Freedom of Expression on the Internet in Sri Lanka

Centre for Policy Alternatives

NOVEMBER 2011

This report is part of a larger project to strengthen the freedom of expression on the Internet in South Asia implemented by Global Partners, a social purpose company based in London that works to strengthen human rights, democracy and governance in countries around the world. Content herein is updated and revised from 'Freedom of Expression and the Internet in Sri Lanka', a report published by the Centre for Policy Alternatives in August 2010.

The Centre for Policy Alternatives (CPA) is an independent, non-partisan organisation that focuses primarily on issues of governance and conflict resolution. Formed in 1996 in the firm belief that the vital contribution of civil society to the public policy debate is in need of strengthening, CPA is committed to programmes of research and advocacy through which public policy is critiqued, alternatives identified and disseminated.

Address: 24/2 28th Lane, off Flower Road Colombo 7

Telephone: +94 (11) 2565304/5/6 Fax: +94 (11) 4714460

Web www.cpalanka.org Email info@cpalanka.org

Acronyms

BBC	British Broadcasting Service
DDoS	Distributed Denial-of-Service Attack
FMM	Free Media Movement
ADSL	Asymmetric Digital Subscriber Line
URL	Uniform Resource Locator
IP	Internet Protocol
IPTV	Internet Protocol Television
ISP	Internet Service Provider
LTTE	Liberation Tigers of Tamil Eelam
PTA	Prevention of Terrorism Act No 45 1979 (Sri Lanka)
SLT	Sri Lanka Telecom
ACLU	American Civil Liberties Union
TRC	Telecommunications Regulatory Commission (Sri Lanka)
CERT | CC	Computer Emergency Readiness Team | Coordination Centre
CDA	(Federal) Communications Decency Act 1996
ICTA	Information and Communication Technology Agency
UNHRC	United Nations Human Rights Council
UDHR	Universal Declaration of Human Rights
ICCPR	International Covenant on Civil and Political Rights
HSPA	High Speed Packet Access
DNS	Domain Name System
NIPO	National Intellectual Property Office of Sri Lanka

Table of Contents

Executive Summary

The history of freedom of expression in Sri Lanka is inextricably linked to a nearly three-decade-old war and the policies pursued as well as actions undertaken by successive governments and non-state actors. These have led to the murder and abduction of journalists, censorship, intimidation and tolerance of a culture of impunity, which continues to have a direct impact on media freedom and represents a threat to the freedom of expression on the Internet. The directives of national security and arbitrary judgements by government officials on what constitutes the national interest and public morality have been manipulated to stifle dissent and block web content that is considered offensive. The situation is compounded by a legislative framework with broad provisions that allow for civil liberties to be trumped in favour of national security provisions and regulatory standards that demand neither an independent regulatory commission nor transparent administrative practices and adequate protection of data and privacy.

International rights groups and media watchdog organisations have articulated their concern about greater regulation and surveillance becoming a global trend. There is also added concern about the advancement of cheaper and more efficient filtration technologies that make it easier for developing countries to arbitrarily restrict web content. In line with the need to emphasise a rights-based framework for online freedom of expression, this report examines the specific cases and practices that restrict online freedom of expression with respect to regulation, legislation and arbitrary action in Sri Lanka in order to determine whether the incumbent government has abided by international freedom of expression standards and its commitment to upholding Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). This report also considers the freedom of expression standards set out in the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, and examines the conclusions and recommendations of the Special Rapporteur in line with the recent trends of freedom of expression on the Internet in Sri Lanka.

The report looks specifically at the arbitrary blocking and filtering of web content; criminalisation of legitimate expression; the status of intermediary liability and actions of intermediaries. Despite their being no information on disconnecting users from Internet access, including on the basis of intellectual property law, the report highlights the potential for disconnection based on the broad nature of intellectual property legislation. It would however be unlikely to expect either the government or the legislature in the country to approve disconnection from Internet access. The report also examines the potential threat that cyber-attacks may present to online freedom of expression by causing the government to develop more sophisticated surveillance technologies that could be utilised to consolidate a broad regime of surveillance, control and the taking down of content. A critical concern is the protection of privacy and data. The report examines the existing legislative framework, and also highlights the need for specific and comprehensive legislation for the protection of individual privacy and data. The final consideration of this report is with regard to Internet access and the acknowledgement of government policies with respect to providing the necessary infrastructure for increasing Internet penetration in the country. Adequate attention must nevertheless be given to the advantages and disadvantages of technological transfers from developed countries.

While urgent reform of existing legislation and regulatory practices is required in order to address the clear concerns about online freedom of expression, the report proposes national and international advocacy to ensure that the government addresses reform and adheres to international standards on the freedom of expression. There is also a need for a multi-stakeholder initiative so that the perspectives of users, intermediaries and other resource persons are incorporated into the design of the legislative frameworks and regulatory standards, thereby ensuring wide deliberation and participation to achieve the ultimate goal of strengthening freedom of expression on the Internet in Sri Lanka.

1. Introduction

The post-war outlook for freedom of expression on the Internet in Sri Lanka remains unpromising with a great deal evidence pointing towards the government's increased proclivity for imposing restrictions on web content. With a history of online journalists and bloggers under attack, censure and surveillance; websites being shutdown[1] and media premises attacked, and the prevalence of a strong culture of impunity, the government continues to speak of the increasing need for surveillance systems and imposing greater regulation on online content providers in order to preserve cultural values, national security and the national interest. The growing concern at the present moment is the extent to which this technology could be further manipulated to suppress dissent and protect parochial partisan interests.

There is also the issue of technology transfers from countries like China that have established sophisticated online surveillance systems and filtration technologies, which are utilised for the suppression of dissent. In Sri Lanka, the government has established partnerships with Chinese firms and experts for the implementation of broadband infrastructure[2], which has raised concerns about the transfer of surveillance technology as well. These concerns and suspicions are not unfounded given reports of Chinese military intelligence consultants[3] working with the government to assist in the blocking of websites and the Telecommunications Regulatory Commission (TRC) expressing a desire for greater regulation and monitoring of web content.[4]

Several international media watchdogs[5] have already expressed[6] concern about the increase in web censorship following the end of war. In line with reports of a global preference for offline URL filtration and the trends and practices of the Sri Lankan government, there is a need to expose specific cases that contravene international standards and argue for urgent reform, transparency and multi-stakeholder initiatives on Internet governance, the protection of freedom of expression online, and privacy as well as data protection. The latter is all the more important in a context where new media has led to greater freedom of expression through increasing citizen participation in the collection and production of news through innovative citizen media initiatives and the popularity of social media. The risk here is that the government in order to respond to the liberating impact of new media could impose surveillance systems in order to monitor information exchanged on these platforms. This would constitute a violation of the user's right to privacy and fundamentally impact the circulation of information in the country as well as the freedom of expression if citizens fear reprisals based on the content of their online submissions/ conversations. The issue of self-censorship has already deeply impacted mainstream media

---

[1] Examples of on-going web censorship in Sri Lanka, http://ict4peace.wordpress.com/2010/02/23/examples-of-on-going-web-censorship-in-sri-lanka/, 23rd February 2010

[2] "Sri Lanka's Mobitel and ZTE Corporation Carry Out the First Successful 4G (LTE) Trial in South Asia," http://wwwen.zte.com.cn/en/press_center/news/201105/t20110517_234745.html, 17th May 2011

[3] 'Chinese here for cyber censorship,' Sunday Times, http://sundaytimes.lk/100214/News/nws_02.html, February 2010

[4] 'Sri Lankan government prepares new Internet restrictions,' WSWS, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml, 15th February 2010

[5] Enemies of the Internet, Countries under surveillance, RSF, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf, 12th March 2010

[6] In Sri Lanka, censorship and a smear campaign, CPJ, http://www.cpj.org/2009/07/in-sri-lanka-censorship-and-a-smear-campaign.php, 14th July 2009

initiatives, and the risk of a similar trend with alternative news websites is a prospect that would have severe consequences for the future of freedom of expression online.

This report examines legislation and regulation as well as relevant policy trends that do not adhere to the UDHR, ICCPR and international freedom of expression standards. The report will also consider the standards and recommendations detailed in the report by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. It is also important to note the relevance of the cross-regional statement at the 17th session of the HRC in June 2011 where a representative notes that,

> Decisions on Internet governance and policy issues, at global as well as regional levels, should be consistent with international human rights law, including protections for freedom of expression and the right to privacy, and reached in multilateral, transparent and democratic environments. In such environments, it is important that the multistakeholder principle is respected and that governments, the private sector, civil society, academic community and the entire Internet technical community work together to build greater trust in the ICT networks, including necessary cross-border co-operation.[7]

As expressed in the Special Rapportuer's report, there is now clear acknowledgement by a majority of states on the need to safeguard the rights of Internet users as well as the promotion of Internet access as a fundamental human right and enabler of other rights. However, Internet users in Sri Lanka operate within a restrictive legal framework. The Sri Lankan constitution protects the right to free speech and publication. However, it is subject to a host of restrictions including public morality and national security. Moreover, neither the text of the guarantee nor the restrictions imposed on the guarantee meet international standards. In particular, the constitutional text does not require that any restrictions placed on the guarantee be limited by 'reasonableness' or 'necessity'. To date the Supreme Court has not made any pronouncements on the applicability of freedom of expression guarantee to the Internet. The Court has made numerous rulings with regard to the importance of free speech for a democracy, and how criticising the government and political parties are *per se* a permissible exercise of the freedom of speech. Further, the Court has upheld in numerous occasions that arbitrary interference and attacks on journalists are a violation of the freedom of expression guarantee. Thus, a strong argument can be made that the freedom of expression guarantee should be applied to the Internet and that online journalists should receive the same protection afforded to traditional journalists. However, the Court has a weak record when it comes to interpreting restrictions on constitutional rights. Quite often the Court has opted for a narrow conservative approach, which is at odds with comparative international jurisprudence and allows for over-broad national security legislation to trump civil liberties.

Furthermore, there are a host of legislative provisions that currently limit freedom of expression. These laws are not specifically targeted at online content; however, the existence of such laws nonetheless has an impact on the selection and manner in which issues can be discussed online. Broadly, they can be divided in to general laws and laws relating to national security. The national security laws especially emergency regulations (before it was allowed to lapse in September 2011) and the PTA have been criticised often for the broad nature of the legislation, lack of specificity and their insufficient connexion with the objectives they seek to achieve. The Sri Lankan courts have not yet had an opportunity to consider how these content restricting laws can be applied to the online sphere and even though these laws have not yet been enforced in the online sphere, the existence of such a restrictive and repressive legal framework warrants concern.

Given the increasing threats to privacy posed by the Internet, this report considers the right to privacy in Sri Lanka. Under the Roman Dutch common law of Sri Lanka the right to privacy is protected in specific instances. However, there is no right to privacy under the Constitution of Sri Lanka. There are also no legislative provisions that protect general information gathering and handling. The Sri Lanka Telecommunications Act No. 25 of 1991 (as amended) (Sri Lanka) and the Computer Crimes Act No 24 of 2007 (Sri Lanka) provides limited protection to Internet users from surveillance and other forms of intercepting communications. However, both the Acts have

---

[7] Freedom of Expression on the Internet, Cross-regional Statement, Human Rights Council 17th session, 10th June 2011

provisions that allow law enforcement agencies and relevant Ministers to intercept communications without any apparent restrictions or guidelines on their general power to do so.

