs of consumers mean that ICTs are now fully integrated into every day's lives.

As such, the TRA has developed within its regulatory framework, codes of practices which give guidance to value added service providers and telecom service providers, who are the key links between consumers and ICT apps and services, ensuring that content, promotion and operation of all their VAS (whether provided by themselves or by their content providers) comply with all necessary conditions.

For example the TRA's Code of Practice for Value Added Services (VAS) requires Service Providers to ensure that service content does not contain anything in breach of existing laws and does not promote services that are violent, abusive, child-pornographic, demeaning, discriminating, misleading and/or religiously offending.

Identifying priorities and responsibilities of ICT stakeholders (government, industry and consumers) in a digital environment

Children are vulnerable and the cyberspace which they surf daily should be safe. When accessing the internet, children could be target of pedophiles, cyber bandits, hackers and online predators. The TRA believes that priorities of governments and ICT stakeholders should focus on Children Online Protection (COP) which should take an active role within telecom consumer protection strategies. Internet safety has been a main concern for parents, teachers, NGO's, civil societies, Ministries and other stakeholders in Lebanon for many years. Various roundtables, projects and activities were completed revolving around finding solutions that best suit the Lebanese communities. One of the main prerogatives of the Telecommunications Regulatory Authority relates to increasing awareness of the risks that our children face while surfing online. 3 strategies were developed and are recommended as such:

1- *Developing a National Safety Website to direct consumers to:*

The TRA has created a national safety website (e-aman.com) that targets the Lebanese community as a whole including parents, youths and teachers. The site aims at helping Lebanese citizens become more responsible in the cyberspace. Adults must be aware of the many options they have to secure their Internet at home. They also need to understand the potential risk areas and be able to educate their children to act responsibly online. Although parents are the weakest channel to drive awareness for their kids, they still play an important role to support them in case of danger. Parents can also extend the internet to various devices and users at home. Thus the TRA built a dedicated national website that would offer comprehensive tips and exhaustive information for individuals, parents, youngsters and teachers to help them avoid facing Internet risks.

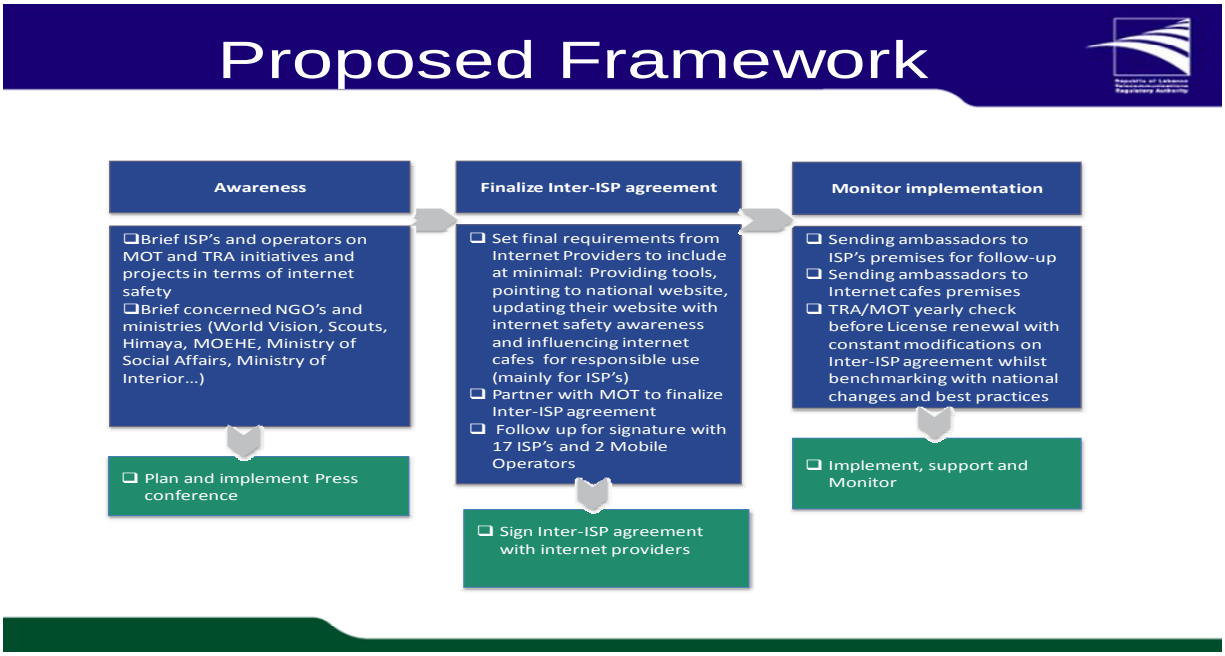
2- *Developing a Code of Practice for COP and for Internet Cafes*

A- The TRA took measures towards influencing Internet Cafes to take actions of ensuring a safe cyberspace for children and to:

- Abide by enforced laws and Secure areas designated for the use of children and minors
  - Age verification
  - Identity checking
  - Content filtering and text analysis
  - Checking contents to be used by children
- Maintain stored data and traffic data information and log use in a safe place for a "specific" period of time.
- Take all necessary measures to protect against unauthorized access such as manipulation/loss of personnel data.
- Protect the privacy of personal information collected from monitoring the use of children.

Another considered approach includes studying the possibility of Lebanese standardization of Internet Cafes through municipalities as Internet Cafes today only require a restaurant commercial license.

