FREEDOM OF EXPRESSION AND THE INTERMEDIARY LIABILITY IN PALESTINE

Huda Alwahidi[1] and Rashid Jayousi[2]
[1]*Ministry of Justice, Palestine, Ramallah*
[2]*Al-QudsUniversity, Palestine, Jerusalem*

ABSTRACT

Internet is an important tool for developing and exercising human rights these include the promotion, protection and enjoyment of human rights on the Internet and the right to freedom of expression (FoE). FoE is essential in any society; it is the cornerstone of all human rights and social needs. The paper objective is to identify to what extent the Right of FoE on the Internet is respected and practiced in Palestine. The aim of protecting FoE is to create an enabling environment for innovation, which balances the needs of governments and other stakeholders around the world based on international human rights instruments and other international legal frameworks. In this paper we explore the reality and the perceptions of FoE on the Internet in Palestine FoE. In this research we studied the Palestinian legal framework of FoE on the Internet in comparison with the International conventions that Palestine State acceded to, the practices of FoE on the Internet in Palestine and the access to the Internet and its infringements in Palestine. This research adopted an exploratory methodology, two methods used to achieve the research objective, first method; a qualitative approach is used in which national and international laws, formal reports and interviewee's opinion were gathered. The sample was three ISPs, a group of Palestinian legal advisory and Palestinian key persons. The second method was a quantitative method in which online data questionnaire was used to collect responses from different subjects. The questionnaire sample was postgraduate from Al-Quds University; the retrieved forms were 169 form. As a result of the research, it was concluded that that theoretically the Palestinian legal framework guarantees FoE though in practice there is a gap between realities and prospective, moreover Palestinian does not have sufficient legal awareness.

KEYWORDS

Human Rights, Internet Access, Net Neutrality, Internet Monitoring, Intermediary Liability, Palestine

1. INTRODUCTION

Freedom of Expression (FoE) is the corner stone of Human Rights (UNESCO.2011); it is the enjoyment of the full freedom of human being to speak the truth, and provide advice in all matters of religion and the world to achieve the benefit of Muslims, protecting the interests of the individual, society and public order. Everyone has the right to freedom of opinion and expression and the right to seek, to receive and impart information and ideas, through any media and regardless of frontiers. This implies free circulation of ideas, pluralism of the sources of information and the media, press freedom, and availability of the tools to access information and share knowledge. As a result FoE on the Internet must be protected by the rule of law rather than through self-regulation and codes of conduct. Nations could not practice their freedoms unless the basic environment guarantees that.

There must be no prior censorship, arbitrary control of, or constraints on, participants in the communication process or on the content, transmission and dissemination of information. Pluralism of the sources of information and the media must be safeguarded and promoted. Communications content that include activities, interactions, and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking, information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Each of these type of information which might be analyzed separately or collectively,

reveal a person's identity, behavior, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event. As a result, all Protected Information should be given the highest protection in law.

In 2012 Palestine became a Non-Member Observer State in the United Nations, this allows Palestine to join and accede to international agreements and conventions. These conventions lay many obligations for Palestine. It is mandatory to abide by international standards and norms.

This paper reflects the authors' research results of Freedom of Expression on the Internet in Palestine, measure the respondent's perceptions of rights and freedoms in the use of the Internet, their perceptions about online surveillance and censorship and their perceptions of Internet content blocking and filtering.

We used an exploratory research methodology to find satisfactory answers to the above questions; therefore we implemented two methods: the qualitative method for gathering international and local laws and the human rights reports, and the quantitative method used for gathering information through an online questionnaire to measure the respondent's perceptions on FoE on the Internet in Palestine. We gathered information from two main sources; the first source includes data and information in international covenants and conventions, policies, principles and legislations, reports from international institutes, studies, conferences paper and workshops. For the second source, we used interviews and questionnaire to collect such information. The interviews were conducted with specialized people in legal framework in Palestine, with local internet service and with general public institutions. The Questionnaire was conducted with graduate students from Al-Quds University.

