Memorandum on the protection of personal data and privacy in Internet social networks, specifically in regard to children and adolescents

Memorandum of Montevideo

GENERAL CONSIDERATIONS

By providing tools such as the Internet and online social networks, the Information and Knowledge Society offers an invaluable opportunity to access and exchange information, as well as to spread ideas and to allow citizen participation, entertainment and social integration, particularly through social networks.

The growing access to a variety of communication systems by children and adolescents - with all the benefits that such access provides - has also lead to an extreme in what should be a balance between the exercise of basic rights on the one hand and safety on the other in matters of personal affairs, reputation, and privacy, among others. In these matters, through whose abuse children and adolescents can be victimized —such as discrimination, sexual exploitation, pornography and so on— could result in a negative effect on their overall development and on their adult lives.

Efforts are being made in Latin America and the Caribbean, as well as in other regions – and within the existing regulations and the social, cultural and political diversity – to attain a certain level of consensus and rationality and to establish a balance between the guarantee of rights and the protection from risks involved in the Information and Knowledge Society. On this topic, recently published documents are: *Settlement of the judicial conflict between the Federal Public Ministry of Brazil and Google*[1] (dated July 1st, 2008); the *Child Online Protection Initiative*[2] of the International Telecommunication Union (dated 18 May, 2009); *Opinion 5/2009 on online social networking,*[3] by the Article 29 of the European Working Group (dated June 12th, 2009); the Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.[4] (dated July 16th, 2009).[5]

The following recommendations are a contribution to the commitment by the various involved parties to address the subject and advance the positive aspects of the Information and

---

[1] *Available at http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/noticia-7584/*
[2] *Available at http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html*
[3] *Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf*
[4] *Available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm*
[5] Other particularly significant documents are: *Strasbourg's Resolution on Privacy Protection in Social Network Services* (October 17th, 2008); *Recommendations regarding social networks* by the Spanish Data Protection Agency, *Study on privacy of personal data, privacy and information safety in online social networks* by INTECO (Spanish acronym for National Institute of Communication Technology and the Spanish Data Protection Agency (2009), *The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents* (November 2008), Advisory Opinion 2/2009 regarding protection of children's personal data by the Article 29 of the European Working Group (2009); the Report on Analysis and Proposals relative to Access to Information and Privacy in Latin America by the Privacy and Access to Information Monitor, and eLAC documents 2007 and 2010.

Knowledge Society, including the Internet and online social networks, as well as to prevent harmful practices that would prove extremely difficult to change, along with the negative effects they entail.

Any approach to the issue necessarily requires two dimensions: on one side, the acknowledgment that children and adolescents are fully entitled to their rights, and may therefore exercise them based on their age and maturity —and their opinions must also be considered based on their age and maturity— and on the other side the fact that, given their specific stage of development, they are entitled to special protection in situations that might prove harmful to their development and rights.

The right to privacy deserves the respect of every democratic society. Furthermore, to ensure the autonomy of individuals and to protect the scope of their privacy rights, the power of both the State and of private organizations must be limited in order to prevent illegal or arbitrary interference in their private lives. Specifically, protection is to be given to personal data of children and adolescents, without affecting their dignity as individuals, for they have a reasonable expectation of privacy when they share their information in digital environments and consider themselves to be in a private space.

In this respect, we must keep in mind the importance of consulting with children and adolescents, and for their opinions to be taken into account in whatever measures are implemented in these areas. Civil society expects that all parties in the economy adhere to the principles, attitudes and procedures oriented to securing the rights of children and adolescents in the Information and Knowledge Society.

With regard to the eradication of child pornography on the Internet, cooperation is expected from all responsible parties —governments, police, access and content providers, civil society, and the private sector— at the national, regional and international levels, so as to mobilize and involve a growing number of companies, public institutions and civil society organizations.

Prior to issuing these recommendations, the specific gender and cultural diversity features of Latin America and the Caribbean have been taken into account, as well as the variety of policies and regulations concerning approaches to the Information and Knowledge Society phenomena, focusing particularly on the Internet and online social networks.

Multi-lateral entities must include children and adolescents in their documents, guidelines and recommendations as specifically protected individuals who are vulnerable to the treatment given to their personal data.