The need for increased recognition of practices and trends with respect to legislation, regulation and arbitrary government action that impact the Internet is needed for a stronger and more sustainable policy response by civil society organisations and media practitioners. It is also required that transparency is promoted among intermediaries and regulators in order to ensure that legislators and politicians can be held accountable for their actions through increased lobbying and engagement with mainstream media so as to publish and circulate information regarding the status of freedom of expression in the country. There are numerous steps that can be taken both at a legal and policy level. The Government in consultation with service providers, Internet users and bloggers should initiate a comprehensive law reform process and laws that restrict discussion of politically and socially relevant content should be repealed. The Government should take immediate steps to legislate for comprehensive privacy protection. Service providers need to provide clear and accessible privacy policies so consumers are informed of their privacy rights. The effort to block websites and filter content has to be catalogued and published. There is also a requirement for an independent third party who can monitor such moves and the implementation of any privacy policies. Breaches in privacy policies and attempts to stifle online content should be publicised so that users are aware of the limits to their privacy and freedom of expression online.

2. Reflections on UN Human Rights Standards and the Special Rapporteur's Recommendations with Regard to Sri Lanka

The Sri Lankan constitution guarantees freedom of speech and expression, including publication. However, this guarantee is subject to several exceptions including public morality and national security. Neither the text of the guarantees nor its exceptions abide by freedom of expression guarantees in international law. The constitutional restrictions on freedom of expression are not limited by requirements of 'necessity or reasonableness' as required under the ICCPR. A critical point in the Special Rapporteur's report is its recognition that guarantees and rights under the UDHR and the ICCPR were 'drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression.'[8] To date, the Supreme Court of Sri Lanka has not had an opportunity to consider the applicability of these guarantees to the Internet. However, the Court's rulings on the right to publish cases can be illustrative. The Court has recognised that it is a *per se* permissible exercise of the freedom of speech to support or criticise the government, political parties and policies of the government. Further, it is not permissible to impose unequal governmental controls on private publications. Yet, despite these judgments, the Court has a weak record when it comes to interpreting the restrictions on constitutional rights. In a string of cases relating to the freedom of expression, the Court has allowed over-broad and vague national security laws to limit the freedom of expression guarantee.

The Special Rapporteur's three-part cumulative test for the restriction of content provides for a comprehensive framework to judge what is permissible and impermissible in the restriction or limitation on the right to the freedom of expression.[9] In consideration of the cases detailed in this report, it is a test that the Sri Lankan government has failed to pass, particularly with respect to abiding by the Constitution of Sri Lanka and the national legal framework when blocking web content given that most measures to block content are extra-legal. Further, the government has failed to prove the necessity of the restriction, and identify an aim for the restriction of most content. The result of such arbitrary practices has led to numerous alternate news websites being blocked during or after elections with no clear legal justification for the restriction of content. It is clear that most of the blocks – temporary or permanent - on news websites are due to the fact that they have become online centres of dissent, which the government seems unable to tolerate and arbitrarily assumes is a threat to either 'national security' or 'national interest'.

The various legal provisions in Sri Lanka allow for the criminalisation of legitimate expression as detailed in this report, but they have not been consistently enforced in the online sphere due to the relative ease with which extra-legal restrictions are placed on web content. However, judging

---

[8] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations Human Rights Council (UNHRC), Seventeenth Session, 16th May 2011

[9] (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and
(b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and
(c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

from the existing cases of the conviction of journalists, it is clear that there has been no direct evidence to demonstrate that expression of that nature could lead the incitement of racial tensions or present a legitimate threat to national security. The impact of questionable convictions and arrests of journalists along with a three-decade-old conflict that led to the killing of dozens of journalists is that it quells dissent and encourages a culture of self-censorship. While content that is entirely damaging to an individual's reputation should be investigated and followed up with appropriate action, it is worth stressing that if the government ever considers criminalising online expression that it considers harmful to national security, it would have to demonstrate that the information in question would lead to 'imminent violence,' 'incite violence' or that there is 'direct and immediate connection between the expression and the likelihood of such violence.'[10]

The issue of intermediary liability has a great deal of relevance to Sri Lanka, particularly as intermediary companies are held hostage to license conditions that require them to pass on information, restrict or filter content and monitor activity for the benefit of regulators and government ministries, amounting to a violation of the fundamental rights of users. Since the independence of the Telecommunications Regulatory Commission (TRC) is in question following the Eighteenth Amendment to the Constitution, which placed all statutory institutions – including the TRC – under the Executive Presidency, it is important that any request for restriction, monitoring and passing on of information to an intermediary company must occur after judicial intervention in order to protect the intermediary and ensure that it is not complicit in the violation of fundamental rights. On the matter of disconnecting users from Internet access, there is no information available to suggest that this has occurred in Sri Lanka, but the relevant legal provisions with regard to intellectual property law allow for necessary action to be taken to prevent infringement from occurring. This requires further monitoring once specific cases actually occur and the competent authority discloses relevant information so as to ensure that punitive measures undertaken by the judiciary are not disproportionate.

The cases of cyber-attacks reported focus on political groups carrying out DNS poisoning and web defacement attacks against the State. The appropriate response has been to strengthen security software and prevent possible violations from occurring in the future. The danger of the existence of such groups is that they necessitate an increase in the layers and sophistication of surveillance, which could in turn be manipulated to crackdown on any dissent against the government. There is also an added risk of outright cyber warfare and attacks against social networking sites and other online communication tools that have actually strengthened the freedom of expression in the country and supported sensitive human rights work by providing relatively secure channels for communication (for example, Skype.) While the Constitution of Sri Lanka does not guarantee the right to privacy, there is legislation that makes it an offence to interfere or collect and monitor information. However, this does not apply if the direction to reveal certain information has been issued by a Minister or another person with such authority and if information is required with respect to a criminal investigation. As the existing legislation does not provide for comprehensive privacy and data protection, it is important that the government - in accordance with Article 17 of the ICCPR and the HRC's general comment No. 16 - puts forward legislation that will guarantee data and privacy protection.

The Special Rapporteur's request for developed states to facilitate 'technology transfer to developing states' is an important move towards reducing the digital divide and increasing Internet penetration in the country. This would complement existing efforts by the government to increase e-literacy through the facilitation of ICT education programmes and the provision of Internet access by constructing WiFi zones across the country. This along with the implementation of adequate infrastructure would aid the delivery of information to citizens in the country and provide them with alternative and freely accessible sources of information online. However, just as technology transfers from other states would be helpful for the advancement of ICTs and strengthen the freedom of expression, it could also be harmful as closer cooperation with certain states could result in technology transfers that lead to sophisticated surveillance networks and web filtration technology, which may further curtail the freedom of expression and increase arbitrary actions with respect to online censorship in the country.

---

[10] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations Human Rights Council (UNHRC), Seventeenth Session, 16th May 2011

3. Key Constitutional Texts

Article 14(1)(a) of the Sri Lankan Constitution provides that every citizen is entitled to 'freedom of speech and expression including publication'. Article 14 also guarantees freedom of assembly, association, movement, freedom to form and join trade unions, manifest the freedom of religion, promote one's own culture and use of one's own language, freedom to profess a business or profession, the freedom of choice of one's place of residence and the freedom to return to Sri Lanka.

However, the freedom of expression guaranteed by 14(1)(a) is limited by articles 15(2) and 15(7). Article 15 (2) provides that freedom of expression may be limited such restrictions prescribed by law in the interests of 'racial and religious harmony, or in relation to parliamentary privilege, contempt of court, defamation or incitement to an offence'. Article 15(7) provides that the freedom may be limited by restrictions prescribed in law in the interests of 'national security, public order and the protection of public health or morality, or for the purpose of securing due recognition and respect for the rights and freedoms of others, or of meeting the just requirements of the general welfare of a democratic society'. For the purpose of article 15(7) law includes regulations made under the law relating to public security.

It is important to note some of the structural impediments in the Constitution, which impedes the exercise of constitutional rights. Article 16 of the Constitution provides that all existing and written as well as unwritten laws shall be valid and operative notwithstanding any inconsistency with the fundamental rights declared and recognised by the Constitution. This significantly undermines the protection of the constitutional rights guaranteed and the supremacy of the Constitution.[11] In practical terms, all other laws that limit freedom of expression (considered in the previous section) such as the Penal Code 1889 continue to be in force even though they may be inconsistent with the Constitution.

Nonetheless, Article 126 provides for a means of redress whereby citizens can make an application to the Supreme Court upon their fundamental rights being infringed. However, the Sri Lankan Supreme Court has a weak record when it comes to liberal interpretation of constitutional rights. The Court has generally displayed a tendency to favour the State in constitutional rights cases, especially in cases that deal with restrictions imposed under emergency laws.[12] The protection afforded under Article 14 falls short of international standards. In particular, Article 19 of the ICCPR is much broader in scope and includes 'a right to hold opinions without interference, to 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 a person's choice.'[13] Unlike the ICCPR under the Sri Lankan Constitution there is no express requirement that restrictions on constitutional rights be 'reasonable or necessary'.[14] The lack of such a requirement provides much leeway to a government when imposing restrictions and little ammunition for a Court seeking to read down any restrictions.

The leading case on the application of freedom of expression guarantees to the Internet is the American case of ACLU v Reno. The Federal Communications Decency Act (1996) (CDA)

---

[11] Rohan Edrisinha and Asanga Welikala, 'GSP Plus and the ICCPR: A Critical Appraisal of the Official Position of Sri Lanka in respect of Compliance Requirements', in GSP+ and Sri Lanka: Economic, Labour and Human Rights Issues, (2008), p 81.

[12] Sunila Abeysekara v Ariya Rubesinghe and Others (2000) 1 SLR 314; Rohan Edrisinha & Asanga Welikala, above n 280, p 133.

[13] Rohan Edrisinha & Asanga Welikala, above n 280, p 131.

[14] Malagoda v AG (1982) 2 SLR. 777.

contained two subsections 223(a) and 223(d) which prohibited the knowing transmission and display of obscene or indecent materials to minors over the Internet. Over 20 plaintiffs filed a suit alleging *inter alia* that the sections violated the First Amendment. A federal court issued a temporary restraining order against the enforcement of 223(a) claiming that the subsection violated principles of freedom of expression. The Government appealed and the validity of the sections were heard before the Supreme Court. The Supreme Court agreed with the lower courts and held that the CDA violated the first amendment. The Supreme Court held that terms 'indecent' and 'patently offensive' were unconstitutionally vague and that the objectives of the CDA could be achieved using laws that were less restrictive of speech.