2. CONTROLLING ACCESS TO ONLINE

"Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers." (ITU.2003). FoE on the Internet depends on several factors: the Internet access, Internet speed, Internet service price, Internet filtering, censorship and the granted rights of Internet user (Mada, 2014). According to the APC-La Rue Framework for Assessing FoE and Related Rights on the Internet, the framework checklist of indicators that are intended to provide guidance in monitoring and reporting on internet related human rights violations summarize into three steps, the general protection of FoE, the restrictions on online content and the Internet access (APC, 2013).

2.1 Internet Access

Access to the Internet is crucial for the enjoyment of the right to FoE and other rights in the digital age, it has been observed that without the means to connect or without an affordable connection, the right to FoE and the freedom of the media become meaningless in the online world.

In 2002 the UN Committee on Economic, Social and Cultural Rights (CESCR) issued its General Comment No. 15 on the human right to water, defining access to drinking water and sanitation as a human right. Access to water would be considered as implicitly contained in the International Covenant on Economic, Social and Cultural Rights (ICESCR) within the right to an adequate standard of living (Article 11), and the right to the enjoyment of the highest attainable standard of physical and mental health (Article 12). This would open the gates to the recognition of several different services that could be considered within the "adequate standard of living", including access to the internet and postal delivery services.

According to the Palestinian ministry of telecommunications Palestine has 320 thousands Asymmetric digital subscriber line (ADSL) (Minister Deputy of Ministry of Information and Telecommunication, Personal interview, 2017). And 96% of the respondents of this research acknowledge the necessity of Internet in their profession or education.

A close look to the Internet access in Palestine and according to the household survey on information and communications technology implemented by the Palestinian Central Bureau of Statistics (PCBS) in 2014, we see that (48.3%) of the Palestinian families access the Internet from home while (25.3%) access to the Internet elsewhere. The reason why (19.3%) of the Palestinian families don't access the Internet from home due to the lack of confidence, while (11.6%) in cause of privacy or security concerns and (13.2%) regarding cultural reasons (e.g. exposure to harmful content). Moreover, (3.4%) said that the Internet service is not available in the area they live and even if the Internet service is available (4.5%) said that it will not correspond to household needs (e.g. quality, speed) (PCBS, 2014).

The research found that 70.5% of the respondents express their views online to reach the widest possible audience, 26% because of fear of direct confrontation, 37% express their views through online to ensure personal protection for themselves and their family members, and the high percentage of 70.1% who disagreed to use aliases when expressing their views and perspectives through online publishing and interaction assured that Palestinian people have a powerful characteristic to express themselves in any environment.

There is difficulty in access to all areas in Palestine, especially some of the villages, due to the blockade and the separation wall and area C which increases the costs for Internet connection which shad on the overall cost of Internet Service, and the biggest problem facing Internet access is related to Israeli occupation, which prohibit Palestinian from the enjoyment of third generation (G3) and the fourth generation (G4) Internet service on their mobile phones (Minister Deputy of Ministry of Information and Telecommunication, Personal interview, 2017). This prohibit limits user to participate immediately and express their views from anywhere. Also the rise in prices on Internet services limits the ability of citizens of low income to use it, we conclude that they will not be able to communicate rapidly with others and express their opinion (Minister Deputy of Ministry of Information and Telecommunication, Personal interview, 2017).

Applying La Rue checklist we find that Palestine has national action plan for Internet access and Palestine considered the third country in the region for the infrastructure for the ADSL connection. Moreover Palestinian government supports the schools Internet connectivity project, this project connects all public Palestinian schools to Internet and gives the students the opportunity to seek information they need (Minister Deputy of Ministry of Information and Telecommunication, Personal interview, 2017).

2.2 Net Neutrality

An important component of the right of access to the internet is the principle of 'network neutrality' or 'net neutrality.' This protects the right to access internet content, applications, services and hardware according to individual choice. It requires that ISPs and governments treat all traffic and data on the internet equally, without discrimination, regardless of the nature of the user, type of data, content and platform. ISPs and governments are also prohibited from prioritizing the transmission of data, from blocking content, or from slowing down access to certain applications or services. (ARTICLE19, 2013)

Net neutrality is not yet anchored as a legal norm within international law. However, the 2011 Joint Declaration on FoE and the internet of the four Reporters recommended that: There should be no discrimination in the treatment of internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application.