The recommendations contained in this document refer to the United Nations *Convention* on the *Rights* of the *Child* (henceforth referred to as CRC) as their main basis. The CRC has been ratified by all countries in the region and that clearly acknowledges the shared responsibility of the State and society, in their respective environments, in regard to the protection of children and adolescents. This is based on three basic aspects, which are: acknowledging the significant role played by families —or by whoever is responsible for the process of bringing up children and adolescents— in instructing them and protecting and ensuring their rights; the need for all measures adopted to prioritize the best interests of children and adolescents, while maintaining the balance between the need for protection against the violation of their rights and the responsible use of those tools representing ways of exercising their rights; and

the fact that all those benefiting in any way from the Internet and online social networks are responsible for the services they provide and must therefore take responsibility for the solutions defined for the problems generated by these services.

RECOMMENDATIONS FOR STATES AND EDUCATION INSTITUTIONS FOR PREVENTION AND FOR EDUCATING CHILDREN AND ADOLESCENTS

All actions intended to protect the personal information and privacy of children and adolescents,[6] must take into account the best interests principle,[7] as well as Article 16 of the CRC, which reads as follows: "(1). *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honor and reputation.* (2). *The child has the right to the protection of the law against such interference or attacks".*

Prevention is a priority —regardless of the policy, regulation or legal approach— in addressing through education the aspects identified as risks of the Information and Knowledge Society, specifically the Internet and digital social networks. This effort must include the active participation of children and adolescents themselves, as well as their elders and other individuals in charge of their care and teachers, and consideration of the best interests of children and adolescents as the basic principle.

For this purpose, the following recommendations are to be considered:

1. State and educational institutions must consider the role played by parents, or those responsible for the care of children and adolescents, in the education of the latter, including on the responsible and safe use of the Internet and online social networks. It is the duty of the State and educational institutions to provide information and to strengthen the capability of parents and responsible adults about the potential risk to which children and adolescents are exposed in digital environments.

2. All measures involving the control of communications must respect the proportionality principle, and it must be determined that they are intended to protect and guarantee rights in a manner appropriate to this objective, and that no other measures exist for attaining the same results that would be less restrictive of such rights.

3. Children and adolescents must be clearly informed that the Internet is in no way a space free of rules, punishment or responsibility. They should be warned against believing that everything is allowed on the Internet, because each and every action will necessarily have consequences.

---

[6] The expression "children and adolescents" is to be used with the meaning set forth by the respective legislation in each country. Depending on the country, the term "children" may refer to individuals under the age of 12 or 13, and the term "adolescents" to individuals over that age and under 18 years old. In countries where the "adolescent" category has not been introduced in the applicable laws, the concept applies to the so-called "adult minors" or "pubescent minors". In Honduras, for example, a boy is defined as an individual younger than 14, and a girl is an individual younger than 12 years of age, while adolescents are those over such ages but younger than 18.

[7] Article 3.1 of CRC reads as follow: *"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration".*

They should be instructed in the responsible and safe use of the Internet and online social networks, specifically in regard to:

3.1. Anonymous participation and the use of pseudonyms are both possible in online social networks. The process of education must reflect on the positive aspects of using pseudonyms as a means of protection, and the responsible use thereof, which includes not using them to deceive or confuse others regarding an actual identity, among other concerns.

Children and adolescents must be alerted to the possibility of their being in communication or sharing information with someone in fact different from the individual they think they are in communication with. They must also be cautioned about the possibility of phishing allowed by anonymous participation and the use of pseudonyms.

3.2. In the process of education it is necessary to emphasize, among other things, the respect for the personal affairs, privacy and reputation of others. It is important for children and adolescents to be aware that any data they reveal may end up endangering their rights and the rights of third parties.

3.3. Children and adolescents must be informed that distributing content banned by local and regional laws (particularly child pornography), harassment (particularly sexual harassment), discrimination, the promotion of racial hate, defamation, and violence, among others are not legal on the Internet or in online social networks and are liable to legal punishment.

3.4. The learning process must provide knowledge regarding the responsible and safe use by children and adolescents of privacy and safety policies and alerts included in access instruments and websites frequently used by children and adolescents, such as online social networks.

