ARTICLE 19

Pakistan: Telecommunications (Re-organization) Act

January 2012

Legal analysis

Executive Summary

In January 2012, ARTICLE 19 has analysed the provisions of the Pakistan Telecommunications (Re-organisation) Act, 1996 (the Act) to assess their compatibility with international standards relating to the rights to freedom of expression and information and privacy. ARTICLE 19 finds the Act has many provisions which are incompatible with Pakistan's obligations under international law and violate citizens' rights of freedom of expression, access to information and protection of privacy.

As a general matter, the Act gives broad, largely unrestricted powers to the Government of Pakistan to issue policy statements and regulations in the name of protecting national security. These provisions provide few limitations on the ability of the government to issue directives and orders in violation of freedom of expression and privacy rights.

In addition, the Act criminalises vague and broad offenses, banning the dissemination of "false" or fabricated" information, as well as indecent materials and causing "mischief."

Furthermore, the Act allows for the shutdown of communications both individually with a vague warning, and in broader cases, based on a decree by the government of potentially the entire telecommunications networks.

Finally, there are significant problems with the broad powers of surveillance given under the Act. It allows for the interception of communications with little or no regulation or oversight. It also places restrictions on the use of encryption by users to prevent unlawful interception of their communications. These create a significant chilling effect on telecommunications users' ability to seek and receive information.

These concerns are not theoretical. Over the past several years, the Act has been used by the Government to suppress freedom of speech in the country. It has been cited by the Government as the legal basis for numerous violations of freedom of expression, including the indiscriminate and unlawful blocking of web pages, filtering of communications systems based on keywords, the stopping of internet services using encryption and the ordering of mass surveillance of communications systems. Its revision and reform is therefore more urgent than ever.

Key recommendations:

- Section 34(d) of the Act - creating criminal penalties for dissemination of information which can be considered false, indecent or obscene - should be eliminated.
- Section 34(h) of the Act on mischief should be eliminated.
- Section 54(2) of the Act - authorising the shutdown of communications in an emergency - should be removed.
- Section 54(3) of the Act - authorizing the interception of communications - should be removed and replaced with a detailed provision in the criminal procedural code setting

out the limited circumstances in which interception can be approved by an independent judge.

- Broad range of provisions restricting freedom of expression and freedom of association to protect national security and public order should be amended to comply with international standards.

- Provisions which restrict the use of encryption by users, and regulations and decrees which restrict its provision by providers, should be eliminated.

Table of Contents

About the Article 19 Law Programme

The ARTICLE 19 Law Programme advocates for the development of progressive standards on freedom of expression and access to information at the international level, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the Law Programme publishes a number of legal analyses each year, comments on legislative proposals, as well as existing laws that affect the right to freedom of expression, and develops policy papers and other documents. This work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All materials developed by the Law Programme are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this policy brief further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org.

.

Introduction

In this analysis, ARTICLE 19 sets out its concerns about the Telecommunications (Re-organization) Act, 1996 as amended (the Act)[1] from the perspective of international standards on the right to freedom of expression and information and the right to privacy. ARTICLE 19 finds the Act has many provisions which are incompatible with Pakistan's obligations under international law and violate citizens' rights of freedom of expression, access to information and protection of privacy.

In the past several years, the Government of Pakistan has increasingly used the Act to justify a series of decrees that have been expressly in violation of freedom of expression and other human rights. Actions taken by the Pakistani government have included banning major international web sites containing millions of pages of information, such as YouTube and Facebook, requiring all mobile users to register or risk having their phones blocked, increasing surveillance of online communications and banning encryption found in Blackberry systems.
The source of these problems is the Act itself, which does not adequately respect human rights, in violation of international law as signed and ratified by the Government of Pakistan. The Act gives broad powers to the Government in the name of national security and regulatory enforcement. The powers themselves are open-ended and provide no adequate guidelines and boundaries.

In addition, the Act contains a number of specific, highly problematic sections creating criminal offenses for broad but undefined areas, authorising the interception of communications with no practical limits and limiting the ability of ICT users to protect their private communications and online activities.

