MEDIA INITIATIVES CENTER

Internet Freedom in Armenia and Execution of Basic Human Rights in Online Freedom

Independent Research Report Conducted in the Framework of the Project

"Advocating and Educating Online Human Rights"

Hasmik TAMAMYAN

Movses HAKOBYAN

June 2017 (updated in December 2017)

This report has been prepared by a team of external consultants. The views expressed herein are those of the consultants and therefore do not necessarily reflect the official opinion of Media Initiative Center/Armenia or ABA ROLI.

ACKNOWLEDGEMENT

The research team would like to acknowledge the valuable insight and feedback they received from the Journalists and Civil Society representatives as well as IT Security and Media experts that participated in in-depth interviews and focus group discussions. Special thanks to Samvel Martirosyan and Artur Papyan for their expertise and continuous support throughout the research cycle. The research team is grateful for the extensive support they received from the MIC Project team and Anna Barseghyan in particular as well as broader MIC team and Nouneh Sarkissian, Arshaluys Muradyan, and Gegham Vardanyan for their project related expertise and for facilitating the research process.

Table of Contents

I. INTRODUCTION

This is the Independent Research Report summarizing the findings drawn from document analysis, a series of in-depth interviews and focus group discussions conducted in the framework of the project "Advocating and Educating Online Human Rights" being implemented by the Media Initiative Center/Armenia (the Project). This is a summative research to assess Internet freedom in Armenia and the execution of basic human rights in online environment. The research is also intended to develop recommendations and lessons learned to inform potential future program design and policy making.

1.1. Background and Context

As reported by the Freedom House in its "Freedom on the Net 2016" annual report "Internet freedom remained largely uninhibited in the [previous] year, though Armenia's overall score declined somewhat after police physically attacked journalists livestreaming protests in Yerevan." While Armenians are generally free to express themselves online without major restriction or fear of being sanctioned, some incidents of control and censorship occurred during and after the Freedom House coverage period, mainly coinciding with the periods of violence, unrest, and spontaneous escalations of the Nagorno Karabakh conflict. Moreover, after the independent media Twitter accounts were briefly suspended around the April 2017 parliamentary elections, Internet freedom and Internet freedom scores declined in Armenia by changing the country's status to "partly free" as reported by the Freedom House's "Freedom on the Net 2017" annual report. Facebook was briefly unavailable in July 2016 while armed militants were challenging the authorities, and Internet users were "advised" to self-censor as violent clashes briefly resumed on the Nagorno-Karabakh frontline. Earlier in June 2015, police targeted journalists and civic activists livestreaming the Electric Yerevan protests in the capital, forcing them to leave the area and confiscating their video equipment. Nevertheless, traditionally Internet has remained relatively free in Armenia, with steady improvements in accessibility and infrastructure connecting over the half of the Armenian population (as of 2016 with 62% using the Internet as reported by ITU). Journalists and civic activists largely use social media as a tool to promote their causes, and opposition and independent media flourish online.

The experts in the field and the Freedom House Index classify Armenia as Free with few obstacles to the Internet access, limits on online content, and violations of the Internet user rights. The observations however point out that while Armenia's laws are generally non-aligned, there are still big concerns related the state intervening with the online content and traffic of a number of targeted Internet users. The specific issues the analysis raises are quite a few incidents of wiretapping, hacked websites and personal accounts, and the government's non-response to the issues.

With its newly initiated "Advocating and Educating Online Human Rights" Project the Media Initiatives Center (MIC) targets civil society representatives and journalists to first of all evaluate the level of their knowledge and skills related to cyber security and to study the scope of the problems they are facing in the Internet while dealing with their day-to-day activities. The Project aims at understanding to what extent the targeted professionals enjoy their basic human rights in the online environment and how best they can combat the existing and emerging cyber security risks and threats.

The last decades has witnessed an incredible rise of online media, which is overtaking the area held by traditional media. The Internet also offers what seems to be a potential solution for civil society integration into the representative democracy activating weak ties between citizens and decision-makers and encouraging public participation. It is a good platform for enhanced deliberation, information exchange, and public participation, which in its turn serves greatly to the final goal of the democratization of information. However, the democratization of information through world-wide net depends on access and literacy guaranteed by the principles of Internet freedom and media literacy of individual users. To ensure their own freedom in the Net, societies and individual professionals should seek and claim for freer Internet - free form government control over the online content as well as unrestrained by big business forces. Having in mind the right to free Internet and having in hand tools, knowledge, and skills to ensure one's own digital security is the only way for individuals and particularly media professionals and civic activists to make most of the opportunities provided by the Internet, hence contributing to the democratization of information and participatory decision-making.

The advocacy and outreach project initiated by the MIC will have two main outputs: (a) this Report summarizing the research findings, and (b) an online game - the Cyber Freedom online multimedia toolkit. This Report outlines the main challenges related to the Internet security in the country and recommends solution strategies to address those challenges. It will hopefully serve as a working document for policy-makers, Project stakeholders and the targeted groups of professionals. The Game will educate people on their online human rights and raise awareness on existing cyber security threats.

II. PURPOSE AND METHODOLOGY OF THE RESEARCH

2.1. Purpose of the Research and the Research Team

The main objective of the Research was to:

- analyze the Internet, Internet freedom and cyber security related legal framework and policies of Armenia;
- evaluate how wide-spread are the cases of violations of online human rights;
- assess how these rights are being exercised by targeting media professionals and civic activists;
- evaluate the information security related knowledge and skills of the targeted professionals/activists;
- Recommend possible initiatives and further activities for improved and safe use of the Internet among the targeted professionals.

The Research was conducted by a team of independent consultants - an independent researcher specialized in development and media related research, and a legal expert with extensive experience in the Internet and digital security related issues:

Research team leader:	Hasmik Tamamyan
Legal expert:	Movses Hakobyan

2.2. Data Sources and Data Collection Methods

The research team draws conclusions based on triangulation of evidence from different data collection methods and primary/secondary data sources.

Data collection methods

The following data collection methods were employed to conduct the evaluation:

1. **Legislation Review/Document Analysis** of the RA laws and legal acts as well as International treaties signed/ratified by Armenia. Document analysis also included country reports and statistics provided by national agencies and international organizations. A thorough review and analysis of legal documents and National/International reports provided a wealth of evidence for this research assignment.

2. **Individual in-depth interviews** with selected key experts and representatives of the targeted groups of media professionals and civic activists. In-depth interviews were conducted to get comprehensive information and opinions about the topics such as Net Neutrality, Recognition and protection of human rights in online space, Problems that the targeted professionals usually face in dealing with their day-to-day activities. Individual in-depth interviews were conducted with selected key IT security experts and media professionals, as well as civil society representatives. The team developed a semi-structured interview guide (see Annex 5.1) for expert interviews. 14 face-to-face interviews (Annex5.2) were conducted based on purposive sampling technique, where the key experts were selected based on the level of their expertise and involvement in the field.

3. **Focus group discussions** with journalists, civic activists and NGO representatives. Use of this method aimed at promoting discussion on self-created and external IT security risks, recognition and protection of online human rights, etc. The research team explored and identified how these issues are being addressed at an individual, institutional, and policy levels by moderating discussions among media and civil society representatives actively using the Internet and social networks for promoting their causes and the content they created. Focus group discussions Guideline is included in Annex 5.1.