Internet intermediaries have to be transparent about any traffic or information management practices they employ, and relevant information and put in place special measures to ensure equitable access to the Internet for the disabled and for disadvantaged persons.

Governments typically conduct or order shutdowns, often with the assistance of private actors that operate networks or facilitate network traffic. Shutdowns may affect towns or regions within a country, an entire country or even multiple countries and may last for periods ranging from hours to months (Kaye, D. 2016) paragraph 10.

Shutting down the Internet can never be justified, including on public order or national security grounds. Other measures which limit access to the Internet, such as imposing registration or other requirements on service providers, are not legitimate unless they conform to the test for restrictions on FoE under international law. (La Rue, et al, 2010)

The right to FoE imposes an obligation on States to promote universal access to the internet all times including during times of political unrest (HRC, 2014A) paragraph 3 (La Rue, et al, 2010) and to develop a concrete and effective policy, to make the internet widely available, accessible and affordable to all segments of population." that foster greater access to the Internet, including for the poor and in 'last mile' rural areas. (La Rue, et al, 2010)(La Rue, 2011) Paragraph79.

2.3 Internet Monitoring

According to Privacy International organization Internet monitoring is capturing data as it travels across the internet towards its intended destination. The infrastructure that supports the Internet involves physical infrastructure and electronic systems to connect the world (Privacy International, 2016). It is recorded that (60.1%) of Palestinian families monitor their children Internet program (5-17 years) use. In order to protect the children on the Internet (22.5%) install Internet monitoring (PCBS, 2014).

Some States have the capability to track and record Internet and telephone communications on a national scale. By placing taps on the fiber optic cables, Such as the Egyptian and Libyan Governments in the lead-up to the Arab Spring (La Rue, 2013) paragraph 38. States have the capacity physically to monitor activities on social networking sites, blogs and media outlets to map connections and relationships, opinions and associations, and even locations. States can also apply highly sophisticated data mining technologies to publicly available information or to communications data provided by third party service providers.

Intermediaries have access to information created by users such as posts, tweets, comments, blogs as well as a range of information directly related to users such as registration details, private messages, search and browsing history, transaction details, location. For this reason, intermediaries are the key of facilitating and protecting the rights to free expression and privacy. They also serve as avenues through which governments can monitor, regulate and control individuals' online activities and access to information. The role that intermediaries play in protecting or restricting FoE is further complicated by the global nature of many companies. Multinational companies, as well as internet services with users in multiple jurisdictions, can be subject to a global patchwork of legal and regulatory regimes. It is notable that 71.2% of the respondents believe that Internet content is monitored, 86.5% believe that it is monitored by Israeli occupation and 63.2 % by ISPs.

2.4 Internet Censorship and Surveillance

"No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks"Article12 (UDHR,1948).

Government surveillance relies on access to communications and associated data belonging to users of privately owned networks. While such access frequently requires the assistance of private actors, it may also be obtained without their knowledge or involvement (Privacy International, 2017).

We can see that of ICCPR refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communication, both online and offline article 17 paragraph 2: "Everyone has the right to the protection of the law against such interference or attacks."

Communications surveillance was required to be authorized by the judiciary; increasingly this requirement is being weakened or removed (La Rue, 2013) paragraph 54. Even when judicial authorization is required by law, often it is de facto an arbitrary approval of law enforcement requests (La Rue, 2013) paragraph 56.

The Palestinian Intelligence service agency aim is to protect the Palestinian national security, their work starts according to judicial decision not prior to that and it is legitimated by law vice chairman of the Palestinian Intelligent agency, Personal interview, 2017).

The UN High Commissioner for Human Rights has called for reform of surveillance laws, and referred to the recommendations by global civil society for the application of the 'necessary and proportionate' principles with strong accountability, transparency, and remedy.

As gatekeepers of vast information networks, providers face significant government pressure to comply with censorship and surveillance activities. To operate a network in a country, they are required to invest substantial physical and business infrastructure, including network equipment and personnel. They are typically subject to local law and other licensing requirements set out in agreements with the State. In addition to legal pressure, providers have also faced extralegal intimidation, such as threats to the safety of their employees and infrastructure in the event of non-compliance (Kaye,D. 2017) paragraph 31.