ARTICLE 19 has previously raised concerns about the misuse of the Act to stifle freedom of expression in Pakistan.[2] For example, in September 2011, we criticized the Pakistan Telecommunications Authority (PTA) for serving legal directives to all internet service providers in the country requiring that they implement an earlier regulation banning in the name of anti-terrorism all internet encryption. In response to the measures adopted by the PTA, ARTICLE 19 pointed out that related provisions in the Act of 1996 violate international legal standards on the right to freedom of expression and the right to privacy, and call on the Government to amend the Act urgently.

This analysis is intended to assist the Government of Pakistan in the reform process and also to support local stakeholders in their campaign for protection freedom of expression in the country.

---

[1] Pakistan Telecommunication (Re-organization) Act, 1996 as amended; available at http://www.pta.gov.pk/media/telecom_act_170510.pdf.

[2] ARTICLE 19, Pakistan: Ban on internet encryption a violation of freedom of expression; available at http://www.article19.org/resources.php/resource/2719/en/index.php?lang=en.

International Freedom of Expression Standards

The right to freedom of expression is a fundamental human right. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy, particularly in countries transitioning to democracy. Freedom of expression is a necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights.

The Telecommunications Act engages a number of international freedom of expression standards that form the basis of the legal analysis in the following section. This section identifies those standards that are most relevant to the protection of freedom of expression and, in particular, their relationship to the regulations' relation to telecommunications, including criminal penalties.

Universal Declaration of Human Rights

Article 19 of the Universal Declaration of Human Rights (UDHR)[3] guarantees the right to freedom of expression in the following terms:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.

The UDHR, as a UN General Assembly Resolution, is not directly binding on states. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948.[4]

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the UDHR. The ICCPR binds its 167 member states to respect its provisions and implement its framework at the national level.[5] Pakistan acceded to the ICCPR only in 2010, and as a state party must ensure that any attempts to criminalise actions to seek, receive or impart information are compliant with Article 19 of the ICCPR.

Article 19 ICCPR guarantees the right to freedom of expression in its first two paragraphs:

1. Everyone shall have the right to freedom of opinion.

[3] UN General Assembly Resolution 217A(III), adopted 10 December 1948.

[4] See, e.g., De Schutter, International Human Rights Law, Cambridge University Press, 2010.

[5] Article 2 ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).

> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

The United Nations Human Rights Committee (HR Committee), as the monitoring body for the ICCPR, issued General Comment No. 34 in relation to Article 19 on 21 June 2011.[6] The General Comment constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 of the ICCPR and provides a progressive and detailed elucidation of international law related to freedom of expression and access to information.[7] It is instructive on a number of freedom of expression concerns raised by the Act.

The Comment notes that Article 19:

> requires States parties to guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers. This right includes the expression and receipt of communications of every form of idea and opinion capable of transmission to others, subject to the provisions in article 19, paragraph 3, and article 20. It includes political discourse, commentary on one's own and on public affairs canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse. It may also include commercial advertising. The scope of paragraph 2 embraces even expression that may be regarded as deeply offensive, although such expression may be restricted in accordance with the provisions of article 19, paragraph 3 and article 20.

While the right to freedom of expression is fundamental, it is not guaranteed in absolute terms. Article 19(3) of the ICCPR permits limitations on the right that are necessary and proportionate to protect the rights or reputations of others, for the protection of national security or public order, or public health and morals. Restrictions on the right to freedom of expression must be strictly and narrowly tailored to achieve one of these objectives and may not put in jeopardy the right itself. Determining whether a restriction is narrowly tailored is often articulated as a three-part test, requiring that restrictions are prescribed by law, pursue a legitimate aim and conform to the strict tests of necessity and proportionality.[8]

Article 19(3) of the ICCPR requires that restrictions on the right to freedom of expression must be prescribed by law. This requires a normative assessment; to be characterised as a law a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[9] Ambiguous or overly-broad restrictions on freedom of expression fail to elucidate the exact scope of their application are therefore impermissible under Article 19(3).

---

[6] UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 21 June 2011.

[7] ARTICLE 19 statement on HR Committee Comment No. 34; available at http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression.

[8] *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[9] *Leonardus J.M. de Groot v. The Netherlands*, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).