Focus Group (FG) Discussions Participants

FGs	Type of participants	Number of FGs	Number of participants per FG	Type of sampling	Selection criteria (female/male)
FG1	Individual civic activists	1	7	Purposive sampling	5-f/2-m
FG2	NGO representatives	1	7	Purposive sampling	5-f/2-m
FG3	Journalists	1	6	Purposive sampling	4-f/2-m

III. ANALYSIS AND FINDINGS

3.1. Legislative Framework related to Human Rights and Freedoms in Armenia equally applicable in Cyber Space

The Armenian legislation does not literally specify differences between online and offline legal relations nor digital rights and freedoms of individuals are identified. However, the common interpretation of legal acts in force implies equal application of law to cyber space. Armenia is a member state of a number of international organizations and the signatory to the key international and regional human rights treaties, and, therefore, is legally bound by these commitments, including those directly or indirectly guarantying freedoms and rights in digital sphere. Armenia is a member of the United Nations, thus is a party to the International Covenant on Civil and Political Rights (ratified on 23 June 1993), which sets out in Article 19 "freedom to hold opinions" and to "seek, receive and impart information and ideas through any medium and regardless of frontiers." As a member of the Organization for Security and Co-operation in Europe (since 30 January 1992), Armenia undertook to respect the standards set out in the Helsinki Final Document and further declarations of the OSCE. Moreover, as a member State of the Council of Europe, Armenia signed (on 25 January 2001) and ratified (on 26 April 2002) the European Convention on Human Rights (ECHR), Article 10 of which protects freedom of opinion and expression.

The Constitution of the Republic of Armenia as of December 2015 provides for all basic rights and freedoms that are enshrined in the abovementioned international treaties. And as of the opinion of the European Commission for Democracy Through Law, also known as the Venice Commission, the last amendments made to Constitution of Armenia in 2015 are in line with basic international standards. The second chapter of the Constitution (Basic Rights and Freedoms of the Human Being and the Citizen) is totally devoted, inter alia, to such rights and freedoms as (1) Freedom of expression; (2) Privacy and protection of personal data; (3) Right to Receive Information. In particular, Article 31 (Inviolability of Private and Family Life, Honour and Good Reputation) stipulates that everyone shall have the right to inviolability of his or her private and family life, honour and good reputation that might be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others.

In the same way, through the Article 33 (Freedom and Secrecy of Communications), Constitution ensures the right to freedom and secrecy of correspondence, telephone conversations and other means of communication to everyone. The limitations on freedom and secrecy of communication might be envisaged only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others. Authorization for interception, wiretapping or other limitations on secrecy of communication is granted only upon court decision, according to purposes prescribed by law.

The Constitution of Armenia also provides for Right to Receive Information as a basic right of human (Article 51) that is directly related to securing transparency and accountability of the executive. Particularly, the Constitution stipulates that everyone shall have the right to receive information and get familiar with documents relating to the activities of state and local self-government bodies and officials. Furthermore, the second point of the Article 51 provides that the right to receive information may be restricted only by law, for the purpose of protecting public interests or the basic rights and freedoms of others.

Freedom of Expression of Opinion is one of the key principles envisaged by Article 42. It provides the right to freely express opinion including freedom to hold own opinion, as well as to seek, receive and disseminate information and ideas through any media, without the interference of state or local self-government bodies and regardless of state frontiers. It is noteworthy that this norm in its essence is technologically neutral and does not differentiate means of media and communication types. In other words, it is equally applicable to enjoyment of free speech, mass media and information in cyber space. The same wording might be seen in the Resolution on the promotion, protection and enjoyment of human rights on the Internet that was adopted by the UN Human Rights Council on 29 June 2012. The restrictions on Freedom of expression of opinion might be imposed only by law, for the purpose of state security, protecting public order, health and morals or the honor and good reputation of others and other basic rights and freedoms thereof.

According to Article 34 (Protection of Personal Data) of the Constitution everyone shall have the right to protection of data concerning him or her. The processing of personal data shall be carried out in good faith, for the purpose prescribed by law, with the consent of the person concerned or without such consent in case there exists another legitimate ground prescribed by law. Everyone shall have the right to get familiar with the data concerning him or her collected at state and local self-government bodies and the right to request correction of any inaccurate data concerning him or her, as well as elimination of data obtained illegally or no longer having legal grounds. The right to get familiar with personal data may be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others. Details related to the protection of personal data are prescribed by Law on Protection of Personal Data. The later, also prescribes establishment of Agency for Protection of Personal Data under the Ministry of Justice. This Agency, as an authorized regulatory body, is in charge of controlling the implementation of Law requirements for the protection of personal data and may impose guidelines, regulations and provide legal assistance to the people.

In line with ECHR standards, the Armenian Constitution provides conditions of proportionality - Article 78 (Principle of Proportionality) and certainty - Article 79 (Principle of Certainty) applicable to all restrictions on fundamental rights and freedoms. Furthermore, the Constitution envisages the notion of "inviolability of the essence of provisions on Fundamental Rights and Freedoms" - Article 80. On the other hand, Article 76 of the Constitution makes it possible to restrict the mentioned rights and freedoms in State of Emergency or Martial Law.

For further regulation of basic rights and freedoms, Article 75 of the Constitution stipulates that laws shall define organizational mechanisms and procedures necessary for effective exercise of these rights and freedoms. In line with the Article 75 of the Constitution, the legislative body of Republic of Armenia adopted several laws related to freedom of information and rights that can be both exercised and restricted in the cyberspace such as:

Law on Mass Media (13 December 2003; in Armenian)

Law on Freedom of Information (23 September 2003; in Armenian)

Law on Protection of Personal Data (May 18 2015)

Criminal Procedure Code (1 July 1998; in Armenian)

Criminal Code (18 April 2003; in Armenian)

Law on State and Official Secrets (3 December 1996, in Armenian)

Law on Operative Investigative Activities (22 October 2007, in Armenian)

Government Decision on Setting List of Special Technical Means for Conducting Operative Investigation (31 July 2008, in Armenian)

Law on Electronic Communication (13 August 2005, in Armenian)

Law on Copyright and Related Rights (15 June 2006, in Armenian)

Law on Television and Radio (9 October 2000, in Armenian)

3.2. Net neutrality

The net neutrality principle is not defined by the legislation of Armenia but the telecom operators and providers of the services must publish and inform the subscribers, in case, if they don't support in the net certain protocols or make the priority for the specific traffic (see p.4 (6) of the Resolution of Public Services Regulation Commission 471-N dated September 8, 2008).

Blocking/Filtering and Illegal Content: Relevant regulation on blocking or filtering online content is missing in Armenian legislation and court practice (case law) is not formed yet. Moreover, the reported cases of restriction on public communication or access to public resources is one of the vague areas of Armenian communication and media legislation.

Armenia joined the Budapest Convention on Cybercrime in 2006 and officially stands behind that mechanism as the best approach to combat cybercrime. Respectively, Armenia amended Criminal Code to criminalize those cyber offenses enshrined in the Convention on Cybercrime. Although Armenia is a signatory of the Convention, there is very little publicly available empirical data on cybercrime. Neither systemized nor analytical data is available for research purposes. Limited information can be obtained from official statements and press releases of the Police Service, General Prosecutor's Office, private security companies and mass media.

The Criminal Code envisages general limitations on content, without specification of means of dissemination. In particular dissemination of pornographic materials, hate speech, and campaigning for the overthrow of the Constitutional order are classified as criminal offenses. However Armenian legislation does not specifically require communication service providers to block or filter online content.