3.5. Education policies —expressed in language consistent with the age of children and adolescents— must include an informational and developmental strategy to aid children and adolescents in managing the potential risks derived from the Information and Knowledge Society, specifically with regard to the use of the Internet and online social networks.

3.6. Information must be provided about protection mechanisms and the civil, criminal and administrative liability for the violation of one's own rights or the rights of others on the net.

3.7. Warnings must be made about the dangers of identity theft and impersonation that exist in online environments and that can lead to deceit.

3.8. It is necessary to explain to children and adolescents in an easily understood manner the spirit of legislation concerning the protection of personal data and privacy so that they may grasp the importance of respect for the privacy of the personal information of each individual, themselves included.

3.9. Education is necessary in regard to the uncertainty of the veracity of content and the validation of data sources. Children and adolescents must be trained and taught how to search for and be discerning about sources.

4. It is particularly recommended that a comprehensive and continuing education about the Information and Knowledge Society be developed, especially on the responsible and safe use of the Internet and online social networks and in particular by means of:

4.1. Including, in all syllabuses at all educational levels, basic information on the significance of privacy and the protection of personal data and other aspects as mentioned in item three.

4.2. Producing educational material, specifically, audio-visual material, web pages and interactive tools (such as online games) showing both the potential and risk involved. Such material must include information related to the mechanisms for the protection of rights.

The nature of these topics and materials calls for the participation of and discussion by all parties involved in order to take into consideration local and cultural peculiarities.[8]

4.3. Teachers must be trained in how to enable the discussion and place the advantages and risks of social networks of the Information and Knowledge Society in due context, with the possible support of authorities responsible for the protection of personal data and any and all entities that work on that subject in different countries.

4.4. The education authorities —supported by authorities responsible for the protection of data (if any), the academic sector, civil society organizations, private sector entities, and (when necessary) with the aid of international cooperation— must assist educators and support all work in the areas mentioned.

5. The appropriate authorities should establish guidelines by which schools and other educational programs can resolve incidents that arise in the usage of the Internet and online social networks by children and adolescents, using these incidents as an opportunity to educate but always bearing in mind the best interests of the children involved and without violating their rights or entitlements, in particular their right to education.

RECOMMENDATIONS FOR STATES REGARDING LEGAL FRAMEWORKS

The regional legal frameworks that regulate the Information and Knowledge Society —in particular the Internet and online social networks— have developed more slowly than the development of new applications and content, and have a series of gaps and significant tensions between the values that motivate them as well as inconsistencies in how they approach the protection of rights. Nevertheless, there is a degree of consensus acknowledging that there are sufficient fundamental and constitutional principles to support any decisions made in these matters.

The creation, amendment or coordination of regulations must consider, in the first place, the best interests of children and adolescents and should specifically take into account the following:

---

[8] **ITU Guidelines for Policy Makers** checklist #3 y #4: " … *It is very important, therefore, that materials are produced locally which reflect local laws as well as local cultural norms. This will be essential for any Internet safety campaign or any training materials that are developed*"; " … *When producing educational materials it is important to bear in mind that many people who are new to the technology will not feel comfortable using it. For that reason it is important to ensure that safety materials are made available in either written form or produced using other media with which newcomers will feel more familiar, for example, with video*".

6. Protecting personal data involves the development of national regulations, applicable to the public and private sectors; such regulations ought to be in compliance with internationally acknowledged basic rights and principles as well as the mechanisms necessary for their effective enforcement. In creating and developing these regulations, States must especially consider children and adolescents.

7. Any action or inaction regarding a child or adolescent that is considered illegal in the real world must also be considered illegal in the virtual world, to always guarantee their well-being and the overall protection of their rights[9].

8. States must legislate the right of children and adolescents –either directly or through their legal representatives– to request access to any information on them included in public and private databases, and to the rectification and removal of such information when necessary, in addition to their entitlement to express their opposition to the use of such information for any purpose whatsoever.

9. Proper regulations must be developed for the operation of locations (both public and private) that provide access to the Internet and this might include, for example, the obligation to use alert messages or content filters, support accessibility for children and adolescents, and so on.