In addition, the Court held that the Internet enjoys full protection under the First Amendment free speech guarantee.[15] The Court rejected the government's arguments that the Internet should be regulated in a similar way to traditional broadcast media. Firstly, the Internet has not historically been subject to extensive regulation in a manner similar to traditional broadcast media. Secondly, unlike broadcast media, the Internet is not limited by a spectrum of available frequencies. Thirdly, Internet is not invasive in the way television or radio is - 'communications over the Internet do not invade an individual's home or appear on one's computer screen unbidden'.[16]

The Sri Lankan Supreme Court has had no opportunity thus far to determine whether freedom of expression extends to communications made *via* the Internet. There is no case law on freedom of expression and other information and communication technologies. The closest examples come from the Court's decisions relating to right to publish and broadcast media. The court has taken a liberal approach to what constitutes 'expression'. The right to vote,[17] and non-speech forms of political protest[18] have been held to be within the ambit of freedom of expression. The Court has explained the freedom as follows,

> Freedom of speech and expression consists primarily not only in the liberty of the citizen to speak and write what he chooses, but in the liberty of the public to hear and read what it needs. No one doubt if a democracy is to work satisfactorily that the ordinary man and woman should feel that they have some share in Government. The basic assumption in a democratic polity is that Government shall be based on the consent of the governed. The consent of the governed implies not only that consent shall be free but also that it shall be grounded on adequate information and discussion aided by the widest possible dissemination of information from diverse and antagonistic sources. The crucial point to note is that freedom of expression is not only politically useful but that it is indispensable to the operation of a democratic system.[19]

In numerous subsequent judgements, the Court has endorsed the important role that free speech plays in a democratic society. In Pradeep Kumar Darmaratne v Inspector of Police W. Dharmaratne, OIC, Police Station, Aranayake and five others No. 163/98 the petitioner was a journalist who had written several articles about the unlawfully distilled liquor industry and criticised police inaction on the issue. After the publication of the article, the petitioner was taken into the custody by the police and beaten. The Court held that the petitioner's right to be free from torture under Article 11 was breached. Though the Court did not make any findings on the right to free speech, the Court held that freedom of speech is designed to provide for robust and transparent debate on public issues. Further, the freedom protects not only speech that we agree with but also speech that we find repulsive.[20] Similarly in Amaratunga v Sirimal (1993) 1 SLR 264

---

[15] ACLU v Reno 521 U.S. 844 (1997), 869.

[16] Ibid.

[17] Karunathilaka v Dayananda Dissanayake (No. 1) (1999) 1 SLR 157.

[18] Amaratunga v Sirimal (1993) 1 SLR 264.

[19] Joseph Perera v AG (1992) 1 SLR 199, at 202 per Sharvananda CJ.

[20] Pradeep Kumar Darmaratne v Inspector of Police W. Dharmaratne, OIC, Police Station, Aranayake and five others No 163/98 at p 7 per Weerasekara J.

the right to support or criticise the Government, political parties, policies and programmes is *per se* a permissible exercise of the freedom of speech and expression under Article 14 of the Constitution.

Furthermore, there is a string of cases decided specifically on the issue of journalists and free speech. In these cases, the Court has held that arbitrary interventions and attacks on the press have chilling effects on the right to free speech. In the Victor Ivan v Sarath N. Silva Attorney General and Others (1998) 1 SLR 340 (Victor Ivan Case), Victor Ivan - editor of a Sinhala newspaper Ravaya - argued that journalists should be treated differently from ordinary individuals. The court rejected this view and held as follows,

> Freedom of press is not a distinct fundamental right but is part of the freedom of speech and expression including publication which article 14(1)(a) has entrenched for everyone alike. It surely does allow the pen of a journalist to be used as a mighty sword to rip open facades which hide misconduct and corruption but it is also two edged weapon which he must wield with care not to wound the innocent while exposing the guilty[21]

In that particular case, Ivan claimed that he had been indicted several times for allegedly having defamed ministers and other high level officials. Ivan alleged that these indictments were arbitrarily transmitted by the Attorney General to the High Court, without proper assessment of facts as required under law. As a consequence, Ivan argued *inter alia* that his freedom of expression was being restricted and the publication of his newspaper was being obstructed. The Supreme Court held that errors and omissions themselves are not proof that actions are arbitrary or discriminatory and Ivan's case was unsuccessful. However, following the judgment of the Supreme Court, Ivan exercised his rights under the first optional protocol to the ICCPR and took the case to the Human Rights Committee. The Committee held *inter alia* that the Attorney General's actions did have a 'chilling effect' which 'unduly restricted' Ivan's freedom of speech.[22]

In other cases, the Court has held that attacking journalists and interfering with their work can amount to a violation of their right to free speech. In S.J. Dias v Honourable Reggie Ranatunga, Deputy Minister of Transport, Environment and Women's Affairs and six others (1999) 2 SLR 8 the court again considered the free speech rights of a journalist in the course of her work. A television news journalist and her film crew noticed a burning lorry on the side of a main road and filmed the event. The Deputy Minister who was passing in his own vehicle demanded to know why the crew was filming the Minister's vehicle. When the petitioner denied filming the Minister's vehicle, the Minister's security guards assaulted him and forcibly took him to a police station where he was detained for over six hours. Further, the police recorded a statement and made the petitioner sign it without letting him read it. The Court held that there was a violation of Article 11 and 13(1). With regard to Article 14(1)(a) the Court held that had the news item been broadcast it would have amounted to an exercise of the petitioner's right to free speech. Thus the respondent's conduct amounted to a violation of the petitioner's right to free speech. The Court held that freedom of speech may also include other rights such as the right to obtain and record other information; for example, interviews and photographs, that are necessary to make the actual exercise of that freedom effective.

The Court has also recognised that arbitrarily stopping a television show from being aired can amount to a violation of a viewer's right to free speech. In Fernando v The Sri Lanka Broadcasting Corporation and Others (1996) 1 SLR 157 a listener of a educational programme broadcast by the government challenged its actions when the programme was arbitrarily stopped from being aired. The petitioner argued that he was not only a regular listener but also participated in the programme on several occasions. The Court held that the freedom of speech of the petitioner qua participatory listener had been infringed because the stoppage of the programme prevented further participation by him.[23]

---

[21] Victor Ivan v Sarath N. Silva Attorney General and Others (1998) 1 SLR 340, 347 per Fernando J.

[22] Victor Ivan Majuwana Kankanamge v Sri Lanka CCPR/C/81/D/909/2000 at para 9.4.

[23] Fernando J at 180.

Regarding the constitutionality of the Sri Lanka Broadcasting Bill SC 81/95, the Court held that imposing unequal governmental controls on private broadcasting institutions is a violation of their right to free speech. The petitioners challenged a bill that sought to appoint the 'Sri Lanka Broadcasting Authority', which had the power to licence private broadcasting and television stations. However, the bill did not require public broadcasters or television stations to be licensed. Further the government broadcasters were only required to conform to certain guidelines where it was practicable to do so. The private sector broadcasters though, were required to follow the guidelines at all time and failure to do so amounted to an offence. Thus, it was argued that the government broadcaster was subject to a less strict standard of accountability than the private sector broadcaster.

The Court held that there was a violation of the right to equality and the freedom of expression provisions of the Constitution. The unequal conditions for the private broadcasters amounted to imposing governmental controls upon the private radio and TV broadcasts of the island. The Court held that by controlling media publications, the freedom of speech and expression enshrined in the Constitution was impinged upon. However, in deciding that freedom of expression was impinged, the Court went to quote from earlier judgements to state that constitutional freedoms are not absolute and 'there must be a happy compromise between [the individual's] rights and the interests of society'.

4. Restriction of Content on the Internet

a. Arbitrary blocking or filtering of content

During the latter part of the war, websites that purported to provide alternative coverage on the war were blocked. From June 2007, allegedly on the orders of the Sri Lankan government, all Internet service providers in Sri Lanka blocked users from being able to access the website Tamilnet.com.[24] The website was regarded as being supprtive of the LTTE and the Government accused it of being a propaganda instrument of the movement. To date, the Government has denied any knowledge of the unavailability of Tamilnet.com. The Government spokesperson at the time and current Mass Media and Information Minister Keheliya Rambukwella denied any government involvement in the blocking of Tamilnet.com and added that 'the government is looking to hire hackers to disable Tamilnet but could not find anyone yet'.[25]

Article 19, an international human rights group, condemned the government for cutting off an important source of independent and alternative views.[26] Local media watchdog Free Media Movement criticised the government as follows:

> The ban on Tamilnet is the first instance of what the FMM believes may soon be a slippery slope of web & Internet censorship in Sri Lanka. It is also a regrettable yet revealing extension of this Government's threats against and coercion of print and electronic media in Sri Lanka since assuming office in late 2005.... The FMM stresses that the danger of censoring the web & Internet is that it gives a Government and State agencies with no demonstrable track record of protecting & strengthening human rights and media freedom flimsy grounds to violate privacy, curtail the free flow of information and restrict freedom of expression[27]

For example, although not completely blocked during the latter part of the war, the website of Human Rights Watch remained regularly inaccessible.[28] Other websites such as TamilCanadian.com, Lankanewsweb.com, Nidahasa.com and Lankaenews.com were also blocked.[29] Despite the fact that the website was not shutdown, the Attorney General's Department noted that 'the government has received a complaint that the Tamil National Alliance website directly contributes towards dividing the country and that it promotes the concept of a separate Eelam State'.[30]

---

[24] Groundviews, 'Sri Lanka blocks TamilNet', Groundviews, 19 June 2007, http://www.groundviews.org/2007/06/19/sri-lanka-blocks- tamilnet/

[25] BBC, 'Tamil Net Blocked in Sri Lanka', BBC, http://www.bbc.co.uk/sinhala/news/story/2007/06/070620_tamilnet.shtml

[26] Article 19, 'Sri Lanka News Agency Blocked in Attack on Press Freedom', 20 June 2007, http://www.article19.org/pdfs/press/sri- lanka-tamilnet-blocked.pdf

[27] Lanka Business Online, 'Slippery Slope Sri Lanka media body slams moves to block Internet', 20 June 2007, http:// www.lankabusinessonline.com/fullstory.php?SEARCH_TERM=33&newsID=1539658495&no_view=1

[28] Reporters Without Borders, Internet Enemies – Countries under surveillance: Sri Lanka, 12 March 2009, http://www.unhcr.org/ refworld/docid/4a38f97fc.html

[29] Kumar David, 'Implications of an Information Dark Age', Lakbima News, 21 February 2010, http:// ict4peace.files.wordpress.com/ 2010/02/lakbima-21-2-2010.pdf

[30] The Bottom Line, 'Plans to kill TNA website?', The Bottom Line, 9 April 2008, http://www.thebottomline.lk/2008/04/09/B38.htm

On the eve of the Presidential election, a number of Sri Lankan news websites were also blocked. Lankaenews.com, Lankanewsweb.com, Infolanka.com and Srilankaguardian.org websites were blocked hours before the results of the presidential election were announced.[31] The sites were inaccessible from Sri Lanka's main ISP, the state-owned Sri Lanka Telecom (SLT).[32] However, the sites were accessible by the privately owned ISP Dialog WiMax. It was further reported - according to a source who worked for SLT - that 'verbal directives were given' to block the websites. Several complaints were made to the Election Commissioner, who had in turn referred the complaints to SLT. SLT, however, refused to answer any questions. Reporters without Borders condemned the government by stating that,