Internet hosting or service providers registered as a local company can only be held liable for illegal content if it can be proven they were aware of it. This offence is treated within corporate liability leading only to Administrative sanctions. Moreover, these companies are not obliged to monitor transmitted or stored content, as there is no legal obligation prescribed by law. However, if operator's particular employee in charge willingly and knowingly thus intentionally disseminates illegal content such as pornographic materials, he or she could be liable under Article 263 of the Criminal Code.

In contrast, electronic mass media companies such as online resources and broadcast media have explicit obligations in regard to content prescribed by the Law on Mass Media (Article 7) and the Law on Television and Radio (Article 22) (Restrictions on the freedom of speech in the sphere of the media – hate speech, erotic/pornographic content, ethnic, religious or racial discrimination, protection of minors, state or other secrets protected by the law, etc).

Surveillance: Unlawful surveillance in Armenia does not appear to be prevalent. However, the legal environment grants extensive powers to the authorities to conduct lawful surveillance within a well-developed legal framework. Article 33 (Freedom and Secrecy of Communications) of the Constitution protects “Everyone shall have the right to freedom and secrecy of correspondence, telephone conversations and other means of communication, [….] which could be restricted only by law for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others [….] only upon court decision, except where it is necessary for the protection of state security and is conditioned by the particular status of communicators prescribed by law.”

The Criminal Procedure Code defines the boundaries of confidentiality as well as lawful powers to intercept and wiretap phone conversations, correspondence, and other types of communication. Surveillance without a court order or consent of the intercepted persons is considered a crime (Article 146).

In fact, the Main Department of the National Security Service is the only body authorized to intercept private communication and wiretap telephone conversations, or to access equipment located in the facilities of telecom operators (Article 284). In order to monitor/wiretap any individual, the investigative body must first obtain a court order. It is noteworthy that the Criminal Procedure Code does not provide precise legal criteria neither for courts to order interception nor benchmarks for the investigatory bodies’ motion (Article 50). In practice, judges consider the appeal on an ad hoc basis. As a result, court rulings lack consistency and predictability.

The List of Special Technical Means for Conducting Operative Investigation set by the Government Decision enumerates the tools and applications for conducting lawful surveillance. The list of technology requirements is comprehensive. It authorizes the development of technical tools, both software and hardware, specifically designed to capture information in computer systems and computer networks, and to intercept all forms of electronic communication, including text, voice, and multimedia content. The Armenian authorities are developing advanced technical capabilities to monitor and investigate online activity, though a rigorous legal framework of checks and balances is designed to provide the necessary safeguards to prevent state abuse of such powers. In this regard, telecommunication operators are obliged to provide facilities and support for rendering operative-investigative actions to relevant bodies. Moreover, the wording of Article 31 of the Law on Operative-Investigative Activities imposes obligation on telecommunication and postal companies to provide technical systems per request of the Main Department of National Security Service (NSS) and create other relevant conditions, which are necessary for implementation of operational investigation activities. The later could be (and most likely will be) interpreted as an explicit obligation of communication operators to provide all those interception equipment at their expense.

In exceptional cases, if surveillance is required immediately and a procedural delay could lead to a terrorist act or threaten national, military or environmental security, the head of the investigative body can make a direct request to the Main Department of the National Security Service to provide access to the information 48 hours prior to receiving a court order (Article 31, 32 of the Law on Operative Investigation Activities); Article 239 (2, 4) of Criminal Procedure Code; Article 31 of the Law on Operative Investigation Activities; Article 50 of the Law on Electronic Communication). If the court denies the motion, the investigative body must desist immediately and destroy the obtained data (Article 284 (8) of Criminal Procedure Code). Investigative bodies are not allowed to store or disclose data except in cases prescribed by law (Article 50 of the Law on Electronic Communications).

Private Data Protection/Secrecy of Communication: The Law on Protection of Personal data is adopted in May 18, 2015 to meet the obligations undertaken by the CoE Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data. The law regulates the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-government bodies, state or community institutions or organisations, legal or natural persons. What is more, the Agency for Protection of Personal Data has been established, which is a specialized regulatory body in charge of enforcement and protection of rights envisaged by the Law. It shall be noted that Law on Protection of Personal Data provides basic mandatory principles for processing of personal data such as:

(1) Principle of lawfulness - Personal data shall be processed in observance of the requirements of the law for legitimate and specified purposes and may not be used for other purposes without the data subject's consent.

(2) Principle of proportionality - the processing of data must pursue a legitimate purpose, measures to achieve it must be suitable, necessary and moderate with the processing of the minimum volume of personal data that are necessary for achieving legitimate purposes. The processing of personal data that are not necessary for the purpose of processing of data or are incompatible with it shall be prohibited. The prohibition is applicable also when the purpose of processing of data is possible to achieve in a depersonalised manner. Personal data must be stored in such a way as to exclude the identification thereof with the data subject for a period longer than is necessary for achieving predetermined purposes.

(3) Principle of reliability - The personal data being processed must be complete, accurate, simple and, where necessary, kept up to date.

(4) Principle of minimum engagement of subjects - Where the state administration or local self-government body, the notary are able to obtain the personal data from other body through a uniform electronic information system, personal data subject shall not be required to submit personal data necessary for certain operations. In case of a written consent of the personal data subject, natural or legal persons considered as a processor of personal data may obtain from a state or local self-government body personal data necessary for a certain operation and directly specified in the written consent of a personal data subject.

On the part of telecom operators, the Law on Electronic Communications defines the circumstances under which telecommunication providers can or must disclose the personal data of their users. These circumstances are:

“Article 49. Privacy of Customer Information

[…] 2. An operator or service provider may disclose such information:

1) As authorized by law in connection with the surveillance, investigation or prosecution of a criminal offense or threat to national security;

2) With the written consent of the customer;

3) Where the disclosure is necessary in defense of the operator or service provider (in any law proceedings brought against that operator or service provider). The customer may request that such disclosure be made on a confidential basis at an in-camera proceeding.”

As a matter of general rule, telecom operators are not allowed to store or disclose in any manner communications (content) except in cases prescribed by the Law. Moreover, according to Article 50 of the Law on Electronic Communications “no person other than a party to a message transmitted by any electronic communications means may intercept, tap or disclose the content of this message unless authorized to do so in writing by the parties to the message or by a court decision pursuant to the Law.”

Legal protection: Protection of individuals’ rights are enforced by means of filing a suit, complaint or application to the court, Law enforcement bodies, higher body supervising the respondent body, specialized body like Agency for Protection of Personal Data or Office of Human Rights Defender. Except national legislation, protection of individual rights is imposed on Armenia as a positive obligation to have a leading role in enforcement of individual rights either in offline or online environment. In particular, protection of online rights is recommended by International legal acts such as the Council of Europe's Recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a Guide to human rights for Internet users which emphasizes: *"the obligation to secure for everyone within their jurisdiction the human rights and fundamental freedoms enshrined in the European Convention on Human Rights (ETS No. 5, the Convention). This obligation is also valid in the context of Internet use. Other Council of Europe conventions and instruments, which deal with the protection of the right to freedom of expression, access to information, the right to freedom of assembly, protection from cybercrime and of the right to private life and to the protection of personal data, are also applicable."*

International Standards/Recommendations

Nowadays digital tools and technologies evidently present serious challenges to the enforcement of the basic human rights, particularly to privacy, freedom of speech, media and related rights. Moreover, one person's right to freedom of expression may impinge on someone else's right to privacy or national security concern might be opposed to civil liberties. This tension is exacerbated by proliferation of digital technologies into everyday life of more and more people. Whilst they have been central to the facilitation of the exercise of freedom of expression and the sharing of information, digital technologies have also greatly increased the opportunity for violations of the rights and limitations on freedoms. In particular, digital technologies present serious challenges to the enforcement of the right to privacy and related rights because personal information can be collected and made available across borders on an unprecedented scale and at minimal cost for both companies and states. At the same time, the application of data protection laws and other measures to protect the right to privacy can have a disproportionate impact on the legitimate exercise of freedom of expression.