Interferences with the right to freedom of expression must pursue a legitimate protective aim as exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR. Legitimate aims are those that protect the human rights of others, protect national security or public order or protect public health and morals. General Comment No. 34 notes that extreme care must be taken in crafting and applying laws that purport to restrict expression to protect national security. Whether characterised as treason laws, official secrets laws or sedition laws they must conform to the strict requirements of Article 19(3). General Comment No. 34 also provides guidance on laws that restrict expression with the purported purpose of protecting morals. Such purposes must be based on principles not deriving exclusively from a single tradition but must be understood in the light of the universality of human rights and the principle of non-discrimination.[10] It would therefore be incompatible with the ICCPR, for example, to privilege one particular religious view or historical perspective by law.

States party to the ICCPR are obliged to ensure that legitimate restrictions on the right to freedom of expression are necessary and proportionate. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.

[10] Paragraph 32, HR Committee General Comment 34.

Analysis of the Telecommunications Act

The Telecommunications Act contains a number of provisions which affect the right to freedom of expression and information, as well as the right to privacy. While all countries have some form of telecommunications law, which sets out the conditions of and a regulatory system for telecommunications, the Telecommunications Act provisions violate international laws on human rights. This analysis identifies aspects of these rights thematically, and organises the Analysis according to how these themes are engaged. The structure of the analysis does not, therefore, reflect the structure of the legislation.

Criminal Penalties: Restrictions on Speech

Article 31 of the Act contains a number of broadly-drafted criminal prohibitions of categories of speech. Section 31(d) states that it is a criminal offense when a person:

> (d) unauthorisedly transmits through a telecommunication system or telecommunication service any intelligence which he knows or has reason to believe to be false, fabricated, indecent or obscene;

This section will review these restrictions and evaluate how these provisions critically fail the tests required by international law, as set out above, to be adequately defined, proportional and necessary.

False and Fabricated Information

As set out above, Article 31 of the Act prohibits the dissemination of "false" or "fabricated" information knowingly or negligently transmitted without any other requirements. This is not in compliance with international law. As a matter of practice, it is extremely difficult to determine what is "true" or "false" or "fabricated" for the following reasons.

- *First*, in situations of rapidly developing news, or where different sources contradict each other, facts may be difficult to check. If, however, journalists have the sword of a false news law hanging over their heads, they might simply decide not to report news of which they are not completely certain at all, for fear of ending up in jail. As a result, citizens will be deprived of potentially vital information on current developments.

- *Second*, facts and opinions are not always easily separated. In many cases, opinions are expressed through superficially false statements, such as sarcastic, satirical, hyperbolic or comical remarks. A ban on false news can thus easily become a ban on opinions not favoured by the authorities, endangering the free confrontation between different points of view which lies at the heart of democracy.

- *Third*, the provisions fail to recognise that it is often far from clear what the "truth" on a particular matter is. If a particular "truth" is well-established at the moment, it may not always remain that way. New opinions and new ways of thinking often replace old ones. No authority holds the absolute truth. To give the government that power allows it to silence anyone with whom it may disagree, no matter the veracity of the matter.

Thus, bans on "false news" severely impact both the right of freedom of expression and the discussion of truth by society and has severe negative effects. As noted by the OAS Special Rapporteur for Freedom of Expression:

> [T]he effect that this principle has is precisely opposite to the one that its proponents argue as the basis for its application. In other words, the search for truth in information would be severely hampered by inhibiting the free flow of information for fear of possible penalties. The right to freedom of information also protects all the information that we have labeled "erroneous".[11]

Numerous UN human rights bodies have made it clear that false news provisions are inconsistent with the guarantee of freedom of expression, particularly if they are enforced through the criminal law. The Human Rights Committee has stated that "the prosecution and punishment of journalists for the crime of publication of false news merely on the ground, without more, that the news was false, [is a] clear violation of Article 19 of the Covenant."[12] The Committee has also reiterated that false news provisions "unduly limit the exercise of freedom of opinion and expression."[13] It has taken this position even with respect to laws which only prohibit the dissemination of false news which causes a threat of public unrest.
In 2000, the UN Special Rapporteur on freedom of opinion and expression declared:

> In the case of offences such as ... publishing or broadcasting "false" or "alarmist" information, prison terms are both reprehensible and out of proportion to the harm suffered by the victim. In all such cases, imprisonment as punishment for the peaceful expression of an opinion constitutes a serious violation of human rights.[14]

The Privy Council has also held that criminal penalties which do not cause the separate offense of disturbing public order are unlawful:

> If... a particular false statement although likely to undermine public confidence in the conduct of public affairs is not likely to disturb public order, a law which makes it a criminal offence cannot be reasonably required in the interests of public order by reference to the remote and improbable consequences that it might possibly do so.[15]

More recently, the HR Committee stated in General Comment 34 that provisions about ensuring the truth of historical facts also are not justifiable under international law:

---

[11] Report of the Rapporteur for Freedom of Expression, OEA/Ser.L/V/II.106, Doc. 3 rev. April 13, 2000.