> Such censorship reflects a beleaguered government's nervousness and readiness to resort to manipulation...The free flow of news and information during an election offers one of the few guarantees against massive fraud. We urge the government to restore access to these sites...[33]

On the 20th of June 2011, Groundviews[34], a citizen journalism initiative, was completely inaccessible for over eight hours on SLT (Sri Lanka Telecom) ADSL broadband connexions. Since it began operations in 2006, this was the first time the site was inaccessible over an ISP in Sri Lanka. Several reader reports from across Sri Lanka confirmed the site could not be accessed, as well as that over ISPs like Dialog and Etisalat the site continued to be accessible. Reader reports also indicated that the vernacular citizen journalism initiative Vikalpa[35] and the website of Transparency International Sri Lanka (TISL) were also inaccessible over SLT ADSL broadband connexions at the same time as Groundviews. In response to widespread news reports of the issue, TRC Director General, Anusha Palpita, responded by stating that the TRC has "not taken measures to block any news sites during the past year except for the LankaeNews website, which was following a court order."[36] It is interesting to note that the requirement of a court order appears to have been overlooked with regard to websites such as Tamilnet.com and a number of other websites mentioned above that were intermittently and arbitrarily blocked in the past. Following the conclusion of a court case concerning Lankaenews this year, it was reported in October that access to the site had once again been blocked *sans* any legal basis and due to its coverage of an incident of intra-party violence.[37]

The concerns over a possible registration process that were mooted by the TRC in 2010 were realised when the Director General of Government Information Department issued a press release on the 5th of November 2011, which pointed to a requirement of all 'websites carrying any content relating to Sri Lanka or the people of Sri Lanka... uploaded from Sri Lanka or elsewhere' to 'register' for 'accreditation.' On the same day, the TRC moved to block several websites without allowing an adequate period of time for the owners of websites to respond to the request. [38] There were several other issues about the request, which highlight the arbitrary nature of policy-

---

[31] BBC, 'Sri Lanka news websites 'blocked', BBC, 27 January 2010, http://www.bbc.co.uk/sinhala/news/story/ 2010/01/100127_lankaenews_rsf.shtml

[32] Reporters Sans Frontiers, 'Websites blocked just hours before poll results due to be announced', Reporters Sans Frontiers, 26 January 2010, http://en.rsf.org/sri-lanka-websites-blocked-just-hours-before-26-01-2010,36213

[33] Ibid.

[34] The Centre for Policy Alternatives is the host institution of Groundviews.

[35] The Centre for Policy Alternatives is the host institution of Vikalpa.

[36] "TRC denies blocking of websites," Daily Mirror, 23rd June 2011

[37] "In Sri Lanka, anti-government websites blocked," CPJ, http://www.cpj.org/2011/10/in-sri-lanka-access-to-anti-government-website-blo.php, 19th October 2011

[38] "Govt. blocks more websites, all must register," Sunday Times, http://www.sundaytimes.lk/111106/News/nws_03.html, 6th November 2011

making and imposition of regulations by the government, as well as the threat to freedom of expression on the Internet. A statement issued by civil society organisations and concerned individuals noted the following,

> Firstly, there was no clarification about what the process of registration will entail and whether any sort of liability or conditions will be imposed. Secondly, the press release does not establish with sufficient clarity the categories of either websites or persons who are required to register with the Ministry. Thirdly, it is not clear whether and how the requirement for registration will apply to international news websites and websites operated by international organisations that publish news on and in Sri Lanka. Finally, in the interests of transparency, consistency and equal treatment, the Information Department did not explain in the statement the legal framework and process under which registration of this nature can be enforced.
>
> The requirement of registration coupled with the blocking of websites, which potentially constitutes a form of prior-censorship, not only produces a chilling effect on the freedoms of expression and information on the Internet, but also constitutes a prima facie violation of a number of constitutionally protected fundamental rights, including Article 14(1)(a) of the Constitution of Sri Lanka. The obligations of the government with respect to international standards are made clear by Sri Lanka's ratification of enforceable international legal instruments, which includes the ICCPR. Needless to say, these measures also do not meet broader standards of international best practice as reflected in the Special Rapporteur's report.[39]

An added concern with regard to the issue of filtration has been the emerging global trend of ISPs utilising offline URL filtering, which is 'the best option for ISPs that need to conform to government regulations to censor the Internet' and where the '…system performs URL filtering on Web traffic "destined" to arrive at a filtered Web site, and this can be determined based on the destination's IP address.'[40] Given that offline URL filtering is a relatively cost effective option when compared to DNS and IP filtering, and further allows ISPs to block specific URLs rather than entire websites, this new form filtering provides an effective solution for governments to block web content that is considered offensive or deemed to be in violation of very broad national security legislation.

In August 2008, the President ordered the country's TRC to block access to adult entertainment websites. The Government spokesperson explained that the move was designed to prevent children from viewing pornography over the Internet.[41] The ISPs were to filter out sexually explicit material by default and only make it available to adults who request and pay an additional fee to access the unfiltered service. Obviously the directive had been issued without much consideration as to how such a ban would be effectively implemented. In any event, to date the directive has not been effectively implemented. Foreign pornography websites continue to be available even on an SLT (the state-owned ISP) Internet connexion. In June 2009, on an application brought forward by the Inspector General of Police, the Colombo Magistrates Court ordered the TRC to ban twelve Sri Lankan pornography websites. Once again, the extent to which the court order has been implemented is questionable. Ironically this official ban on websites appears to be less effective than the unofficial ban on websites such as Tamilnet.com. Four of the twelve banned

---

[39] 'Arbitrary Blocking and Registration of Websites: The Continuing Violation of Freedom of Expression on the Internet,' http://cpalanka.org/arbitrary-blocking-and-registration-of-websites-the-continuing-violation-of-freedom-of-expression-on-the-internet/, 9th November 2011

[40] Offline filtering preferred way of Web Censorship, ZDNet, http://www.zdnetasia.com/offline-filtering-preferred-way-of-web-censorship-62301507.htm, 3rd August 2011

[41] Daily News, 'TRC directed to filter obscene websites', Daily News, 2 August 2008, http://www.dailynews.lk/2008/08/02/ news11.asp

pornographic websites were available on a Dialog Internet connexion.[42]

In the post-war context, the government's concern over pornography has not lessened. It was recently reported that the Women and Child's Bureau within the Police has formally requested that pornography websites be banned on mobile phones.[43] As a result, it was estimated that up to 400 websites could be banned under such a request.[44] Director General of the TRC has confirmed that it had received such a request, but had stated at the time that it is waiting on Cabinet approval prior to implementing such a ban.[45] The Sri Lankan government has proposed new stringent legislation under the Obscene Publications Act of 2011 that would 'prohibit the publication, exhibition, print, telecast, broadcast or lets on hire or knowingly sells or distributes or in any manner introduces into circulation through any medium of communication – print or electronic – object or thing which is obscene or imports, exports, makes, produces, prints or knowingly transmits, transports or possesses or does any other act whatsoever with regard to any matter object or material which is obscene, for any purpose' in the country.[46] It is unclear at this point what new restrictions will be imposed online and how the TRC as well as ISPs will respond to the provisions of the legislation. The Ministry of Justice has placed emphasis on the need to prevent the circulation of child pornography, which has also been noted by the Special Rapporteur as an urgent requirement in order to prevent the sexual exploitation of children. The immediate concern with the new legislation is the lack of, firstly, detailed provisions and, secondly, an exact definition of what may constitute 'obscene' content. The latter in consideration with the Ministry's stress on the need to ensure that print and electronic media conforms to 'cultural, religious and moral values' in the country,[47] could result in the manipulation of legislation leading to the imposition of restrictions on legitimate forms of expression that oppose conservative norms, religious doctrine and cultural values.

As the critics have noted, protecting children from pornography is a worthy policy objective. However, the question remains whether banning all pornography - even from adults - is the appropriate response. The Special Rapporteur notes the following with regard to protecting children from pornographic content,

> ...while the protection of children from inappropriate content may constitute a legitimate aim, the availability of software filters that parents and school authorities can use to control access to certain content renders action by the Government such as blocking less necessary, and difficult to justify.[48]

This is an issue that other jurisdictions have grappled with. In Australia, when a move to filter pornographic content was mooted, Internet service providers pointed to the infeasibility and

---

[42] Sanjana Hattotuwa, 'Banning Sri Lankan porn online: a couple of months after', ICT for Peacebuilding, 31 January 2010, http://ict4peace.wordpress.com/2010/01/31/banning-sri-lankan-porn-online-a-couple-of-months-after/

[43] Daily Mirror, 'Police seek mobile porn ban', Daily Mirror, 12 May 2010, http://srilankanewsfirst.com/politics/17315.html

[44] Ibid.

[45] Ibid.

[46] Tough new laws against porn, Daily Mirror, http://www.dailymirror.lk/news/14318-tough-new-laws-against-porn.html, 25th October 2011

[47] Ibid.

[48] The Special Rapporteur's report refers to this citation with respect to this point: Center for Democracy & Technology, "Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age," version 0.5 - Discussion draft (April 2011), p.5.

unworkability of such a broad filtering regime.[49] In the US, the Supreme Court held that though removing access to pornographic content from children is acceptable, withholding adult access to such content would be in violation of the First Amendment.[50] Critics of the Chinese attempts to block pornography have pointed out that the Chinese government in its objective to block 'vulgarity' has also blocked other social and political content that is critical of the Chinese government.[51]

b. Criminalisation of legitimate expression

As noted in the previous section, much of what happens to restrict freedom of expression in Sri Lanka is extralegal. However, it is important to note the legal restrictions as well. At present, there are a host of laws that limit the full exercise of freedom of expression in Sri Lanka. These laws can be grouped into two categories: national security laws and general laws. General laws are all laws that do not pertain to national security. The examples include the Official Secrets Act, Sri Lanka Press Council Law, Parliament (Powers and Privileges) Act and defamation and contempt of court laws at common law. Laws relating to national security include both emergency laws and other general laws, specifically enacted to protect national security. These laws affect all forms of speech and not just those that are communicated on the Internet. To date, these laws have not been enforced with respect to online content in Sri Lanka. However, their presence has to be considered as they limit what can be discussed online. In addition, these laws when applied to the online sphere can have novel and often unintended consequences. This section firstly identifies the key content restricting laws currently in force in Sri Lanka and secondly - with references to examples from other jurisdictions - attempts to explain how such laws can be enforced online.

National Security Laws

There are three main problems with national security laws. They are often vague so their scope is difficult to determine, there is the issue of over-breadth as they cover matters that are insufficiently connected with national security to warrant censorship and they impose harsh penalties that encourage self-censorship. There are two categories of national security laws: general laws that exist until repealed and emergency regulations that are only in force during a state of emergency.