To address these issues and explore the intersection between these opposing concepts and find balanced approach, united efforts of society are needed. Fortunately, global community is striving for development of universal set of digital rights accompanied by calls and efforts to formulate an "Internet Bill of Rights" or Internet Magna Carta that would define a new set of rights for the digital age. These are generally elaborated main standards of digital rights that might be considered in the Armenian society:

- **Right to Inter-Networking** - Everyone has the right to benefit from Internet architecture that is based on decentralization, open standards, interoperability and end-to-end principles.

- **Right to Access** - Everyone has the right to participate in the information society and to access, regardless of their geographical location, universally available Internet services at affordable price.

- **Net Neutrality** - Everyone has the right to receive an unimpeded flow of transboundary Internet traffic.

- **Right to anonymity** - Everyone has the right not to be identified and not to disclose their identity when using the Internet.

- **Right to encryption** - Everyone has the right to use secure communication tools, in particular any hardware and software encryption products and other cryptographic methods of their choice.
- **Right to be free from surveillance** - Everyone has the right to be free from mass surveillance, interception and persuasive monitoring measures by State, commercial and other entities.
- **Right to blog** - Everyone has the right to disseminate information and ideas to the public through the Internet and digital technologies without permission, license or registration.
- **Right to create** - Everyone has the right to create content online.
- **Right to share** - Everyone has the right to receive, impart and personally enjoy cultural goods online.
- **Right to digital protest** - Everyone has the right to use digital tools to engage in individual or collective protest actions. This right includes the usage of the Internet and digital tools as both a medium and a venue of protests.
- **Right to dissent, offend and be offended** - Everyone has the right to express, disseminate and receive oppositional, dissenting, reactive or responsive views, values or interests through the use of digital technology.
- **Right to be free from liability -** Everyone has the right to be free from liability for content of others online. This right includes immunity from liability for

    a) the content of third parties where he/she has not been involved in modifying that content;
    b) the failure to restrict lawful content;
    c) hosting unlawful third-party content; or
    d) the failure to proactively monitor content of others.

- **Right to hack** - Everyone has the right to break and explore digital codes in public interest and for non-commercial purposes; in particular to surmount technological barriers to information that implement and enforce restrictions to content which should be readily available and accessible.
- **(VPN) Right to run one's own** - Everyone has the right to run their own servers and services, create virtual private networks and provide services to others on the net.

- **Right to floss** - Everyone has the right to access and use free/libre and open source software (FLOSS)
- **Right to control data** - Everyone has the right to exercise full control over their personal data. Personal data should be processed only if the individual gives full and informed consent to their processing.
- **Right to know-how** - Everyone has the right to free digital education and knowledge to exercise their rights in the digital environment.
- **Right to participate** - Everyone has the right to make informed decisions and participate in Internet governance, in particular in governance mechanisms and in the development of Internet-related public policies, in full confidence and freedom.

3.3. Internet freedom, cyber security related knowledge and practices among the targeted groups of media professionals and civil society representatives

Journalists and advocates should be increasingly concerned about their digital security and freedom in the Net with good reason. While computers and the Internet can be really useful and prevailing tools for collecting and disseminating the necessary information and advocating for causes, they also expose those groups to new threats. The more those groups have begun to rely on technology and the Internet to achieve their research, communication, content development, and outreach objectives, the greater these risks have become. Given all this, we started our interviews and discussions with the targeted journalists and civil society representatives with the main question on how much of their daily work and communication was done through the Internet and whether or not they think they were advanced Internet users.

Usually the focus group members and interviewed journalists/civic activists reported themselves as not very advanced users, although they had been using the Internet on everyday basis for both professional and personal purposes. They can hardly imagine their lives without email, Facebook, Twitter, Skype, WhatsApp, Viber and other social networks and communication platforms these days. However, they wouldn’t say they had good or advanced knowledge and skills to ensure security of their devices, accounts and sources. A good number of interviewed journalists and civil society representatives are in charge of updating and uploading new content into their organizations’ websites. All of them widely use the Internet for their work related research coming across and evaluating the credibility of the new websites and online resources on a daily basis. Last but not least, they keep in touch with their sources, key informants, and beneficiaries/stakeholders through all the above mentioned communication channels and should be concerned about the protection and confidentiality of their information and sources.

The level of digital security related knowledge and skills among the Armenian journalists and civil society representatives (also as reported by themselves) leaves much to be desired. Most of them try to create long and complex passwords and quite often they turn on 2-factor authentication for their accounts. They follow the simple rules of not having the same password for all accounts or changing passwords once in 1-2 months. Most of them also reported being cautious while surfing the Internet for new sources of information and unfamiliar URLs. This is however the complete list of the security measures commonly followed by the representatives of the targeted groups. Only very few mentioned that they have passwords for their portable devices and among those only the minority knew exactly what they were going to do, if their devices full of sensitive information and contacts were confiscated, stolen and/or lost.

All interviewed journalists and civil society representatives as well as those who took part in the focus group discussions have heard true stories about the risks related to pubic Wi-Fi. This however doesn't make most of them refrain from using public Wi-Fi from time to time "in case of urgency" without being fully aware of the consequences and risks the exposure of their traffic and data could cause and without realizing that they can easily leak their personal and company data. With only a few exceptions, when the organization has strict policies related to public Wi-Fi, the majority of interviewed journalists/civil society representatives admitted using free Wi-Fi, because they were desperate to be online not just for business, but for personal reasons as well.

Everyone among the interviewed journalists and advocates is sure that the organization they represent uses licensed program packages and software, but very few reported having them on their personal devices. Nevertheless, conclusions drawn from the interviews with Armenian IT security experts as well as the most recent statistics provided by the Software Alliance completely shatters the confidence that the journalists and NGO representatives had in the software running in the LAN networks of their organizations. According to the BSA Global Software Survey (2015), the rate of unlicensed software in Armenia is 86% compared to the total 39% worldwide. The explanation why companies or individuals choose unlicensed software over the licensed ones can be quite complex, however in one way or another they can be summed up into two basic rationale – scarcity of financial resources and inaccurate evaluation of IT security risks. Very few representatives of media outlets and NGOs mentioned that their organizations were running open source operating system, namely Ubuntu/Linux, the majority still heavily relies on Windows.

Only some of the interviewed/focus group participant journalists and civil society representatives said they were using Tor browsers to protect their digital identities, despite all the discomfort caused by a much more sluggish Internet than usual. Even fewer respondents mentioned that they were using PGP encryption to communicate with their colleagues, sources, and stakeholders. An interesting observation is that all journalists/civil society representatives, who reported using PGP encryption tools (mainly Mailvelope and rarely FTP video downloader), had to do so, because of the strict requirement from their foreign or international counterparts, partners, and colleagues. Those who prefer not to use encryption, think it would take much more time to send/receive/decrypt messages and a lot of effort to become skilled at using encryption and private keys.

The interviewed and focus group participant journalists seemed to agree that self-censorship is what works the best to protect them from unwanted attention and attacks in the Internet in general and social networks in particular. It is mainly done out of fear of sensibilities and real or perceived preferences of others (especially politicians and business leaders) and without any evident pressure from any specific institution or authority. However, during focus group discussions the journalists shared true stories about continuous attacks on their social media profiles (quite often from fake accounts), just because someone or a group didn't like the content (a comment, video or photo) they shared. Journalists have often self-censored publications of news stories out of concern for the safety of people involved.