In response to the increased data flows across borders and the fact the majority of communications are stored with foreign third party service providers, a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions (La Rue, 2013) paragraph 64.

In this context the research shows that 52.7% of the respondents do not feel comfortable talking about the political topic while 80.7% feel comfortable talking about cultural and literary topics, 75.1% feel comfortable talking about social topics while 70.9% feel comfortable talking about religious topics. In conclusion 53% of them feel comfortable expressing your opinion online.

This research also shows that 63% of the respondents agree that censorship restricts online FoE; respondents don't think that filtering and blocking restrict online FoE on the contrary 80.1% believe on the need of filtering, this could be justified for filtering and blocking pornographic websites where the respondents mostly agree on filtering and blocking s the pornographic websites with 79.6%, followed by the disseminate incitement and racism of various political websites with 73.4%.

Also 75.1% agree that online censorship protects his/her family from the risk of disintegration and 69.8% agree that online censorship protects the customs and traditions of society and these are major reason of why 74.5% agree on the need to online censorship, the perceptions of that censorship makes them committed to social life or focused on their studies and work close to each other with medium percentages.

2.5 Internet Filtering, Blocking

In many countries, Internet filtering is conducted under the guise of maintaining social harmony or eradicating hate speech, but is in fact used to eradicate dissent, criticism or activism (La Rue, 2013) paragraph 44. Governments around the world block access to online content to shield children from obscene content, to prevent access to copyright infringing material or confusingly named domains, or to protect national security (EFF, 2017). Filtering can be applied through Internet Service Providers, Gateways to the Internet backbone, Institutions, Individual computers and Law enforcement (Dutton, et al, 2011).

Palestinian Internet service providers offer filtering service to their subscribers with low cost to help families protecting their children, ISP's do not apply any other kind of filtering on their customers (Palestinian ISPs, Personal interview, 2017), and according to the household survey on information and communications technology implemented by the Palestinian Central Bureau of Statistics (PCBS) in 2014, (53.9%) of Palestinian families install Internet filter software on the computer in order to protect their children (5-17 years) on the Internet (PCBS, 2014).

The burden of such policing is transferred to private intermediaries, such as search engines and social network platforms, through laws that widen liability for proscribed content from the original speaker to all intermediaries (La Rue, 2013) paragraph 46.

Search engines involves three potential parties regarding FoE; the individual internet users seeking information; the creators and operators of websites that are or potentially may be indexed by search engines and the search engines.

Government requests data about people who use Facebook. In many of these cases, they request basic subscriber information, such as name and length of service. Or request IP address, logs or account content.

They also ask Facebook to restrict access to content that violates their laws. (Facebook, 2017)

It is notable that (75%) of Palestinian Social Media users use it on purpose of acquaintance, the purpose of debate varies of (25.8%) on political topics, (34.2 %) dialogue on religious topics, (3.33 %) cultural and literary topics and (19.8%) on topics of heritage (PCBS, 2014).

Israel's military intelligence is monitoring Palestinian social media accounts. As a result, has arrested around 800 Palestinians (Haaretz, 2017) because of their posts on social media, particularly on Facebook, Palestinians' preferred platform. Israel program monitors tens of thousands of young Palestinians' Facebook accounts, looking for words such as shaheed (martyr), Zionist state, Al-Quds (Jerusalem), or Al Aqsa. It also

searches for accounts that post photos of Palestinians recently killed or jailed by Israel. The system thus identifies "suspects" based on a prediction of violence, rather than any actual attack – or even a plan to commit an attack. Any Facebook profile marked suspicious by the system is a potential target for arrest, and Israel's main accusation of those detained is "incitement to violence." According to Facebook government requests report of 2016, Israel requests 710 user data and 1623 restriction for content while Palestine requests one user data (Facebook, 2017).