Emergency Regulations[52]

Emergency Regulations are made under the Public Security Ordinance No 25 1947 (Sri Lanka) (Public Security Ordinance). Articles 76 and 155 of the Constitution also provide legal basis for the President to make emergency regulations. The Public Security Ordinance itself does not create any specific offences. It makes legal provisions for the President to declare a state of emergency, after which the President can make regulations, which create specific offences and prescribe punishments. The procedure for making emergency regulations is to first announce that part II of the Public Security Ordinance has been brought in to operation by way of proclamation and then to publish the proclamation in a gazette notice.[53] An emergency can be declared solely at the discretion of the President. Whenever in the opinion of the President it is expedient to do so in the interests of public security, preservation of public order, maintenance of supplies and services

---

[49] James Kirby, The Net- Overseas pornography will filter through, Business Review Weekly, 12 November 1999, http://www.brw.com.au/stories/19991112/4092.htm

[50] ACLU v Reno 535 U.S. 1 (2002).

[51] Evgeny Morozov, 'Will Bahrain's censorship efforts run into 'cute cat theory'?', Net.effect, 2 April 2009, http://neteffect.foreignpolicy.com/posts/2009/03/30/will_bahrains_censorship_efforts_run_into_the_cute_cat_theory

[52]* At the time of writing this report, President Rajapakse announced that emergency regulations would be lifted. Further information: 'Sri Lanka president lifts wartime laws,' Reuters, http://in.reuters.com/article/2011/08/25/idINIndia-58967520110825, September 2011

[53] Public Security Ordinance No. 25 of 1947 (Sri Lanka), s (2)

essential to the life of community, the President may declare an Emergency.[54] There is no requirement of an 'exceptional threat' that is generally understood to be a condition precedent to the valid declaration of an emergency.[55] The discretion afforded to the President and allowing expediency to be a factor is at odds with international standards, which require the 'life of the nation to be under threat' prior to declaring a state of emergency.[56] Once an Emergency is in operation, the President is empowered to make such regulations as s/he views necessary, expedient or in the interests of public security, preservation of public order, suppression of mutiny, riot or civil commotion or for the maintenance of supplies and services essential to the life of the community.[57]

Emergency Regulations come into force the moment they are made by the President[58] and have the legal effect of overriding all laws except provisions of the Constitution.[59] However, the Constitution itself permits emergency regulations to restrict certain constitutional provisions including Article 14(1)(a) that guarantee freedom of expression.[60] Emergency Regulations do not have a permanent nature; their duration is limited to a period of one month from the date of coming into effect.[61] However, they may be revoked before the end of the one-month period or extended before or at the end of that period.[62]

Parliament retains limited powers over the process of creating emergency regulations. Once an emergency has been proclaimed, it must be communicated to Parliament within a set time frame.[63] Further, within fourteen days the proclamation must be approved by resolution in Parliament.[64] If Parliament does not approve a proclamation then the emergency ceases to be valid.[65]

Up until September 2011, Sri Lanka was under almost uninterrupted emergency rule for over three decades. During the ceasefire period of 2001, emergency rule lapsed. However, once the government recommenced the war, the country came back under emergency rule. In fact, it has been observed that a state of emergency is the norm, not the exception in Sri Lanka.[66] One of the effects of the frequent 'emergencies' is that each emergency sets a higher bar than the previous one allowing the government to expand its role and increase the nature and scope of its

---

[54] Ibid.

[55] Welikala, A, 'A State of Permanent Crisis: Constitutional Government, Fundamental Rights and States of Emergency in Sri Lanka (2008), Centre for Policy Alternatives and FNST, p199.

[56] Ibid.

[57] Public Security Ordinance No 25 of 1947 (Sri Lanka), s (5)(1).

[58] Public Security Ordinance No 25 of 1947 (Sri Lanka), s (11).

[59] Public Security Ordinance No 25 of 1947 (Sri Lanka), s (7).

[60] The Constitution of the Democratic Socialist Republic of Sri Lanka 1978, s 15.

[61] Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2)(2).

[62] Ibid.

[63] Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2)(3).

[64] Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2)(4).

[65] Ibid.

[66] Publius, 'Normalizing the exception: state of emergency in peace time', Groundviews, 30 May 2009, http://www.groundviews.org/ 2009/05/30/normalising-the-exception-the-state-of-emergency-in-peacetime/

extraordinary powers.[67] As a result, the public have become accustomed to the government's expanding role and less likely and willing to question the government.[68]

Emergency regulations most commonly limit freedom of expression by either imposing a complete prohibition on the reportage of certain subjects and/or requiring that news reports have to be approved by a 'competent authority' before publication. Among the most restrictive regulations introduced are the following:

- Editorial comment, feature stories, news reports on any subject should be submitted for approval to a government appointed authority;
- There should be no publication of any matter which is under consideration or alleged to be under consideration by any Minister or Ministry;
- No person may affix in a public place or distribute among the public any poster or leaflet prior to police permission;
- No person shall bring the President or government into hatred or contempt or incite feelings of dissatisfaction;
- Printing presses could be sealed if public security, public order or essential services are threatened.[69]

Even two years after the war ended, Sri Lanka continued to be in a state of emergency.[70] However, in May 2010 many of the emergency regulations were relaxed, particularly regulations relating to holding meetings and gatherings, curfews, printing literature and providing householder's names to the police.[71] However, the military continues to enjoy wide police powers to investigate suspected terrorist activities.[72] There is very little legal redress available once emergency regulations are in force. Once an emergency has been declared, the fact of emergency cannot be questioned in court.[73] However, on occasion the Supreme Court has been willing to strike down the validity of emergency regulations on the grounds that they violate fundamental rights. While it was reported that Emergency regulations would be allowed to lapse in September 2011, the government also made sure that key provisions of the emergency regulations were added as amendments to the existing Prevention of Terrorism Act of 1979, including extraordinary powers of arrest and detention.[74]

Prevention of Terrorism Act

Prevention of Terrorism (Temporary Provisions) Act No. 48 of 1979 (PTA) grants the police wide powers of search, arrest and detention. The PTA along with emergency regulations was suspended during the ceasefire period as part of the government's commitment not to arrest anyone under the PTA. However, even in the post war period the PTA continues to be in force.

There are several sections that specifically seek to restrict freedom of expression. Section 14(2) of the PTA makes it an offence to print or publish in any newspaper without the prior approval of a competent authority (appointed by the relevant Minister) any matter relating to the commission or

---

[67] Ibid.

[68] Ibid.

[69] Article 19, War of Words: Conflict and Freedom of Expression in South Asia Thematic Reports, (May 2005), p 66.

[70] Extraordinary Gazette Notice no 1651/24 (Sri Lanka), 2 May 2010.

[71] Colombo Page, 'Sri Lankan government relaxes emergency regulations', Colombo Page, 4 May 2010, http:// www.colombopage.com/archive_10/May1272987911JV.php

[72] Ibid.

[73] Public Security Ordinance No 25 1947 (Sri Lanka), s 3.

[74] CPA Statement on the New Regulations Under the Prevention of Terrorism Act, http://cpalanka.org/cpa-statement-on-the-new-regulations-under-the-prevention-of-terrorism-act/, 23rd September 2011

investigation of an offence under the Act; or incitement to violence, or which is likely to cause racial or communal disharmony or feelings of ill-will or hostility between different communities or racial or religious groups. Section 2(1)(h) of the PTA provides that any person who by words either spoken or intended to be read or by signs or by visible representation or otherwise causes or intends to cause commission of acts of violence or religious, racial or communal disharmony or feelings of ill-will or hostility among different communities or racial or religious groups shall be guilty of an offence.

General Laws

Sri Lanka Press Council Law

The Sri Lanka Press Council Law No 5 of 1973 (Press Council Law) came into force as a means of regulating the press. The law remained inactive for a number of years, and was reintroduced by the government in June 2009.[75] It establishes a Press Council to regulate the press.[76] The Council constitutes the Director for Information and six other members appointed by the President.[77] The objectives of the Council are *inter alia* to ensure freedom of the press and high standards of journalistic ethics.[78] The council has the power to require a proprietor, printer, publisher, editor or journalist of any newspaper to provide any information requested by the Council and prescribe a code of ethics for journalists. In particular, the Council has power to hold inquiries where it has reason to believe that an untrue statement has been published in a newspaper or where there has been a breach of journalistic ethics.[79] After such an inquiry, the Council has the power to order a correction, censure the proprietor, editor or journalist or order an apology to be tendered.[80] An order made by the Council is deemed final and cannot be questioned in a court of law.[81]

A 'newspaper' is defined in the Act as 'any paper containing public news, intelligence or occurrences printed or published in Sri Lanka...'[82] Given this narrow definition it might be possible to argue that an online newspaper or a more informal news blog would not fall within the purview of the Press Council.

The Press Council Law prohibits publication of material falling into the following broad categories: obscenity and profanity,[83] government decision-making,[84] fiscal policy[85] and official secrets.[86] Section 16(1) makes it an offence to publish any proceeding of a cabinet meeting without prior approval from the secretary to the Cabinet. Section 16(5) prohibits the publication of any matter alleged to be under consideration by a Minister or the government when such a matter is in fact

---

[75] 'Opinion: Sri Lanka Elections Don't Translate Into Political Will,' http://www.globalpost.com/dispatch/worldview/100127/sri-lanka-elections, 27th January 2010

[76] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s2.

[77] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s3.

[78] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s8.

[79] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s9.

[80] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s9(1)(a)-(c).

[81] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s9(5).

[82] Sri Lanka Press Council Law No.5 of 1973, s 33.

[83] Sri Lanka Press Council Law No 5 of 1973 (Sri Lanka), s15(1)(a),(d).

[84] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s16(1),(2),(5).

[85] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s16(4).

[86] Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s16(3).

not under consideration. The Act also prohibits any official secrets and any matter relating to military, naval, air force or police establishments, equipment or installation, which is likely to be prejudicial to the defence and security of the country.

The prohibitions imposed by the Press Council Law are especially damaging, given that current constitutional arrangements only allow for a very limited time for the public to challenge a bill for its unconstitutionality. In such contexts, it is important for a newspaper to have the freedom to report on government decision-making and cabinet proceedings, so that the public have a chance to be informed and if necessary initiate legal action within the specified time frame.[87]

Official Secrets Act

The Official Secrets Act No 32 of 1955 makes it an offence for anyone in possession of an official secret to communicate it to any unauthorised person.[88] An official secret is widely defined to include any information relating to any arm of the armed forces; any implements of war maintained for use in the service of the country; any equipment, organisation or establishment intended to be or capable of being used for the purpose of the defence of Sri Lanka; and any information directly or indirectly related to the defences of Sri Lanka.[89] Quite similar to the Press Council Law, this Act has not been used that widely. However, critics argue that by its mere presence, laws such as these have a 'chilling' effect on freedom of expression in the country.

Defamation

In 2002, Sri Lanka repealed laws concerning criminal defamation. Civil defamation can be established if the publication is 'malicious'.[90] Civil defamation does not require intent to harm or knowledge of likely harm. Whether or not the publication was in the national interest is not a defence in a defamation case.

Contempt of Court

The courts have defined what constitutes contempt in a very conservative manner. Contempt has been found in publications that suggested judges were responsible for a serious breach of duty in taking unauthorised holidays by going to race meets and thereby contributing to arrears of work.[91]

In the Ceylon Daily News[92] case, a deputy editor was imprisoned for six months for commenting that a judge's criticism with regard to a witness's clothing was 'not in keeping with the new legal trends of the day'. The Supreme Court has ruled that publication of a report on a parliamentary proceeding even though fair, accurate and made without malice, may nonetheless be punished if it constitutes contempt of court. In Hewamanne v Manik de Silva (1983) 1 S.L.R. 1 it was held that the "law of contempt would operate untrammeled by the fundamental right of freedom of speech and expression."