From the legal point of view, although the Armenian Constitution guarantees freedom of speech, information and media, and legislation in general is considered as pretty liberal, still there are risks impeding realization of those rights and freedoms. As evidence, in 2008 for the first time in the history of the Republic of Armenia, under the terms of the state of emergency declared by the outgoing president, publications of mass media concerning state and internal political issues were limited to "official information of state bodies" only. During 2016 civil unrest triggered by protests surrounding a political hostage crisis in Yerevan, Facebook was cut off for about an hour. Moreover, journalists streaming live broadcasts from the site were targeted and prevented from getting media coverage. Consequently, according to the last report on Freedom of Net 2017 by Freedom House, Armenia lost two points and ranked among countries with partly free Internet. This fact negatively affects the image of Armenian democracy, let alone Press freedom status that is not free since 2003. Decline is followed the closing of the country's leading independent television station A1+ and the government's continued attempts to stifle criticism in the media. The reasons behind of the abovementioned are purportedly lack of checks and balances between branches of power, low level of public participation and institutional capacity of the civil society. To sum up, the state of Internet, as a matter of fact, is a reflection of not only the legal environment, but also a political reality that might directly affect freedoms guaranteed by the law.

3.4. Online vs. Offline Human Rights: If not completely the same, where is the overlap? Cases of the Internet restrictions during the last decade in the territory of Armenia

It has been almost a year since Internet access was declared a human right, yet violations continue. In Resolution A/HRC/32/L.20 passed in July 2016, the UN Human Rights Council described the Internet as having "great potential to accelerate human progress" by condemning "measures to intentionally prevent or disrupt access to or dissemination of information online." The non-binding resolution emphasized that the exercise of human rights on the Internet (and namely the right to freedom of expression) is an issue of increasing interest and importance. Over the last several years the Human Rights Council (UNHRC) has said that rights which the individual enjoys offline apply online as well. Nevertheless, there's a little if anything in international and national human rights laws that says everyone has a right to the Internet. The only mention is in the Universal Declaration of Human Rights and the international covenant on civil and political rights both having an Article 19, which sets the standard and says that “everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

To understand what this means for journalists, civil society representatives as well as IT security experts based in Armenia, we elaborated the discussion further on the topic during the in-depth interviews and focus group meetings. To what extent is Internet access a human right? Whether the basic human rights anyone enjoys in real life is applicable to online environment as well? Where there any recent cases of the government blocking the Internet access or social media and what can be done in situations like that? What are the legal justification for controlling the net and traffic? Those were the main questions provoking big discussion during the sessions.

In March 2008 the Internet Society of Armenia froze several opposition newspaper domains after a series of mass protests against widely believed electoral fraud. Under the state of emergency, mass media could only publish official government news and several opposition media had been shut down, including A1+ and Haykakan Zhamanak news portals. Radio Free Europe/Radio Liberty's Armenian Service has been terminated and even their website has been blocked by the Armenian authorities. The YouTube web site was blocked for a week time period preventing the dissemination of eye-witness videos from the sites of the protests. Since then all national elections have been accompanied by minor cases of blocked websites. It is not, however, always clear, if we are dealing with the so-called DDoS attack or just some sort of technical limitations of the domain hosting and websites’ disability to maintain high levels of peak traffic, when a piece of election fraud exposing content goes viral. The most recent example is www.sut.am, the website of an independent mass media founded by the Union of

Informed Citizens Advisory NGO that collected evidence and uncovered and published cases of widespread misuse of administrative resources in schools and kindergartens of the country ahead of the Parliamentary elections 2017. Social media accounts of media representatives and activists have also constantly been at gunpoint during elections with the most recent cases of Twitter accounts of several prominent Armenian journalists suspended for several hours a day before the Parliamentary elections in April 2017.

Earlier in April 2016 the Armenian government censored reporting during the outbreak of violent hostility over Nagorno Karabakh. Journalists working along the borderline of military activities reported having restricted access to the Internet most probably due to national security reasons. Likewise, to meet a legitimate objective like national security and public order, Facebook was temporarily unavailable in Yerevan in an isolated incident in July 2016, when a group of armed rebels seized a police regimen and held hostages. In June 2015, police targeted journalists and civic activists livestreaming the Electric Yerevan protests in the capital, forcing them to leave the area and confiscating their video equipment. Journalists, who were covering the protests from Baghramyan street, reported that the Internet services were widely disrupted although admitting that it could be caused by the big number of users connecting to the Internet from the same physical space. In May 2015, a parody of the police response to protests in Yerevan was removed by YouTube. The video was reported by the police for "removal for copyright infringement, since it contained a copyrighted clip of a news report", though it was likely targeted, because it was mocking police behavior. The incident was followed by the Armenian police taking the authors of the web series, SOS TV, to court claiming the episode contained insults towards the police.

These cases came along with the Freedom House report, the US-based freedom of expression watchdog, saying that Internet freedom across Armenia had slightly declined for the last couple of years. The organization said that in general, online content is widely accessible for Internet users in Armenia. However, during times of civil unrest and Karabakh conflict escalations, the government has been known to restrict access to social networks and other websites by targeting journalists, bloggers, and civic activists, which is clearly a direct interference with freedom of expression.

The rule in human rights law is that any restriction on freedom of expression or any breach of personal data has to be provided by law, necessary, and proportionate in order to protect a specific objective - basically the rights and reputations of others, national security and public order. When we see a state block a website or take down the Internet, a lot of questions arise. Most focus group participants and interviewed professionals agree that it is not enough for a state to have a law that allows the blocking of a website, not even speaking about unwritten agreements with mobile operators to do so. Often, when a state intervenes to the Internet traffic and blocks access to a specific website, the state does not show why it is necessary to do that to meet a legitimate objective like national security and whether they have alternative means to deal with threats to national security and public order.

Majority of the focus group participants and interviewed professionals agreed that the rights a person could enjoy in her/his real life should be equally protected in the online environment as well. The Internet provides a huge space and better opportunities to exercise freedom of speech and other basic human rights; however it is also a fertile soil for online bullying and anonymous treats and attacks. The journalists and civil society representatives shared plenty of stories from their own experience claiming also that each individual victim of online bullying had to deal with their case on their own without any support from or involvement of their professional communities. Given the general distrust towards the state, the law enforcement agencies, and the court, they did not even try to seek protection through legal channels.

The line between the legitimate objectives (such as national security or reputation of others) and free Internet is very thin. How much a state has the power to intervene in the net and manage the traffic is the biggest policy-related question in the field. Is the state's power limited to the cyber crimes that took place in its territory only or there should be some other principle applied to the matter? Those were the questions that provoked big discussion among the journalists and civil society representatives during the focus group discussions without bringing to any consensus in the end. The interviewed representatives of the Armenian IT community, however, share more or less similar opinion on this. They all agreed that the lack of any specific laws or policies regulating the Internet makes Internet governance more liberal than it could be expected. Paradoxically, Armenia has not been following the path Russia has recently adopted to take the control over the Internet traffic in the territory of its country. Armenian decision makers and the IT community are more inclined to the western approach of the Internet governance shaped by the multi-layered nature and historic development of the net.