By law enforcement and intelligence agencies through a variety of methods could apply intercepting communication transmission via a telecommunications system and divulging information to a third party on account of national security, the prevention or detention of serious crime, or the economic safeguarding of a state. Logging, recording, retaining and giving access to information about visited websites, emails sent and received, or applications used vice chairman of the Palestinian Intelligent agency, Personal interview, 2017).

Internet in Palestine was distinguished by its openness and non-use of filtering and blocking of websites by authorities (Mada, 2014), Beginning in early June, Palestinian internet providers began blocking approximately sixteen websites, the decision made by the Attorney General. Blocking websites on the internet may impinge on the right to FoE online (Alhaq, 2017).

2.6 Intermediary Liability

The importance of ISPs and their key role is in enabling expression. At the same time, ISPs can be a single point of failure for expression online particularly when content or entire services are filtered (blocked from being accessed by the user) or networks are shut down locally or nationally.
Because ISPs must be physically present in a country to provide service and operate, the extent to which they facilitate or restrict FoE is most directly affected by laws, regulations, and government actions compared to the other intermediaries studied (MacKinnon, et al, 2014).

According to the Palestinian Cybercrime law by Decree of 2018 article 31; ISP's liability determined on supplying the data or information requested on special case, gathering and taping data or information, blocking or filtering content upon court decision, but Protected Information should be given the highest protection in law.

FoE can be restricted via ISPs, search engines and social media, through three primary levels:

i. The network-level where telecommunications access providers and Internet service providers can restrict FoE by filtering, service shutdown and non-neutral.
ii. The platform level where intermediaries that operate at the platform level such as search engines and social networks can act to remove content completely, block it from view to particular categories of users (usually based on geography), or deactivate user accounts.
iii. Both network and platform levels where Internet users who believe that their communications and online behavior is being monitored or exposed in a manner that violates their privacy rights are less likely to express themselves freely while using the services of internet intermediaries.

According to the principles on business and human rights, the responsibility of business enterprises to respect human rights refers to internationally recognized human rights understood, at a minimum, as those expressed in the International Bill of Human Rights and the principles concerning fundamental rights set out in the International Labor Organization's Declaration on Fundamental Principles and Rights at Work (Ruggie, 2011) princple12.

Companies should assume an active and engaged role in developing expression and privacy enhancing measures. For example, digital security measures that detect and prevent distributed denial-of-service attacks and hacking should be implemented in a manner that targets malicious traffic without compromising legitimate interactions among individuals, organizations and communities. Configuring network equipment's to minimize unnecessary information collection about users (Kaye, D. 2017) paragraph 60. Companies that deal directly with governments should push for human rights safeguards in operating licenses and sales contracts, such as assurances that network equipment will not be accessed or modified without the company's knowledge this can be for the purpose of facilitating human rights abuses (Kaye, D. 2017) paragraph 61.

According to Manila principles the roles and responsibilities of the intermediary liability are (La Rue, et al, 2011) (Manila principles, 2015):

i. They should not be liable for content generated by others.
ii. They shouldn't be required to monitor user-generated content and shouldn't be subject to extrajudicial content takedown rules which fail to provide sufficient protection for FoE.
iii. Intermediary should only be compelled to release user data when ordered by judicial authorities certifying necessity and proportionality to achieve a legitimate objective (Kaye, D. 2017) paragraph 19.

3. CONCLUSION

Everyone has the right to freedom of opinion and expression and the right to seek, to receive and impart information and ideas, through any media and regardless of frontiers.

This implies free circulation of ideas, pluralism of the sources of information and the media, press freedom, and availability of the tools to access information and share knowledge. FoE on the Internet must be protected by the rule of law rather than through self-regulation and codes of conduct. There must be no prior censorship, arbitrary control of, or constraints on, participants in the communication process or on the content, transmission and dissemination of information. Pluralism of the sources of information and the media must be safeguarded and promoted.

Communications content that include activities, interactions, and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking, information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Each of these type of information which might be analyzed separately or collectively, reveal a person's identity, behavior, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event. Any Communication Surveillance is an interference with human rights and so international human rights law applies.