In Re Garuminige v Tillekratne (1991) 1 SLR 134 a provincial correspondent of Divaina sent a report of a speech made by a member of the Opposition at a time when the Presidential election petition was being heard in which the Opposition member was quoted as having said that the 'petition had already been proved and if the petitioner did not win her case it would be the end of justice in Sri Lanka'. The journalist argued that he merely reported the contents of a speech and that it was clearly done in a political context, which readers would appreciate. The court rejected

---

[87] Sabina Fernando, 'Freedom of Expression and Media Freedom', in ed Kanagananda Dharmananda and Lisa M. Kios, Sri Lanka: State of Human Rights Report 1997 (1997), p 71.

[88] Official Secrets Act No 32 of 1955 (Sri Lanka), s 7.

[89] Official Secrets Act No 32 of 1955 (Sri Lanka), s 27(1).

[90] Jayawardane v Aberan (1964) Ramanathan Reports.

[91] Re Hulugalle 39 NLR 294.

[92] Re Hulugalle 39 NLR 294.

this view and found contempt on the basis that the publication might or was likely to result in prejudice to the pending hearing of the Presidential election petition and that the report inferred that the judges had already made up their minds and thus possibly deterred potential witnesses from giving evidence. In Sri Lanka, where cases can drag on for interminable lengths of time, this rule can seriously impede the discussion of matters of public interest.[93] In A.M. E. Fernando v Attorney General (2003) 2 SLR 52, a human rights activist was convicted for contempt for having raised his voice and continuing to speak even after the court had explained to him that he cannot proceed with his fundamental rights case.

To varying extent, the power of subordinate courts to punish for contempt is regulated. However, comparable powers of the superior courts are unrestricted. Section 105(2) of the Constitution empowers the Supreme Court and Court of Appeal to punish on the basis of contempt. There are no procedures to regulate the contempt of court inquiries. Section 136 of the Constitution authorises the Chief Justice along with three other Supreme Court justices nominated by him to make rules regulating generally the practice and procedure of the Court, including the making of rules as to the proceedings in the Supreme Court and Court of Appeal. However, to date the Supreme Court has not formulated such rules.

Parliamentary Privilege

The law of parliamentary privilege gives the Parliament the power to punish attempts to interfere with its work including actions or statements directed against the legislature as a whole or an individual in his or her capacity as a member. The Parliament (Powers and Privileges) Act No. 21 of 1953 (as amended by the Parliament (Powers and Privileges) Amendment Law No. 5 of 1978, Parliament Act No. 17 of 1980, Parliament (Powers and Privileges) (Amendment) 1997) empowers the Supreme Court to punish any of the following types of publications:

i. Willfully publishing any false or perverted report of any debate proceedings of the House or Committee or willfully misrepresenting any speech made by a member in the House or in Committee;
ii. Willfully publishing any report or any debate or proceedings of the House or a Committee, the publication of which has been prohibited by the House or Committee;
iii. The publication of any defamatory statement reflecting on the proceedings and character of the House;
iv. The publication of any defamatory statement concerning any member of parliament in respect of his or her conduct as a member; and
v. The willful publication of any report of any debate or proceedings of Parliament containing words or statements after the Speaker has ordered such words or statements to be expunged from the official report of Parliamentary debates.

Penal Code

As with other legislation, there are over-broad provisions in the Penal Code, which impose unreasonable and disproportionate restrictions on freedom of speech. Section 120 of the Penal Code makes it an offence to utter such words which 'excite or attempt to excite' feelings of dissatisfaction towards the government; inciting hatred or contempt towards the administration of justice; raising discontent or disaffection among citizens; or promoting ill will and hostility between different classes of subjects. Section 118 makes it an offence to bring the President into contempt by insulting words or disparaging words, signs or by any other visible representations.

The Public Performance Ordinance

The Public Performance Ordinance No 7 of 1912 (as amended) has been used to censor films, dramas and other 'entertainments' as defined by the Public Performances Board (PPB). The law also gives the relevant Minister a wide range of powers to make rules for the regulation of films,

[93] Human Rights Commission, Contempt of Court the need for substantive cum procedural definition and codification of the law in Sri Lanka (2005), p 11.

dramas and other entertainments.[94] Under the power to make regulations, the Minister can issue, withdraw or suspend permits for the exhibition of such performances.[95]

Obscene Publications Ordinance[96]

The Obscene Publications Ordinance No. 4 of 1927 (as amended) makes it an offence to produce, possess, import, export, carry on, take part in a business or advertise the availability of obscene publications.[97] However, the Act does not define the term 'obscenity'.

Profane Publications Act

The Profane Publications Act No 41 of 1958 makes it an offence for any writer, publisher, printer or distributor to write, produce, print, publish, sell, distribute or exhibit any profane publication.[98] A profane publication is defined to mean any newspaper, book, picture, film or other visible representation containing an insult to the founder of any religion, any deity, saint or person venerated by the followers of any religion, or any religious belief or any representation that ridicules any figure, picture, emblem, device or other thing associated with or sacred to the following of any religion.[99] There is an inbuilt defence by way of 'fair comment and fair criticism'.[100]

In Sri Lanka, though these laws have not yet been enforced in the online sphere, their mere existence warrants concern. In particular, the emergency regulations and the PTA - combined with the culture of violence against those who speak out - have created a far more effective culture of self-censorship that limits freedom of expression. Both Internet users and regulators need to be aware that existing laws, which restrict content, may present severe challenges to the online sphere.

Restrictions

The Supreme Court has a poor record when interpreting restrictions to constitutional rights. In particular when constitutional rights and national security collide, the Court has come down on the side of the State favouring the interests of national security at the expense of constitutional rights. The Court departed from this approach in the seminal case of Joseph Perera v Attorney General (1992) 1 SLR 199 where it was held that restrictions on constitutional rights needed to be narrowly constructed to suit specific objectives. In particular, the Court implied that such restrictions needed to be 'reasonable' and 'necessary'. In subsequent cases, the Court though following the reasoning in the Joseph Perera case still concluded that over-broad and vague national security laws can restrict constitutional rights.

In Visvalingam v Liyanage (1984) (2) SLR 305 the Petitioner complained against the prohibition of the publication of the "Saturday Review," which was a regional newspaper published in Jaffna. Though censorship was imposed on virtually all newspapers, the Saturday Review was banned outright. The prohibition was ordered in the aftermath of communal riots in 1983. The Supreme

---

[94] Public Performances Ordinaces No 7 of 1912 (Sri Lanka), s 3.

[95] Public Performances Ordinaces No 7 of 1912 (Sri Lanka), s 3(e).

[96] The Government recently announced its decision to introduce updated legislation in order to restrict obscenity - Obscene Publications Act of 2011. Please refer to 'Tough new laws against porn,' Daily Mirror, http://www.dailymirror.lk/news/14318-tough-new-laws-against-porn.html, 24th October 2011 and p. 18 of this report for further information on the implications of such legislation for electronic and print media.

[97] Obscene Publications Ordinance No 4 of 1927 (Sri Lanka), s 2.

[98] Profane Publications Act No 41 of 1958 (Sri Lanka), s 2.

[99] Profane Publications Act No 41 of 1958, s 5.

[100] Profane Publications Act No 41 of 1958 (Sri Lanka), s 2.

Court held that the restriction on freedom of expression was justified given that the editorial policy of the newspaper was extremely prejudicial to the security and safety of the country and its citizens.

In Siriwardena v Liyanage (1983) 2 SLR 164, the President declared a State of Emergency soon after the conclusion of the Presidential elections. Under the Emergency regulations, the Competent Authority sealed the petitioner's press, which printed and published the newspaper of an opposition political party. The order additionally prohibited the publication of the Aththa newspaper. The petitioner alleged that the sealing of the press constituted *inter alia* an infringement of Article 14(1)(a). The Supreme Court held that there was a need to prohibit the publication in light of the reasonable concern that such a publication could inflame the political passions of the people to cause a condition of civil unrest.

In Wickremasinghe v Edmund Jayasinghe, Secretary to the Ministry of Media (1995) 1 SLR 300 the Court held that where there is a proximate or rationale nexus between the restrictions imposed and the objective to be achieved, there will not be a violation of Article 14(1)(a). In that case, the government prohibited the media from publishing material in relation to the following:

> a) Information of Military operations carried out or proposed to be carried out by the Defence Forces;
> b) Information concerning procurement or proposed procurement of arms or supplies of armed forces;
> c) Information concerning the deployment of troops or personal, or the deployment or use of equipment, including aircraft or naval vessels, by such forces;
> d) Information pertaining to the official conduct or the performance of the Head or any member of any of the armed forces or the police forces.

The Court considered whether these restrictions violated the freedom of speech, expression and publication and held that they did. However, the Court also held that the restrictions were justified as they achieved an objective set out in Article 15, namely 'national security.'

The Court observed that,

> In the instant case, it cannot be said that the occasion and manner of pre-censorship is arbitrary. The government is faced with a serious civil war. The matters in respect of which censorship is imposed are specified. The restriction is against the publication of matters that could be classified as sensitive information. Those who are responsible for national security must be the sole judges of what the national security requires. It would be obviously undesirable that such matters should be made the object of evidence in a court of Law or otherwise discussed in public.

Further Amerasinghe J noted that,[101]

> In this connection the 'dual aspect' of the freedom of expression needs to be stressed. It requires on the one hand, that no one be arbitrarily limited or impeded in expressing his or her own thoughts. In that sense, it is a right that belongs to each individual. Its second aspect on the other hand, in general implies a collective right to receive information and have access to the thoughts expressed by others.

The tide turned in Joseph Perera v Attorney General (1992) 1 SLR 199 where the police disrupted a meeting about public education by utilising powers under emergency regulations. Two days prior to the meeting, the petitioner had distributed a leaflet that was critical of the Government. The police claimed that the organisers of the meeting should have obtained police permission before distributing the leaflets. The Court held that the requirement that leaflets be approved by the police violated the petitioner's freedom of speech. In particular, the Court held 'that pre-censorship which confers unguided, and unfettered discretion upon an executive authority without narrow, objective and definite standards to guide the official is unconstitutional.' This

[101] [2000] 1 SLR 314, 337.

decision is especially significant as it was the first time that the Court recognised that restrictions on constitutional rights need to be 'necessary' or 'reasonable'.

The Prasanna Withanage v Sarath Amunugama, Minister of Rehabilitation, Reconstruction and Development of the Northern Region and Others (Purahanda Kaluwara case), is an example of how national security laws can restrict artistic expression. In that case, the Minister for Media alleged that the screening of the film Purahanda Kaluwara (Death on a Full Moon Day) would be a violation of Emergency Regulation 14 (same as that considered in the Abeysekara case above). The Minister for Media argued that it would adversely affect the war effort and directed the Chairperson of the National Film Corporation to prevent the release of the film until the security situation improves. The Court held that indefinite suspension of the release of the film was a violation of the right to free speech. With regard to the Minister's direction, the Court held it to be invalid as the relevant Act only authorised the Minister to give general directions related to policy. Further, under the relevant emergency regulation only certain kinds of persons were prohibited from publishing and this did not include producers of films, distributors of films and cinema owners.