[12] Concluding Observations of the Human Rights Committee: Cameroon, CCPR/C/79/ Add.116, 4 November 1999, para. 24.

[13] See, for example, Annual General Assembly Report of the Human Rights Committee, UN Doc. A/50/40, 3 October 1995, para. 89; Concluding Observations of the Human Rights Committee: Mauritius, U.N. Doc. CCPR/C/79/Add.60, 4 April 1996, para. 19.

[14] Annual Report to the UN Commission on Human Rights, Promotion and protection of the right to freedom of opinion and expression, 18 January 2000, U.N. Doc. E/CN.4/2000/63, para. 205.

[15] *Hector v. Attorney-General of Antigua and Barbuda* (1990) 2 AC 312 (Judicial Committee of the Privy Council).

> Laws that penalize the expression of opinions about historical facts are incompatible with the obligations that the Covenant imposes on States parties in relation to the respect for freedom of opinion and expression.[16] The Covenant does not permit general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events. Restrictions on the right of freedom of opinion should never be imposed and, with regard to freedom of expression, they should not go beyond what is permitted in paragraph 3 or required under article 20.

Indecent or Obscene Materials

Article 31(d) also prohibits the transmission of materials which are "indecent or obscene." Article 19(3) of the ICCPR allows for limits on freedom of expression for materials in order to protect public morals. However, this does not provide for an open ended ability to ban all materials which officials might find offensive.[17] As noted by the Committee in General Comment No 34:

> the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations ... for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition. Any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination.

The UN Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights also places limitations on the application of pubic morality as grounds for limiting expression:

> Since public morality varies over time and from one culture to another, a state which invokes public morality as a ground for restricting human rights, while enjoying a certain margin of discretion, shall demonstrate that the limitation in question is essential to the maintenance of respect for fundamental values of the community. The margin of discretion left to states does not apply to the rule of non-discrimination as defined in the Covenant.[18]

ARTICLE 19 notes that this section has been cited by the Authority in the justification of Decree CPD-2(101)/11-PTA of 14 November 2011, on "Implementation – Content Filtering Through SMS" which requires that telecommunications providers filter hundreds of words in English and Urdu.[19] Having reviewed this list, ARTICLE 19 is of the opinion that it is a serious violation of international law relating to both freedom of expression and privacy to require that all communications be monitored and blocked on the basis of this seemingly arbitrary list,

---

[16] So called "memory-laws," see communication No., No. 550/93, *Faurisson v. France*. See also concluding observations on Hungary (CCPR/C/HUN/CO/5) paragraph 19.

[17] See also, e.g., *Murphy v. Ireland*, Application No. 44179/98, Judgment dated 10 July 2003.

[18] United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities, *Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights*, Annex, U.N. Doc E/CN.4/1984/4 (1984), pp. 17-18.

[19] Pakistan Telecommunications Authority, Implementation – Content Filtering Through SMS Letter; available at http://content.bytesforall.pk/sites/default/files/PTA%20Letter%20on%20Content%20filtering_0.pdf.

which includes many common words, names of celebrities and others clearly non-obscene materials.

As a matter of international law, all filtering systems are subject to strict limitations. The four international representatives on freedom of expression declared in 2011 that filtering systems were not justified under international law:

> Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.[20]

The UN Special Rapporteur for Freedom of Opinion and Expression, in his 2011 report to the UN Human Rights Council, sets out standards on blocking and filtering systems, noting that all systems 1) must be established in law; 2) which must be clearly justified under international law, based on the exemptions found in Article 19(3) of the ICCPR and subject to public scrutiny; 3) must be necessary and proportionate to achieve their aim, which prohibits limiting access to materials not intended to be blocked; and 4) must be subject to review by a judicial or independent body. [21]

Decree CPD-2(101)/11-PTA and other recently-issued orders blocking access to certain sites have clearly failed to satisfy these legal requirements.[22]

Mischief

Finally, we note with particular concern Article 31(h), which creates a penalty for any person who "commits mischief." The Act does not define this term (although it is defined in the Pakistan Penal Code, which is generally not applicable in the telecommunications arena) or even explain if it is limited to "committing mischief" using a telecommunications service. There is also no requirement of harm.