The complex multi-layered nature of the Internet means that there is no one that overseas all aspects of the Internet. The development of the Internet as a patchwork of computer networks using shared software protocols and which is largely operated by private entities has led to a unique multi-stakeholder governance model, which entails the participation of governments, the private sector, civil society as well as the end users. This model sets the Internet apart from all previous communication channels and technologies, such us the telegraph or telephone, which were largely controlled by governments across the world, and shapes new realities, questions, and principles for the Internet development. In recent years, policy debates and regulations on network neutrality have crystallized several key principles:

- **Transparency** – Operators must provide comprehensive and accurate information on their network management practices and quality of service to their customers;

- **Non-discrimination** – Operators should make no discrimination on traffic based on origin of sender/receiver; and type of content, type of application and/or service.

- **Access** – Users should be able to have unrestricted access to any LEGAL content, service or application (with minimum quality of service guaranteed for the meaningful use) or to connect any hardware that doesn't harm the network.

Drawn from the interviews and focus group discussions, unfortunately in Armenia the main mobile operation and telecommunication companies do not have a lot of opportunity to fully comply with these principles and resist government restrictions. If the government says to shut down the Internet in a place or to provide full access for surveillance, it is hard for them to say no. The issue here is to try to encourage those companies take the side of their customers and to push back where they can and demand judicial orders. These companies surely lose part of their profit during Internet shutdowns, so they should do the cost-effectiveness analysis and realize what economic leverage they might have to push back these restrictions. It is not a big secret that they do not have a lot of flexibility in responding to the government's demands, so the protection of the end-users rights has to be looked for in another place. Those groups of people, who are advocating for free Internet and protection of personal data, journalists and activists, need to be constantly pushing for laws and practices that protect digital space and demand that governments meet their obligations in digital spaces just as in non-digital spaces.

The ease and assurance with which the focus group participants were speaking about the continuous surveillance and wiretapping they or their colleagues have been subject to, show how widespread the cases are and speak more about the unrestricted possibilities for the state agencies (namely the National Security Service) to arrange it even without a prior notice to the mobile operators. Not that there are checked facts about such cases, however, especially civic activists believe that because they advocate for specific causes and share sensitive content and ideologies challenging the government and their close-by business, their phone conversations and online communication have always been closely monitored and censored and quite often their blogs and websites were attacked and blocked. Like their websites' DDoS attack cases, their social network accounts are also being targeted by fake visitors by making it almost impossible to identify the attack's mastermind.

3.5. What makes a journalist or an advocate a target for cyber attack and who is responsible for protecting the content they produce, their personal data and their networks?

To go further with our questions to the targeted media professionals and civil society representatives, we initiated the discussion on why they think the content they produce can or cannot be attractive for someone to try to break into their or their organization's system. Why would someone try to hack their accounts or compromise the content they produce? The Research team was looking for their opinions on what makes them a potential target for hacking or surveillance, rather than just a general Internet user. The interviewed journalists and civil society representatives as well as the focus group participants were asked to elaborate more on the possible causes and risks for their online accounts and their digital identities and share their experience on where those threats come from.

According to both the IT security experts and the targeted media and NGO representatives, the most obvious thing that can make a general Internet user a good target for hacking is the number of connections/the size of the audience they have. Journalists and advocates usually enjoy big numbers of followers in social media, which makes it much easier for them to collect data, disseminate their content, exercise more efficient outreach and campaigning, and mobilize more resources for their causes. On the other hand, the big audience is what makes them vulnerable to all sorts of cyber attacks. What is surprising, is that most of the interviewed journalists and civil society representatives fully realize that their big audience and popularity can make them a target for continuous surveillance and cyber attacks from let's' say the National Security Service, however they do not even see the risks coming from data thieves or falling a victim to phishing or personal data breaches related to not so rare data leaks form big corporations.

The opinions on whether or not the targeted groups of Armenian media professionals and civil society representatives possess any piece of valuable information or content, both in terms of its commercial or legal importance and public impact, extremely varied. Some IT security experts claim that journalists and civil society representatives acting in Armenia have nothing at large to lose and the content they work on or produce does not have the commercial or any other value well worth the efforts and expenses of hacking into their systems. The main rationale here is that if the state authorities target or want to silent someone in Armenia, they can probably use less expensive methods. Similarly, even some journalists and civic activists think that they have nothing to hide, including their communication with their sources/stakeholders, and any extra security measure can attract more unwanted attention from state agencies, rather than help them to protect themselves and their information sources.

There are those among the interviewed IT security experts and media professionals/civil society representatives, who attach enough value to the content the latters produce and to how they manage their data. The advocates, who focus on sensitive issues, and journalists working on confidential and soon-to-be-published content have always experienced digital security and privacy threats. They are sure that the projects they are involved in makes them a potential target for hackers. Some even mentioned that the ideology they share or the value set they have can make them stand out from the general public, thus attracting an extra share of negative attention to their social network profiles, diverse accounts and mobile devices. This is especially true about the investigative journalists and civic activists that produce and spread the content to challenge the state and governmental agencies and corporations. Drawn from the focus group discussions, journalists and civil society groups investigating and advocating for environmental causes and/or promoting pacifist agenda and closely monitoring the developments related to army and military activities over Nagorno Karabakh conflict have quite often been threatened and attacked by the authorities and better know the value of the information security and protection of their digital identities.

While trying to come up with the list of individuals/groups that could have special interest in their personal data or in breaking into their organizations' systems, the interviewed/focus group participant journalists and advocates were in absolute consensus to put the state agencies and the National Security Service in particular at the first place. The confidence that in most cases the mastermind of recent cyber attacks to their personal accounts and their organization's websites are state agents themselves has much to do with the fact that the journalists and especially the civic activists usually have received verbal or physical threats from them at the same time, when their accounts and website contents were compromised. Secondly and surprisingly enough, they reported the cyber attack risks coming from their personal enemies and competitors, as they were sharing true stories about personal data theft by hired hackers. Another widely-believed source of digital security threats that especially Armenian media agencies have been experiencing is the group of Azerbaijani hackers breaking and defacing websites in .am-domain and personal profiles of Armenian users. Only a few interviewed journalists and civil society representatives mentioned about the global threats in digital space by just referring to phishing emails and other suspicious messages.

Despite the overwhelming amount of online evidence, information and advice as well as continuous training on cyber security related issues, the interviewed media professionals and civil society representatives reported having little knowledge and skills to deal with the emerging security threats in the Internet. In case of any IT security related questions or issues they face, the luckiest ones usually turn to their tech savvy friends or IT professional colleagues, usually the LAN administrators of the organizations they are working with. Insufficient levels of digital security related knowledge and lack of time and interest in self-education remains the main problem the targeted journalists and advocates are facing these days. On the other hand, there are only a few media agencies or NGOs that have any corporate policies or sets of rules ensuring the security of their devices, networks, and websites. Wherever the organization has strict corporate data security policies and procedures, the employees do not even try to opt out of the common rules and practices. This seems to be the most efficient way of practicing secure information exchange among the targeted journalists, civil society representatives, and their sources/stakeholders judging from the information we received in a result of the focus group discussions and in-depth interviews. Relying on cyber security awareness and security habits of individual journalists and advocates will never prove to be efficient for ensuring corporate data protection and secure information flow through organizational networks, because first of all there is a need for specialized intervention given the emerging cyber security threats all over the world. Unfortunately, not all media outlets or civil society organizations in Armenia can afford or tend to prioritize information security arrangements or related expenses and prefer to focus on their main mission of news production and advocacy at the expense of cyber-risks exposure.