The approach in Joseph Perera v Attorney General (1992) 1 SLR 199 case was upheld in subsequent cases.[102] However, even in those cases the decisions were criticised for the Court's failure to appropriately balance the competing interests. In Abeysekera v Rubesinghe, an emergency regulation prohibited the publication of news with regard to military operations in the North and East, including operations carried out by armed forces or the police, the deployment of troops or use of equipment by such forces, official conduct, morale or the performance of armed forces, police or any person authorised by the Commander-in-Chief to assist in the preserving national security. The petitioner - a human rights activist - alleged that the regulation was over-broad and violated *inter alia* Article 14. She argued that she needed to know accurate information with regard to the position of the war and that the aim of the regulation was to prevent embarrassment to the government rather than to safeguard national security. The Court expressly observed that freedom of expression was important in a democracy and that there was a need to construe limitations on such rights in a narrow manner. However, the Court also held that the regulations in question struck a fair balance between the competing interests of national security and freedom of expression. The Court held that the Regulation in question was not over-broad, but tailored to achieve a specific objective and not for any extraneous reasons such as covering up government embarrassments. In particular, the Court observed its position as follows,

> Terrorism not only hurts, but tends to destroy democracy and democratic institutions. There are imminent dangers threatening the free, democratic constitutional order of the Republic of Sri Lanka. In such a situation, national security must take precedence over the right of free speech.[103]

These cases illustrate the inherent conservatism of the Court when it comes to balancing national security and constitutional rights.

Application to the Internet

There is a strong case to be made that the Internet should be protected under Article 14 of the Sri Lanka constitution. As the above jurisprudence illustrates, the Supreme Court has on numerous occasions upheld the importance of free speech to a democratic system, and recognised that the freedom to speak applies regardless of the mode used to express one's ideas. The Internet is fast becoming an indispensable tool in facilitating speech, expression and publication. Thus, if it is to have any meaningful use in Sri Lanka, the existing jurisprudence under Article 14 must be applied to the Internet. Thus, online speech that is unpopular and critical of the *status quo* must be protected under Article 14.

---

[102] Abeysekera v Rubesinghe (2000) 1 SLR 314; Wickremabahu v Herath (1990) 2 SLR 348.

[103] Abeysekera v Rubesinghe (2000) 1 SLR 314, 378 per Amersainghe J.

In light of the right to publish cases such as Fernando v The Sri Lankan Broadcasting Corporation and Others, where the Court held that arbitrarily stopping an educational programme would infringe the freedom of speech of the listener, it is possible to argue that arbitrarily blocking websites would infringe on the freedom of speech of the reader. The Court has also held that imposing unequal controls on broadcasting institutions is a violation of the right to free speech. Thus, specific controls such as requiring registration of websites or permission from government authorities prior to publishing content may violate freedom of speech guarantees. The Joseph Perera Case may have special application in the context of websites. In addition, the requirement of websites to register or a website licensing scheme would amount to the sort of censorship prohibited in the Joseph Perera case. If such a scheme was ever to be implemented in Sri Lanka, in line with the view in the Joseph Perera case, a critical caveat would be that the requirements were reasonable and necessary. Further, the Court's jurisprudence on rights of journalists and news publications can be extended to online news publications, online journalists and even potentially to bloggers. Traditional journalists that publish on the online sphere should receive the full protection afforded to journalists under the existing jurisprudence that prohibits arbitrary interference and violent attacks against journalists.

However, it is not yet a settled question whether bloggers are afforded the same protection as journalists. In a landmark case in the United States, a Californian Court of Appeal decided that bloggers are entitled to protect their sources the same way traditional journalists can.[104] In that case, Apple Computers sued several individuals called "Does" who had leaked information about an upcoming Apple product on an online news site. Apple subpoenaed the online news provider's email service provider to reveal various communications belonging to the online news website. The news website argued *inter alia* that discovery of the communications were barred owing to privilege arising from state and federal guarantees of a free press. The privilege holds that a news gatherer cannot be compelled to divulge the identities of confidential sources without showing sufficient grounds. On the question of whether such a privilege was available to bloggers, the Court held that there is no basis to distinguish petitioners from reporters, editors and publishers who provide news to the public through traditional print and broadcast media.

However, this does not appear to be a settled question across the United States. Recently, a Court in New Jersey held that traditional journalists who publish in the online sphere are entitled to be considered journalists. However, bloggers would not be afforded the same entitlement.[105] The Court held that the blogger could not be protected as a journalists as she "exhibited none of the recognised qualities or characteristics traditionally associated with the news process, nor has she demonstrated an established connection or affiliation with any news entity."[106]

In Sri Lanka, the Courts have not yet had an opportunity to consider the legal status of bloggers. However, soft law mechanisms are being developed that may lead to hard law or at least influence the course of future law reform. In this regard, the 2008 Colombo Declaration on Media Freedom and Social Responsibility is significant as it recognises the importance of the Internet as follows:

> One of the most significant developments in the last ten years has been the growth of the Internet, which has resulted in the democratization of media and encouraged the emergence of non-professional journalists in the form of bloggers etc. We acknowledge the contribution of bloggers towards the promotion of free speech and democratic media. We also recognize that bloggers are as susceptible to controls by the state, misuse of their work as traditional print and broadcast media. We take this opportunity to commit our support to responsible bloggers and other new media practitioners, and hope to work with them in solidarity towards establishing a convergent media which is strong and independent

---

[104] Jason O'Grady v Apple Computer Inc, Court of Appeal of the State of California, Sixth Appellate District.

[105] Mary Pat Gallagher, 'No reporter shield for mere blogger, N.J. Appeals Court Says', Law.com, 26 April 2010, http://www.law.com/ jsp/article.jsp?id=1202451742674

[106] Ibid.

> We specifically call on the government to recognize the Internet as an important space for deliberative democracy, and extend to it, all such policies as would enhance the space of free speech on the Internet, and to avoid all policies of banning, blocking, or censoring websites without reasonable grounds. There is now a convergence between the traditional print media and the Internet, with a number of newspapers being accessed through the Internet, and we would strongly urge that all the privileges and protections sought in this declaration be extended to the web editions of newspapers[107]

However, it is important to note that rights, which are protected under the Constitution, can also be severely limited. As noted above, the Courts have a poor record when it comes to reading down the Parliament's zealous national security laws. Thus similar to the way the Courts have limited the content that can be published in traditional newsprint, it is possible that the Courts will take the view that online content must also be limited, where such content is 'prejudicial to the security and safety of the country' or 'capable of inflaming civil rest'. Moreover, though there has been recognition that such limitations must be 'necessary or reasonable' to the objective sought to be achieved, the Court has a poor record of balancing these competing interests of a free society. Quite often the Court has opted for a narrow conservative approach, at odds with comparative international jurisprudence, which allows for over-broad national security legislation to trump civil liberties.

c. Imposition of intermediary liability

When the above cases of restriction and monitoring are considered, it is clear that regulators have imposed specific legal provisions for ISPs to operate, which require them to abide by certain conditions as a requirement for obtaining their license for operation from the state. The terms and conditions of a license can relate to any of the following:

a) Any matter that appear to be the Minister to be requisite or expedient to achieving the objectives of the TRC;

b) Payment of an ongoing license fee;

c) To provide the TRC with any documents, accounts, estimates, returns or other information that may be necessary to carry out the TRC's duties;

d) Conditions preventing the ISPs from discriminating against any person regarding any services provided;
e) Conditions requiring the ISP to publish a notice specifying the charges and other terms and conditions upon which services are provided;

f) Conditions requiring the ISP to ensure that an adequate information system which may include billing information, tariff information, directory services are available to users;

g) Conditions requiring an operator:
1. To comply with any directions given by the TRC in relation to the national transmission plan, signaling, switching plan, numbering plan, and the charging plan to which an operator shall design and maintain his telecommunication network and conditions requiring approval from the TRC before departing from any of the plans;
2. To keep the TRC informed of the practices followed by the ISP in the routing of national and international traffic; and
3. To ensure that compensation is paid to persons affected by the running of underground cables or overhead lines;

h) Conditions requiring an operator to:
4. To comply with any direction given by the TRC as to any matter specified in the

[107] Colombo Declaration on Media Freedom and Social Responsibility, October 2008, http://ict4peace.files.wordpress.com/2009/03/ declaration_eng.pdf

licence;
5. To act with the consent of the TRC when doing things that are required to be done under the licence; and;
6. Refer any questions arising under the licence to the TRC

i) conditions requiring the connection to any other telecommunication systems and apparatus;

j) conditions requiring an operator to develop and publish a plan to restore service during emergencies;

k) conditions specifying acceptable economic criteria in accordance with which the TRC shall approve tariff adjustments proposed by the operator.

The general penalty for the contravention of any of the above conditions is as follows:

> (1) Every person who contravenes or fails to comply with any provision of this Act or any regulation or rule made thereunder or with any requirement imposed thereunder or with any order, award or direction given thereunder shall be guilty of an offence.
>
> (2) All offences under subsection (1) shall be triable summarily by the Magistrate's Court.

The nature of license conditions imposed on intermediaries is problematic and runs the potential risk of private companies being complicit in the violation of fundamental rights in an effort to abide by specific license conditions as well as direct and arbitrary requests for information from relevant government authorities. The latter is clear when the submissive acquiescence of ISPs in the country is considered with respect to abiding by arbitrary orders from the TRC to block websites. Any reform of the provisions under the Act should consider judicial intervention i.e., a court order, as a necessary basis for the fulfillment of any of the above license conditions in order to protect intermediary companies and make them less responsible and/or liable for having to follow through with requests from the state buttressed by repressive and illiberal legislation. As the Special Rapporteur's report notes,

> "…given the pressure exerted upon them by States, coupled with the fact that their primary motive is to generate profit rather than to respect human rights, preventing the private sector from assisting or being complicit in human rights violations of States is essential to guarantee the right to freedom of expression."[108]

An added strategy for the mitigation of intermediary liability would be to promote transparency among intermediary companies that provide an Internet service in the country. The Special Rapporteur's report highlights the value of multi-stakeholder initiatives in order to address any issues related to Internet governance.[109] The report also commends Google's Transparency Report[110], which goes to the extent of providing information on government requests for censoring or removing certain information on services provided by Google. Therefore, it is certainly beneficial for intermediary companies to initiate a multi-stakeholder initiative with the ultimate goal of enabling a 'transparency initiative' so that Internet users in Sri Lanka may either be privy to the number of requests for censoring and taking down of content or to details on the exact nature of the content that is censored or taken down from the web. The impact of legislation and regulatory frameworks on ISPs is examined in the next section.

---

[108] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations Human Rights Council (UNHRC), Seventeenth Session, 16th May 2011

[109] Ibid.