This provision is too vague to be legitimate under international law. As noted by the Human Rights Committee in General Comment No. 34, a law must be sufficiently clear to be justified under international law:

> For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her

[20] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet, 2011. Available at http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf.

[21] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011, p. 31.

[22] See also ARTICLE 19, Pakistan: Freedom of Expression on Internet Must be Respected, 21 May 2010. http://www.article19.org/resources.php/resource/1542/en/pakistan:-freedom-of-expression-on-internet-must-be-respected.

> conduct accordingly[23] and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.[24] Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.

If the intent of the provision is to prevent some defined harms to other persons using the telecommunications service, it would be more appropriate to include those specific provisions in the Prevention of Electronic Crimes Ordinance or in the criminal law in sections on cyber-related offenses such as hacking, fraud, or denial of service. As it currently stands, the Act offers an open-ended, undefined crime which would potentially apply to any communication that someone, including public officials wishing to shut down debate on areas of public interest, could find annoying.

Recommendations:

- Provisions of Sections 31(d) and 31(h) of the Act has to be removed.

National Security

Throughout the Act, there is a strong power given to the Federal Government in the name of national security to set limitations on free expression and the privacy of communications: Article 8(2)(c) allows the Federal Government to issue decrees on "requirements of national security"; Article 54 overrides all other laws and gives the Government the power to intercept communications and shut down telecommunications systems (see below for detailed analysis of sections) without need for any other legal authorisation or court approval; and Article 57(ag) authorises the Government to set rules on "enforcing national security measures."

With this legislative arsenal, law enforcement authorities can claim legal authority for censoring any critical commentary contrary to official government policy or innocuous expression that poses no actual threat to national security or public order, as narrowly defined.

As outlined above, the protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is prescribed by law, necessary in a democratic society and proportionate. However, the Act contains many provisions that justify restrictions on expression and privacy on the basis of protecting undefined national security interests. These provisions all fail to comply with the three-part test of Article 19 of the ICCPR.

To fit within the rubric of protecting national security or public order, and to meet the requirements of necessity and proportionality under Article 19(3) of the ICCPR, the interests pursued by these provisions must be more narrowly tailored. In their current form, the state is given powers to control telecommunications networks with little restriction or oversight.

---

[23] See Communication No. 578/1994, *de Groot v. The Netherlands*, Views adopted on 14 July 1995.

[24] See General Comment No. 27.

The danger of providing vague powers coupled with little oversight is exemplified by the order of the Authority in 2008 to ban the use of mobile phones which had not been registered. Millions of mobile phones were disconnected with little warning or legal remedy. This was initially justified under the Article 8(2)(c) of the Act. There was no debate in the Parliament or a chance for citizens to contest the decision. Final regulations were issued under the general licensing power.

The *Johannesburg Principles* provide authoritative guidance on narrow tailoring for provisions related to national security. Principle 2 states that the genuine purpose and demonstrable effect of a provision must be to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force.

Recommendations:

- The application of the national security exemption must be limited only to grounds allowed under the Johannesburg Principles.

Powers to Order Terminations of Services

The Act also contains a number of troubling provisions relating to disconnection of services. Article 21(4)(f) authorises that all licenses granted by the Authority contains an obligation to "disconnect telecommunication service from any user who, after written notice, misuses it." Article 54(3) of the Act provides that following the issue of a decree by the President, the Federal Government can suspend any or all licenses for those providing telecommunications services.

This individual and universal interruption of services raises significant freedom of expression concerns. As the controversy over the interruption of networks in Egypt earlier this year shows, the internet is a significant communication tool, and limitations on its access are tenuous at best.

The four international mechanisms on freedom of expression issued a "Joint Declaration on Freedom of Expression and the Internet" in May 2011, which states:

> Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.[25]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated that he "considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights

[25] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint *Declaration on Freedom of Expression and the Internet*, 2011, available at http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf.

law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights."[26]

Recommendations:

- Article 21(4)(f) and Article 54(3) of the Act must be revised to ensure that any disconnections or shutting down of services is only approved by a court in limited, specific circumstances allowed under international law.