Last but not least, in their turn most of the interviewed journalists and NGO representatives are not willing to devote much time and efforts for periodically updating their knowledge and skills at the expense of their main duties and day-to-day activities. The reasons they mentioned vary tremendously. Some of them think that their individual efforts will be just a drop in the ocean, since neither their colleagues, nor their contacts follow the IT security standards and procedures. The others claim that despite all efforts they might put in the protection of their personal data, they could not be absolutely protected from cyber attacks or personal data leaks. Many of the focus group participants incorrectly believed that the mere existence of privacy policies and settings indicated that the social network or the website they were using could not share their personal information without their consent. This list is not exhaustive as there is no certain type or amount of knowledge to obtain to get fully protected from all threats and risks the online environment has yet to offer to the Internet users. The main challenge these days as agreed by the majority of the interviewed IT security experts is to keep the journalists, advocates and all general users alert about the existing and emerging cyber security threats and encourage practices and user habits for safer information exchange and online environment. To sum up the practices and common problems the Project targeted group of professionals listed, the areas media agencies and civil society organizations should focus on include, but are not limited to the following:

- How to use PCs, mobile phones, and other devices as securely as possible;
- How to protect devices and sensitive information from physical threats;
- How to create secure passwords and protect online accounts;
- How to use encryption and secure communication channels;
- How to use social networks and how best to protect personal data in there;
- How to protect computers and other devices from viruses and malware and how to verify sources and unfamiliar URLs;
- How to archive and back up important information and how to recover from information loss;
- How to destroy sensitive information, when devices are lost, stolen, or confiscated;
- How not to fall victim to social engineers and phishing;
- How to get information on users rights and the existing cyber security related legislation;
- How to ensure and enforce efficient cyber security policies and practices;
- How to ensure security of organizational websites and networks.

3.6. Development of an Online Multimedia Toolkit in the framework of the Project

Besides this report's summarizing the findings of the research conducted within the framework of the "Advocating and Educating Online Human Rights" Project, the Project team has also initiated the development of an Online Multimedia Toolkit to raise awareness about the existing and emerging cyber security threats and provide solutions, strategies, knowledge, and skills to combat those threats. The Online Multimedia Toolkit is intended for the groups of professionals targeted by the Project - journalists and civil society representatives – but hopefully will serve as a universal toolkit for general users as well. During the focus group sessions and individual interviews, the journalists and civic activists were asked to elaborate on their preferences in terms of the content, the length, the concept, and format of the game. The list of topics used to wrap up the previous chapter can be as the summary of topics and issues the targeted professionals and the interviewed IT security experts were most concerned about. To develop a game concept based on the above listed cyber security related areas is highly recommended. On top of this, the focus group participants also suggested to concentrate on topics such as (1) children's rights and sharing children's personal data in the Internet, (2) the right of being forgotten, and (3) online bullying.

The possible structure of the game provoked big discussion among the focus group participants with most of them suggesting that a quiz-like game offering cyber security related information and tips. Besides the Q&A would be much attractive for them. As a more sophisticated option the hypothetical situation game format was suggested with the possibility to choose among and answer a number of situation questions referring to one or another cyber security threat. This also implies that each question will have its own weight based on its difficulty level and with each correctly answered question the player will move onto a more difficult one. Multi-level nature of the game will ensure the player's continuous interest and drive to move further.

There was no consensus in regard to the duration of the game. Some participants mentioned that they would spend up to 5-10 minutes per day on the game, while the others would be ready to spend over 1 hour especially if the game is designed for mobile devices as well. The most important preference related to the duration of the game is that the player has an opportunity to continue playing the game right where s/he stopped it previously given that they are using the same device and/or account.

IV. CONCLUSIONS AND KEY RECOMMENDATIONS

While technology and the Internet are extremely powerful and helpful tools for producing and efficiently disseminating information, they also expose groups of professionals like journalists and civil society representatives to a great deal of cyber security risks. The more journalists and advocates have begun to use digital technology, the more visible and vulnerable they become in the online environment. While the Internet has helped to decrease costs for nearly everything, a simple mistake one makes in the cyber space can still bear a relatively high price. Compromising security of just one journalist, blogger, or civic activist can mean compromising the security of everyone that individual in connected to online. As our research showed most of the media professionals and civil society representatives do not attach much value to existing cyber security risks and have very little knowledge to protect themselves and their devices, sources, and stakeholders in the Internet. They are not well aware of possible risks and threats related to algorithms that big corporations are applying to collect, generalize, and use data from each and every user, not even speaking about the censorship and control exercised by the governments. Google and Facebook already bases the advertisements they show us taking into account the content we have preciously shared or liked. Not yet fully realizing the existing cyber security threats, we will soon have to deal with emerging threats of "censorship systems that are as detailed and well-tuned to the information needs of their users, as the behavioral advertizing we encounter every day."

The problems and risks that media professionals and civil society activists face cannot be easily solved as they have deep roots in their user habits and attitudes, the overall Internet culture and specific professional practices. However, based on the information collected from the IT security experts and the targeted professionals as well as the analysis of the triangulated data, the Research team identified several areas and came up with the following recommendations for individual journalists, civic activists, Project stakeholder institutions and policy-makers.

Stakeholder institutions:

- A multi-stakeholder foundation should be established to oversee the Internet related developments in the country as well as protect the rights of the Internet users and ensure that they are treated not just as end-users, but rather citizens with basic human rights to be equally exercised in online space.
- Communities of the targeted professionals and IT security specialists should figure out new ways of cooperation, training, and information exchange to effectively combat the Internet security breaches and possible risks.
- The critical first step that institutions should be taking to address cyber security threats is to look inward and take corporate responsibility for their clients' cyber security. The managers and company owners should re-evaluate the cyber security related

risks and possible costs and need to ensure that the software running in their networks is licensed. They should rely more on open source operation systems.

- Institutions need to build a culture of security awareness and fill in the gaps in their team's cyber security knowledge and skills by setting up corporate policies and procedures to ensure secure exchange of information among the team members and partners/stakeholders. The institutions should provide their employees the necessary training and technology to strengthen their organization's human firewall and mitigate the possibility of a cyber attack.
- Institutions should develop archiving and back up strategies for the important and sensitive information their organizations possess. They should also think of possible techniques on how to recover from information loss. This especially refers to media outlets and NGOs that deal with big datasets and large-scale content.

Individuals:

- Individuals should be aware of threats related to using public WiFi and start using at least a VPN when using public WiFi.
- Individuals should use unique and complex passwords and 2-factor authentication for their accounts.
- Individuals should be careful clicking on unknown web-links. They should be extremely cautious when opening email attachments, especially from unknown sources.
- Individuals should keep their mobile phones and other portable devices with them all the time. They should have passwords on their devices and develop strategies for destroy sensitive information from their device, in cases, when their device is stolen, lost, or confiscated.
- Individuals should learn to keep their sensitive information and Internet communication private by mastering the encryption tools and techniques.
- Individuals should be aware how social networks work and should not fully rely on their privacy settings and policies.
- Individuals should never think that this list of recommendations is exhaustive and should always be alert about the existing and emerging cyber security threats and be in constant search for the most efficient techniques and tools to combat those risks.

V. ANNEXES

5.1. In-depth Interview and Focus group discussion guide

INTRODUCTION

1. Names of the Facilitator and the FG coordinator and who is doing what during the FG session.
2. The purpose of the discussion: Your opinion and your experiences are of much importance to us and we would love you to be active and open during the session.