RECOMMENDATIONS FOR STATES IN THE ENFORCEMENT OF LEGISLATION

In recent years, many conflicts and violations of rights resulting from the publication of personal data, the interference in private affairs and defamation on the Internet and online social networks have ended in court. Certain rulings have shown the role of judges in applying fundamental principles to new situations. However, the proportion of conflicts that reach the judicial system is minimal.

Judicial systems play a significant role in ensuring the proper use of the Internet and online social networks. Civil and criminal penalties must be applied not only to redress the violation of rights but also to clearly indicate to the public and to companies how laws and fundamental principles will be interpreted.

10. The following is to be guaranteed:

10.1. The existence of simple, speedy and easily accessible judicial and administrative processes, to be treated as a priority by the courts and the relevant authorities.[10]

The use of strict liability is to be strengthened as a form of regulatory mechanism for guaranteeing fundamental rights in the applications of the Information and Knowledge Society, Internet and online social networks. Judicial penalties that can be applied to the

---

[9] ***ITU Guidelines for Policy Makers*** *#2: "Establish, mutatis mutandis, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for legal minors are also adequate".*

[10] *In this sense, the participation of the Special Courts of Brazil in the protection of citizens' rights in Internet's social networks is to be mentioned.*

derived damages have the advantage of being a quick, efficient response capable of dissuading dangerous designs. This type of civil liability is founded on the child's best interests.

10.2. The settlements arrived at by these means, should be made public and widespread as possible with the use of anonymity techniques to guarantee the protection of personal data.

10.3. Development and publication of a database of cases and legal decisions (anonymized administrative resolutions or court orders) related to the Information and Knowledge Society, and in particular to the Internet and online social networks. This could yield a tool for judges to analyze the national and international context in which they are operating and making decisions.

11. The establishment of a communications channel for allowing children and adolescents to report violations of their rights with regard to the protection of personal data.

12. Promotion of the establishment of jurisdictional entities that specialize in data protection

13. Development of the capabilities of legal parties involved in data protection, focusing on the protection of children and adolescents.

RECOMMENDATIONS REGARDING PUBLIC POLICIES

The need for the best interests of children to be the guiding principle for all measures adopted on this issue is to be borne in mind, specifically in the development of public policies intended to regulate online social networks.[11]

14. The implementation of the following public policies is recommended:

14.1 Definition of response mechanisms for assisting the victims of abuse in the Information and Knowledge Society, particularly on the Internet or in online social networks. Likewise, information systems are to be created for providing assistance and quick support to children and adolescents concerned in any way about content on the Internet or in online social networks. For this purpose, it is possible to create mechanisms to aid online reporting, through toll free numbers, service centers, and so on.

14.2. Definition of protocols to channel the illegal content that is reported.[12]

---

[11] ***Opinion 5:*** *4. "The Opinion emphasized the need for taking into account the best interest of the child as also set out in the UN Convention on the Rights of the Child. The Working Party wishes to stress the importance of this principle also in the context of SNS".*

[12] **ITU Guidelines for Policy Makers** #5, 6 y 7: *"5. Consider taking additional measures to disrupt or reduce the traffic in CAM, for example by establishing a national hotline and by deploying measures which will block access to web sites and Usenet Newsgroups known to contain or advertise the availability of CAM. 6. Ensure that a mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the Internet, for example, a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible. 7. Ensure that national processes are in place which ensure that all CAM found in a country is channeled towards a centralized, national resource. One example is the National Child Abuse Material Management Centre".*

15. Creation of regional and international mechanisms for sharing information reported by private parties regarding these occurrences, in real time, in order to promptly generate protective policies and mechanisms. This is due to the type of problems involved in online social networks, which are often dispersed and not fully detected.

16. Promotion of efforts to raise public awareness and to spread information through the press, the mass media, as well as through the social networks themselves, among others, all of which are effective means for promoting the responsible and safe use of tools of the Information and Knowledge Society.[13]

17. Promote the commitment and participation of public and private associations, as well as national networks of centers for accessing the Internet (if any), to ensure their participation in protection and in alert campaigns on the possibilities and risks involved in the Internet and online social networks.

18. To promote specialized research in order to develop appropriate public policy. With regard to the online behavior of children and adolescents, it is particularly recommended that research be conducted into the roles they play in the acquisition, production, storage and reproduction of illegal content, the protection measures they develop, the individual and collective motivations for such behaviors, as well as the actual dangers they face in the Information and Knowledge Society.