Interception of Communications

Another area of concern is the powers given to the Government to intercept communications, seemingly without limitation. Article 54(1) of the Act provides that the "in the interest of national security or in the apprehension of any offense," the federal government may authorise the interception of communications. Article 57(2)(ah) authorises the Federal Government to make rules on the interception of communications without setting any standards.

The right of private communications is also strongly protected in international law, through Article 17 of the ICCPR, which states that:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

The lack of detailed standards in Article 54 are inconsistent with international law, which requires that restrictions on privacy are based on the same permissible limitations requirements as are found for protection of the freedom of expression. In General Comment 16 on the Right to Privacy, the UN Human Committee stated that:

> The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.... Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.[27]

---

[26] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011.

[27] United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), CCPR/C/GC/16, 4 August 1988.

According the UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism:

> [A]rticle 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[28]

The Special Rapporteur has noted that in order to meet the standards to justify an interference, there must be "on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a [criminal offense]."[29]

Interception of communications also impacts other human rights, including freedom of expression. As noted by the Special Rapporteur in his 2009 report on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

> Surveillance regimes adopted as anti-terrorism measures have had a profound, chilling effect on other fundamental human rights. In addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed. Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively. Surveillance has also resulted in miscarriages of justice, leading to failures of due process and wrongful arrest.[30]

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. The UN Special Rapporteur on Freedom of Opinion and Expression has noted that excessive surveillance may "undermine people's confidence and security on the Internet, thus impeding the free flow of information and ideas online." The Special Rapporteur on Terrorism found that:

> These surveillance measures have a chilling effect on users, who are afraid to visit websites, express their opinions or communicate with other persons for fear that they will face sanctions…. This is especially relevant for individuals wishing to dissent and might deter some of these persons from exercising their democratic right to protest against Government policy.

As a practical matter, surveillance also affects the ability of the media to operate. Journalists are not able to effectively pursue investigations and receive information from confidential and

---

[28] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.

[29] *Ibid.*

[30] *Ibid.*

other sources. Surveillance measures also inhibit individuals' ability to seek and receive information.

Recommendations:

- Provisions of Article 54(1) should be eliminated and replaced it with a comprehensive law which regulates surveillance of communications, consistent with the 1998 Supreme Court judgment requiring that all interceptions be approved by the Supreme Court and limited to 6 weeks.[31]

Restrictions on Encryption Technologies

The Act also includes a number of provisions that restrict the ability of users to be able to communicate privately or to use systems to access the internet and other ICTs without interference and surveillance. Article 2(ac) defines "Approved Crypto Apparatus," while Article 5(2)(b) gives powers to the Authority to "monitor and enforce licenses." Article 32 gives Courts the power to authorise searches for "unapproved crypto apparatus" or "other unapproved terminal equipment."

Article 5(2)(b) was used as justification for the "Monitoring and Reconciliation of Telephony Traffic Regulations, 2010"[32] and 21st July 2011 Directive ordering internet service providers (ISPs) and mobile phone companies to block users from using encrypted networks (VPNs) to access the internet.[33]

In light of the above concerns about the excessive blocking and filtering of legal content and the interception of communications without proper legal authority, we believe that these mechanisms are necessary to ensure each person's freedom of expression rights.

Recommendations:

- Article 2(ac) of the Act should be abolished.
- Application of Article 5(2)(b) of the act should be limited to specific administrative licensing issues, rather than as a general power.
- The 2010 regulations and 21st July 2011 Directive must be repealed.

---

[31] PLD 1998 SC 388, *Mohtarma Benazir Bhutto And Others v. President of Pakistan and Others*; available at http://pakistanconstitution-law.org/p-l-d-1998-sc-388/.

[32] Monitoring and Reconciliation of Telephony Traffic Regulations, 2010, S.R.O. 186 (I)/2010, available at: http://www.pta.gov.pk/media/monitoring_telephony_traffic_reg_070510.pdf.

[33] "Usage of Encrypted VPNs," No. 10-1(Viligance)PTA/11-01, 21 July 2011; available at http://twicsy.com/i/NoxrL .