As a result, Internet intermediaries should be transparent about any traffic or information management practices they employ, and relevant information and put in place special measures to ensure equitable access to the Internet for the disabled and for disadvantaged persons. Moreover they should assume an active and engaged role in developing expression and privacy enhancing measures.

REFERENCES

Alhaq, 2017. Blocking of Websites Critical of Palestinian Authority Violates International and National Laws (http://www.alhaq.org/advocacy/topics/palestinian-violations/1126-blocking-of-websites-critical-of-palestinian-authority-violates-international-and-domestic-laws).

APC, 2013.the APC-La Rue Framework for Assessing Freedom of Expression and Related Rights on the Internet, (https://www.apc.org/en/pubs/internet-freedom-index-draft-checklist)

ARTICLE19, 2013.Freedom of expression and ICTs: Overview of international standards, https://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf

Dutton,W, et al, 2011. FREEDOM OF CONNECTION FREEDOM OF EXPRESSION

EFF, 2017.free-speech, Electronic Frontier Foundation (https://www.eff.org/issues/free-speech)

Facebook, 2017. Publishing Information about Government Requests to Facebook (https://govtrequests.facebook.com/about/)

Haaretz, 2017. Arrest of Palestinians for Potential Terror Attacks Brings New Meaning to 'Minority Report' (https://www.haaretz.com/opinion/.premium-1.785470)

HRC, 2014A. Resolution, (A/HRC/RES/26/13).United Nations. Geneva.

ITU, 2003. Shaping Information Societies for Human Needs, Civil Society Declaration to the World Summit on the Information Society WSIS Civil Society Plenary Geneva, (https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf)

Kaye, D, 2016. Special Rapporteur Report on the promotion and protection of the right to freedom of opinion and expression (Annual Report, A/HRC/32/13).United Nations. Geneva.

Kaye, D, 2017. Special Rapporteur Report on the promotion and protection of the right to freedom of opinion and expression (Annual Report, A/HRC/35/22).United Nations. Geneva.

La Rue, F, et al, 2010. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Tenth anniversary joint declaration: Ten key challenges to freedom of expression in the next decade (A/HRC/14/23/Add.2).United Nations. Geneva. (https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/125/34/PDF/G1012534.pdf?OpenElement)

La Rue, F, et al, 2011. Joint Declaration on Freedom of Expression and the Internet, (https://www.osce.org/fom/99558?download=true)

La Rue, F, 2011. Special Rapporteur Report on the promotion and protection of the right to freedom of opinion and expression (Annual Report, A/HRC/17/27).United Nations. Geneva.

La Rue, F, 2013. Special Rapporteur Report on the promotion and protection of the right to freedom of opinion and expression (Annual Report, A/HRC/23/40).United Nations. Geneva.

MacKinnon, et al, 2014. FOSTERING FREEDOM ONLINE -The Role of Internet Intermediaries (http://unesdoc.unesco.org/images/0023/002311/231162e.pdf)

Mada, 2014. Internet and freedom of expression in Palestine. Palestinian Center for Development and Media Freedoms(MADA)

Manila Principles, 2015. Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation, https://www.manilaprinciples.org/

Necessary and proportionate, 2014. International Principles on the application of Human Rights to Communications Surveillance (http://necessaryandproportionate.org/principles)

OpenNet . About filtering (https://opennet.net/about-filtering)

PCBS, 2014. household survey on information and communications technology implemented by the Palestinian Central Bureau of Statistics (http://www.pcbs.gov.ps/Portals/_pcbs/PressRelease/CommTec06e.pdf).

Privacy International, 2016. The Global Surveillance Industry (https://privacyinternational.org/sites/default/files/global_surveillance.pdf, 1.5.2017)

Ruggie, J, 2011. Special Representative of the Secretary-General Report on the issue of human rights and transnational corporations and other business enterprises (A/HRC/17/31). United Nations. Geneva.

UDHR, 1948. The Universal Declaration of Human Rights, 1948 (http://www.un.org/en/universal-declaration-human-rights/ 27.10.2015)

UNESCO, 2011. Freedom of Connection Freedom of Expression the Changing Legal and Regulatory (http://unesdoc.unesco.org/images/0019/001915/191594e.pdf, 29.11.2016)