RECOMMENDATIONS FOR THE INDUSTRY

Companies in the business of providing access to the Internet and development of applications or online social networks must purposefully undertake the protection of private data and privacy – especially of children and adolescents – and cooperate with national judicial systems. This is in addition to implementing campaigns for prevention and development of capabilities, among other possible instruments, through formal commitments or codes of conduct that should include:

19. A ban on the collection, processing, publication or sharing with third parties of personal data without the express prior consent of the individual whose data is involved. The use of information obtained is to be restricted only for the purpose for which it was originally obtained, particularly with regard to the creation of behavioral profiles.[14]In the case of children, a ban on the handling of personal data is to be especially considered. Regarding adolescents, parent control mechanisms consistent with each country's legislation —about which clear information is to be made available— should be taken into account.

20. The protection of privacy as a primary feature in all online social networks, databases and communication systems, among others. Making changes in the degree of privacy of user profiles must be simple and free of charge.

21. Explicit, simple and clear rules on the privacy of web pages, services, and applications, among others, explained in a language appropriate for children and adolescents.

---

[13] ***ITU Guidelines for Policy Makers, checklist*** *#2: "Consideration should also be given to enlisting the aid of the mass media in promoting awareness messages and campaigns".*

[14] ***Opinion 5:*** *3.4. Sensitive personal data may only be published on the Internet with the explicit consent from the data subject or if the data subject has made the data manifestly public himself.*

Information is to be provided regarding the objectives and purposes for which personal data is to be used, as well as any communication thereof to third parties. Likewise, the name(s) of the individual(s) responsible for handling such information is (are) to be provided.

Also, a link to any "privacy options" is to be provided at the time of registration, with a clear explanation of the purpose of these options.

A notice should also be provided that the social network has pre-selected options, if applicable, and that they can be changed at any time according to the preferences of the children and adolescents.

It would also be desirable for the "default options" to be set such that personal content is accessible only to friends and any networks defined by the user.[15]

22. All online social networks must expressly include (in the section concerning "advertising" contained in their privacy policies) indications about ads and clearly inform children and adolescents about whether personal data from user profiles is used to target advertising in accordance with every profile. Any improper advertising for children and adolescents is to be avoided.[16]

23. Every online social network must clearly indicate the reason for requiring certain personal data, specifically dates of birth at the time of registration and account creation. , It must be explained that the date of birth is required to verify the minimum age required for creating an account in the online social network.

The way in which this personal data (to be facilitated compulsorily) will be used is to be specified.[17]

The industry must implement mechanisms for the reliable verification of the age of children and adolescents upon the creation of user accounts and/or access to specific content.

24. All online social networks, communication systems and databases must include means to access, rectify and remove personal data for users and non-users, with consideration of applicable legal restrictions.[18]

Every online social network must have a defined policy, accessible to users, with regard to the preservation of information according to which the personal data of users who have deactivated their accounts is fully removed from the service's servers after a reasonable period of time. Likewise, all information on non-users is to be removed within a reasonable period after invitations have been forwarded to them to be part of the network. Online social networks should not use data regarding non-users.

---

[15] Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act*, July 16 2009.

[16] *Id.*

[17] *Id.*

[18] The spirit of the last paragraph is to not exclude —for the time necessary— the withholding of data on users that might result necessary in investigating crimes.

The means to deactivate or remove accounts must be fully visible to users, who in turn must understand what is implied in each of the options with regard to how the service will handle the data contained in such accounts.[19]

Users must be informed of the obligations relative to privacy with regard to third parties, and such policy is to be explicit, clear and visible.

25. The indexing of users of online social networks done by search engines is to be prevented, except in cases where the user has allowed such access. Indexing of data on children is to be banned in every form. In the case of adolescents, they must expressly authorize the indexing of their basic personal details.

26. All online social networks must establish the necessary means to restrict the access by third parties who develop the various applications offered by the service (games, questionnaires, notices, among others) to the personal data of users not necessary or relevant to the functioning of such applications.

Every social network must ensure that third parties who develop applications in their platforms may only access personal data of users with their express consent. Online social networks must ensure that third parties developers request nothing other than the data necessary and relevant to the use of their applications.