B- The TRA has also worked actively on developing a Code of Practice (COP) for ISP's with the following proposed framework:

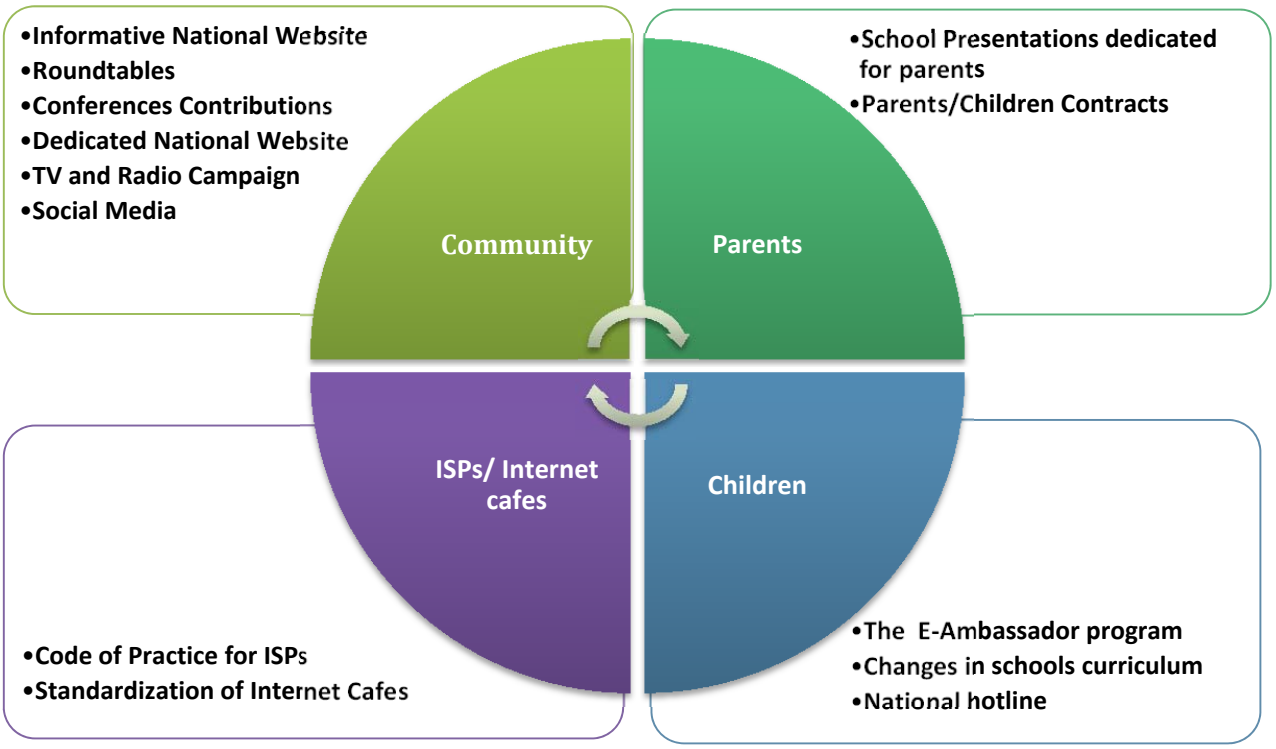


3- Training the youth as ambassadors

This contribution contains a proposal for a new regional initiative to empower young people to promote safe internet awareness among peers and the community. A training model for the E-ambassadors is developed, as well as the key outcomes of 3 activities necessary to develop a training model and apply it to the region to create awareness for the benefit of the community. This strategy includes:

1- determining children's baseline knowledge of online risks and developing a training curriculum while setting the criteria for E-Ambassadors.
2- Piloting the Train the Trainer's program and agreeing on a training model to be replicated in all schools.
3- Replicating the model throughout the public and private schools while reporting progress and evaluating awareness level improvement.

Here is the TRA overall COP vision:



Expanding the regulator's mandate and enforcement measures to ensure effective consumer protection in a converged digital environment (in particular in dealing with privacy, data protection, protection against fraud, misuse, etc.)

The TRA has developed a Consumer Affairs Regulation (CAR) which provides adequate information and guidance to consumers of telecom services so they make informed choices while choosing the services they wish to subscribe to. The CAR also develops processes to ensure that all Service Providers treat consumers fairly and provide the necessary information in a transparent manner. In order to ensure consumer protection in a converged digital environment, the CAR includes requirements to ensure the confidentiality of consumers information while giving the rights to call barring services.

In relation to cybersecurity, although current Lebanese efforts fall short of what is required to address the high levels of cyber risks and threats, a national vision was developed with the following required actions and responsibilities:

Private and public administrations should join forces in order to:

- Develop a national cybersecurity strategy.
- Coordinate public and private sector's collaboration.
- Create national incident management capabilities with the establishment of a National Computer .Incident Response Center to act against threats.
- Establish the Cybersecurity Emergency response Team (CERT) with the help of the Lebanese University.
- Promote a national culture of Cybersecurity.
- Secure government cyberspace.
- Improve regional and international coordination and cooperation.

Industry and businesses should:

- Give a higher priority to legal and security measures within their operation.
- Ensure necessary dedicated resources to plan and implement multiple layers of security technologies to deter threats to their data, information systems and infrastructures
- Implement and enforce security processes and procedures and consider it as a mandatory task with a high priority.

Universities

Universities have a major role in providing the required academic support to promote cybersecurity science, through:

- Advanced academic research about the different technical aspects of network and information security.
- The creation of new security protocols and algorithms.
- The integration of cybersecurity threats and counter measures, as well as legal aspects of combatting cybercrimes in university courses.