I. GROUND RULES

1. This session will last about 2 hours.
2. This session is being video/audio taped and thanks everyone for giving your written consent to do so.
3. There are no wrong answers in what we are about to discuss; we are looking for different points of view and I am sure each of you has something to add to the discussion. So, I would encourage everyone to talk, but you don't have to answer each question.
4. Please talk one at a time and as clearly as possible, and please avoid side conversations. It is distracting to the group and I don't want to miss any of your comments.
5. Exchange points of view with each other – you don't need to address all answers to me.
6. Does anyone have any questions before we begin?
7. Last but not least, PLEASE turn off all mobile phones.

START Video/audio recording

II. BACKGROUND (5-7 minutes)

8. Please, each of you make a brief introduction of yourself and tell us:
    - Who you are;
    - What is the main professional and/or activity area you are involved in.
9. Also, can you please tell us how much of your daily work/communication is done through Internet and weather you think you are an advanced Internet user or not?

III. Online vs. Offline Human Rights: If not completely the same, where is the overlap? (15-20 minutes)

10. Pros and Cons of Network neutrality: what's your take (arguments) on "Internet development Vs. Traffic Management" from the perspective of end-users?
11. In recent years, policy debates and regulations on network neutrality have crystallized several key principles:
    - Transparency – Operators must provide comprehensive and accurate information on their network management practices and quality of service to their customers;
    - Non-discrimination – Operators should make no discrimination on traffic based on origin of sender/receiver; and type of content, type of application and/or service.
    - Access – Users should be able to have unrestricted access to any LEGAL content, service or application (with minimum quality of service guaranteed for the meaningful use) or to connect any hardware that doesn't harm the network.

    Other principles most frequently debated in international forums: Freedom of expression, access to information, and choice; Privacy and protection of personal information; Assuring minimal quality of service and security and resilience of the network; Defining rights, roles and accountability of all parties involved (providers, regulators, and users), etc.

12. In your opinion what's the situation in Armenia related to online human rights, do you feel you can freely exercise your rights through Internet channels? Can you please, elaborate a bit on why you feel this way?
    - What are the regulatory mechanisms in Armenia ensuring/limiting/interfering with your Internet freedom?
    - How often and/or how easy can your colleagues' or your online human rights be restricted? Are you aware of any recent cases of restriction of Internet freedom in Armenia?

IV. Web content you produce: Who is hunting for it? (25-30 minutes)

13. Why do you think the content you produce can or cannot be attractive for someone to try to break into your or your organization's system. Why would someone try to hack you or compromise the content you produce?
14. From a general Internet user to a potential target: things that make you unique in terms of the activity area you are involved in, a broader online audience and larger coverage you may have.
15. Who can be the individuals/groups threatening your/your organization's information systems? Have you/your organization already experienced such threats?
16. Can you please elaborate more on most common problems or specific cases you have experienced so far in relation to information security?

V. The nuts and bolts of information security: What do you/your organization do to ensure secure online environment for your day-to-day work? (20-25 minutes)

"A malicious hacker only needs to find one security hole whereas IT and security professionals and business owners must find and block them all!"[1]

17. Individual level - How would you assess your own knowledge and skills on information security? What are the specific measures you take to ensure secure exchange of information through the Web? Personal accounts, passwords (2-factor authentication), verification/assessment of sources, protection of mobile devices, email encryption programs, etc.?
18. Institutional level – What is your organization's policy (if any) related to IT security and smooth flow of information through institutional network(s)? Licensed software/program packages; advocating for open source (OS X, Linux) operation systems, etc.?
19. Mobile Operators and Policy level – Are there any policies and/or regulations (that you are aware of) to protect you/your organization from breaches into your information systems.

VI. Elementary and advanced skills for IT security: Is there a room for improvement? (15-20 minutes)

20. How well-informed do you consider yourself in terms of the IT hygiene and security rules? Do you always prioritize it? Is it easy to find the right balance between your

[1] https://archive.org/details/Wiley.Hacking.5th.Edition.Jan.2016.ISBN.1119154685.Profescience.blogspot.com

main professional activity and your responsibility to secure yourself and your social networks from potential information security threats? How "paranoiac" one should be in matters related to the health of their devices and the prevention of security breaches.

21. What are the main sources you would consider to get some useful tips from? What are the sources you would never trust and why do you think so? How many of you would use the online resources available on this matter? If not, why?

VII. Game development (5-10 minutes)

22. The MIC is planning to develop a game for educating and advocating online human rights and particularly equipping journalists and civil society representatives with tools on how best to address information threats and vulnerabilities individuals and organizations have been experiencing in the rapidly changing Internet environment. What do you think of this initiative and what are the main features you would like to see in the newly developed game?

VIII. CLOSING REMARKS (5 minutes)

Many thanks for your time and active involvement. This has been a valuable session of brainstorming. Please, let me know, if you feel like adding anything relevant to what we have already discussed….Thank you again!

5.2. In-depth Interview and Focus Group Discussions Schedule

Date/ Time	Name	Organization/Position
26/04/2017; 1:00pm	Mikayel GHAZARYAN	Teamable Software/Software architect
26/04/2017; 2:30pm	Edgar MARUKYAN	RenderForest/CTO
27/04/2017; 11:00am	Ruben MURADYAN	UCOM/IT Auditor; PanArmenian Media Group/Board Member
27/04/2017; 1:30pm	Norayr CHILINGARYAN	Data Architect
27/04/2017; 4:30pm	Nerine DANEGHYAN	Media Max
27/04/2017; 5:30pm	Davit ALAVERDYAN	Media Max
29/04/2017; 12:00pm	Grigory SAGHYAN	ISOC Armenia/Vice President
29/04/2017; 2:30pm	Hasmik ALAVERDYAN	PanArmenian Media Group
4/05/2017; 12:00pm	Gevorg HAYRAPETYAN	RoA Ministry of Justice, Agency for Protection of Personal Data/ Head of the Department of Implementation of Administrative Proceedings
4/05/2017; 2:00pm	Kristine AGHALARYAN	Hetq
12/05/2017; 4:00pm	Vahagn ANTONYAN	Peace Dialogue/Vanadzor
13/05/2017; 12:00pm	Anjela STEPANYAN	Alt TV/Armavir
13/05/2017; 2:00pm	Anahit BAGHDASARYAN	Media Club/Goris, Hetq
15/05/2017; 2:00pm	Armine SADIKYAN	Helsinki Citizens' Assembly/Vanadzor

FG: Date/ Time	Name	Organization
FG1: 3/05/2017; 12:00pm	Anna SHAHNAZARYAN	Civic activist
	Shahen HARUTYUNYAN	Civic activist
	Arpine ZARGARYAN	Civic activist
	Helena MELKONYAN	Civic activist
	Vaghinak SHUSHANYAN	Civic activist
	Piruza PETROSYAN	Civic activist
	Zaruhi HOVHANNISSYAN	Civic activist
FG2: 3/05/2017; 4:00pm	Gohar VOSKANYAN	Helsinki Committee of Armenia
	Mariam SARGSYAN	Civil Society Institute
	Anna ZHAMKOCHYAN	Socioscope
	Mamikon HOVSEPYAN	PINK Armenia
	Eduard DANIELYAN	Helsinki Association
	Arman GHARIBYAN	The Rule of Law NGO
	Lilit HOVHANNISSYAN	Committee to Protect Freedom of Speech NGO
FG3: 4/05/2017; 6:00pm	Christina SLOYAN	CivilNet
	Gayane ASRYAN	Media.am
	Hovhannes MOVSISYAN	Radio Liberty
	Gevorg TOSUNYAN	Iravaban.net
	Knarik KHUDOYAN	Epress.am
	Karine ASATRYAN	A1+ TV online