The adoption of measures necessary to avoid any transfer of personal data of users who have not expressly chosen to install such applications is equally important.[20]

27. These recommendations apply to the handling of personal data in online social networks, despite their legal domicile being outside Latin America and the Caribbean. In order to facilitate users' access to legal recourse, all companies providing online social networks must establish a domicile or legal representative in countries where such social networks have significant use or upon the request of government authorities. Online social networks must provide users with an efficient and effective support service with regard to the issues mentioned above. Such support must be provided in the official language(s) of the user's country.

28. Developers of web pages, services, applications, and platforms, among others, must define security filters as a supplementary means for the education, awareness and penalty instances.[21]

29. The industry must establish technical and operational measures to guarantee data security, specifically: the integrity, availability and confidentiality of information.

---

[19] Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act*, July 16 2009.

[20] Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act*, July 16 2009.

[21] **ITU Guidelines for Policy Makers** #13: *"Consider the role that technical tools such as filtering programmes and child safety software can play in supporting and supplementing education and awareness initiatives".*

30. In order to eradicate child pornography on the Internet, the industry must, as part of a joint effort of all responsible parties, commit to a minimum of:

30.1. Notifying the corresponding authorities of any occurrences of child pornography detected in the profiles of users of online social networks, in order to enable the necessary investigations and actions.

30.2. Preserving all data necessary for investigations for a minimum of six months or otherwise surrender such data to the corresponding officials, upon court authorizations.

30.3. Preserving the content published by users of social networks for an equal period of time, and surrender such content to the appropriate officials, upon court authorization.

30.4. Fully complying with national laws regarding cybercrimes committed by citizens of the countries of Latin America and the Caribbean, or through Internet connections from these national jurisdictions.

30.5. Changing customer service so that it can respond within a reasonable period of time to all claims made by email or conventional mail by individuals who have been victimized by false or offensive communities.

30.6. Developing efficient filtering technology and implementing the involvement of human site administrators in order to prevent the publication of child pornography photographs and images in online social network services.

30.7. Developing tools to enable hotlines to which children and adolescents can direct reports in order to allow the company's officers to analyze and remove any illegal content and inform the appropriate authorities about the inclusion in such contents of signs of child pornography, racism or other hate crimes, preserving all related evidence.

30.8. Removing illegal content, whether by court order or upon the request of the relevant official authorities, while preserving the data necessary for identifying the authors of such content.

30.9. Developing tools for communications with the relevant authorities in order to facilitate the management of reports, and the implementation of requests for the removal and preservation of data.

30.10. Properly informing national users on the common crimes committed in online social networks (child pornography, hate crimes, and attacks upon reputation, among others).

30.11. Developing educational campaigns on the law abiding and safe use of the Internet and online social networks.

30.12. Financing the publication and distribution of flyers to children and adolescents in public schools containing information concerning the safe use of the Internet and social networks.

30.13. Maintaining links in the sites of online social networks to sites for reporting problems or hotlines for the aid of children and adolescents.

FINAL CONSIDERATIONS

31. Recommendations made in the context of children and adolescents should also be applied to other individuals (adults) who may be in vulnerable situations due to their particular personal conditions.

Vulnerable groups are defined as those related to sensitive data (according to each national legislation) that usually include workers, dissidents, the disabled and their families, immigrants and emigrants, among others.

32. All parties involved are urged to discuss and consider these recommendations. Also, in light of what has been set for forth in this document, a permanent dialogue is to be sought concerning the issues herein. A special call is made with regard to the obligations pertaining to the States and to corporate social responsibility in order to implement this document in the best manner possible.

Montevideo, 28 July, 2009.

Recommendations adopted at the Seminar on Rights, Adolescents, and Internet Social Networks (with the participation of Belén Albornoz, Florencia Barindeli, Chantal Bernier, Miguel Cillero, José Clastornik, Rosario Duaso, Carlos G. Gregorio, Esther Mitjans, Federico Monteverde, Erick Iriarte, Thiago Tavares Nunes de Oliveira, Lina Ornelas, Leila Regina Paiva de Souza, Ricardo Pérez Manrique, Nelson Remolina, Farith Simon and María José Viega), held in Montevideo on July 27 and 28, 2009.