[110] Please view www.google.com/transparencyreport

d. Responsibility of intermediaries

Regulatory framework for Internet Service Providers (ISPs)

ISPs in Sri Lanka are regulated under the Sri Lanka Telecommunications Act No. 25 of 1991 (as amended) (the Telecom Act). The Telecom Act as amended establishes the TRC, a five-person body chaired by the Secretary of the Ministry responsible for Telecommunications. In 2010, the President was responsible for the Ministry of Mass Communications, but following a cabinet reshuffle at the end of 2010, Keheliya Rambukwella was appointed the Minister of Mass Media and Information. However, the Secretary to the President, Lalith Weeratunga, continues to chair the TRC. Furthermore, the TRC as a statutory institution falls within the ambit of the executive presidency.[111] This immediately calls into question the independence of the TRC given that it is not constituted of a governing body that is independent of political interests.

Under Section 17 of the Act, ISPs are required to obtain a license from the relevant Minister to operate a 'telecommunication system' in Sri Lanka. The TRC may make recommendations as to whether a Minister should grant a license or not.[112] In order to recommend that a license be granted, the TRC must be satisfied that the operator is capable of operating the relevant telecommunication system.[113] However, the Minister may reject such recommendations and grant a license under his or her own discretion.[114] Applications for licenses are to be made in writing and in a manner required by the TRC.[115] Further a fee must be paid for each license[116] and the Minister may impose conditions on a license.[117]

The actions of the TRC must be in accordance with the provisions of the Telecom Act, the Constitution and other relevant laws. If the TRC were to act outside the powers granted to it or pursue objectives beyond that specified in law, its actions may be checked by a writ application before the Court of Appeal. Further, if the actions of the TRC infringe upon constitutional rights, then a fundamental rights case may be brought against the TRC before the Supreme Court. It is notable that following reports in 2010 that the Government planned to introduce regulations to require news websites to register with the authority, it was pointed out that the TRC had no authority to require or to maintain a register of news websites.[118] Further, any such action could potentially be the subject of a writ or fundamental rights application.[119]

Efforts to regulate online content

In October 2008, the Minister for Mass Media and Information promulgated the Private Television Broadcasting Station Regulations of 2007 (the Regulations) under powers conferred by the Sri Lanka Rupavahini Act No. 6 of 1982. The Regulations sought to regulate private television

---

[111] 'Statutory Institutions and Ministries under the Executive President,' http://www.president.gov.lk/about_presidency.php

[112] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(2).

[113] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(5).

[114] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(2).

[115] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(4).

[116] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(6)(a).

[117] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(6)(c).

[118] Rohan Samarajiva, 'Quo Warranto TRC?', Lirneasia, 14 February 2010, http://lirneasia.net/2010/02/quo-warranto-trc/

[119] Ibid.

broadcasting stations. From the outset civil society groups were highly critical of the Regulations given the negative implications it had for freedom of expression in Sri Lanka. Some of the measures that were subject to criticism included a requirement that only Sri Lankan citizens can apply for television broadcasting licences; political parties would be prohibited from obtaining a television broadcasting licence; any licence granted would be only for one year duration; any licence may be cancelled by the Minister for failure to comply with content restrictions; there would be a committee to advise on the administration of television broadcasting appointed by the Minister; the Regulations required all kinds of organisational information to be supplied to the Minister and at times prior approval from Minister was needed for day to day operations that would in effect undermine the independence of the media.[120] Various civil society groups and private media institutions challenged the Regulations and were successful in getting the Supreme Court to grant an interim order to suspend the Regulations.[121]

Despite the laws never being effectively enforced, it is worth examining the Regulations as they had some unique application to online video content. The Regulations sought to classify private television broadcasting stations on numerous grounds including on the basis of geographical coverage, technology used, on the basis of whether a station uses its own or others broadcast transmission infrastructure and so on.[122] Critics had particular issue with how the classification of 'the method used to access the viewer' would work in practice. In particular, the Regulations applied to 'Internet Based Television Broadcasting Stations' and 'Mobile Telephony Platform Based Television Stations'.[123] The Regulations did not define what 'broadcasting' was, or what constituted an 'Internet Based Television Station' or a 'Mobile Telephone Platform Based Television Station.' Given that potentially any person with access to the Internet or a mobile phone could be a 'broadcaster', it was unclear how such persons would be affected under the Regulations.[124]

The Regulations did not seek to distinguish between the vastly different models of television delivery using the Internet and mobile telephones.[125] In particular, there is an important distinction between the transmission of TV over IP networks (IPTV) and delivering TV generally over the open Internet.[126] IPTV is essentially a digitally based television service, similar to a cable channel that uses the Internet as opposed to cable to deliver television to the viewer.[127] To date Sri Lanka has had only one IPTV service, 'PEO' provided by Sri Lanka Telecom. Usually such services are

---

[120] 'On the new Private Television Broadcasting Regulations', Free Media Movement, 30 October 2008, http:// freemediasrilanka.wordpress.com/2008/10/30/on-the-new-private-television-broadcasting-station-regulations/

[121] 'Draft paper formulated', 3 April 2009, http://www.thefreelibrary.com/Draft+paper+formulated-a0199262018

[122] 'On the new Private Television Broadcasting Regulations', Free Media Movement, 30 October 2008, http:// freemediasrilanka.wordpress.com/2008/10/30/on-the-new-private-television-broadcasting-station-regulations/

[123] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[124] 'On the new Private Television Broadcasting Regulations', Free Media Movement, 30 October 2008, http:// freemediasrilanka.wordpress.com/2008/10/30/on-the-new-private-television-broadcasting-station-regulations/

[125] [125] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[126] Ibid.

[127] New Media Glossary, http://www.sag.org/content/new-media-glossary

delivered over an exclusive network managed by a telecommunications company.[128] They are different from Internet videos or tele-visual content produced by users for other users to be viewed on demand via streaming on the Internet or as downloadable video casts.[129] The latter essentially refers to video sharing websites YouTube, Vimeo and any other instances where Internet users upload videos for viewing by other users. Therefore, given that the Regulations do not distinguish between these two types of services, it potentially requires both to operate under a valid licence from the TRC. In other jurisdictions such as the European Union, lawmakers have drawn a distinction between services such as IPTV and,

> Activities which are primarily non-economic and which are not in competition with television broadcasting, such as private website and services consisting of the provision or distribution of audiovisual content generated by private users for the purposes of sharing and exchanging within communities of interest[130]

Further, the regulations require 'Internet based television broadcasting stations' to a) have an ISP license or b) to enter into an agreement with an ISP for the 'use of such network facilities required for the establishment and maintenance of such a broadcasting station'.[131] Similarly the regulations also require 'Telephony based private broadcasting stations' to a) have a valid license issued by the TRC for a telephony network operator or b) enter into such an agreement with a telephony network operator for the 'use of such network facilities required for the establishment and maintenance of such a broadcasting station'.[132] Critics have pointed out that such a measure is pointedly designed to undermine the freedom and independence of online video content and if necessary to restrict access to such video content.[133] In particular, given that the Regulations require license holders to monitor content or risk losing their license, an agreement for the 'establishment and maintenance' of a broadcasting service could require an ISP or Telephony Network provider to monitor online video content. Moreover, it could force ISPs to enter into agreements with individual customers to not host or access content that are incompatible with the regulations. The lack of any defined framework for such an agreement has negative implications for the rights of all wired and wireless broadband as well as other users of the Internet as those who are not customers of an ISP could still use the Internet to disseminate video productions.[134]

Moreover, the Regulations provide that a license for broadcasting television may be cancelled among other circumstances for broadcasting programmes that are detrimental to the interests of national security, inciting breakdown of public order, inciting ethnic religious or cultural hatred, in violation of any laws of the country, morally offensive or indecent, detrimental to the rights and privileges of children and or in violation of the code of ethics, standards and practices of Television Broadcasting.[135] In the context of Internet Based Broadcasting Stations, these provisions have added meanings. Given that all state-owned and privately owned ISPs are risk averse and have blocked a host of websites, without any public acknowledgement of doing so, it is likely that ISPs will act even more cautiously and limit Internet content even further. More

---

[128] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[129] Ibid.

[130] Directive 2007/65/EC Audiovisual Media Services Directive. April 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=OJ:L:2007:332:0027:0045:EN:PDF

[131] Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 9.

[132] Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 10.

[133] [133] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[134] Ibid.

[135] Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 13(e).

disturbingly, the regulations failed to appreciate that unlike cancelling the private broadcasting licence of an individual television station, cancelling the licence of an ISP can have catastrophic consequences. The act of cancelling the licence of an ISP to broadcast video content would potentially limit the ability of millions of subscribers to share video content online.

In the context of user generated video content, it is often the case that other users can comment and provide responses to video content. It is entirely questionable how an ISP would monitor such user-generated comments to video content so as to comply with content restrictions on the regulations. The regulations also required that licence holders keep electronic copies of all materials broadcast for a minimum period of sixty days.[136] It is technically impossible to monitor all video content on the Internet. It is highly doubtful whether any broadcaster or ISP in Sri Lanka would have had the massive technical, financial and human resources required to comply with these regulations.[137]

The regulations also prohibited the broadcasting of transmissions, which originated outside the territory of Sri Lanka, unless permission had been granted by the Minister.[138] The Regulation can have meaningful application to normal television broadcasts, Cable TV, Satellite TV and even IPTV. However, it cannot in anyway regulate television content already on the Internet and content that will be produced in the future. Therefore, it raises the alarming possibility that in order to comply with the Regulations, ISPs may have to block every website and Internet location containing video content originating outside the territory of Sri Lanka.[139]

The Regulations further provided that the validity of any licence was limited to the number of channels described in the licence. It is important to note that once again in the context of online video content, the term 'channel' has a different meaning. In the context of video sharing sites such as YouTube, there are literally millions of user-generated channels. Thus it is technically impossible to determine the number of channels that can be broadcast over the Internet.[140] Hypothetically, even if it was possible to provide a list of the millions of video streams available, it would be outdated in less than twenty-four hours.[141]

The regulations also prohibited any political party from holding a license for a private television broadcasting station or network.[142] However, given the unclear meaning of 'Internet-based broadcasting stations' it is uncertain whether political parties can use the Internet to disseminate video content. Given the onus on ISPs and license holders to police content, they may refuse to produce, transmit or archive any content affiliated with a political party. In consideration of the nature of politics in Sri Lanka, what was fit for broadcasting under one regime may not be permissible under another. Such a situation would severely undermine the right to information of the general public by potentially cutting off vital video content that can educate and inform them.

The regulations are illustrative of the lawmaker's lack of understanding of the dynamics of the Internet and their complete disregard for freedom of expression both online and elsewhere. Though the Regulations were never enforced, the ill-defined and over-broad nature of the Regulations and the onus placed on ISPs to regulate content over their networks potentially

---

[136] Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 16 (b).

[137] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[138] Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 26(1)(b).

[139] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[140] Ibid.

[141] Ibid.

[142] Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 6.

undermines the freedom of expression of end-users, including citizen journalists, professional media personnel and human rights activists.[143]

In the post-war context, the government has not shown any signs of easing its stance on freedom of expression. There has been a consistent agenda demonstrated by the government to monitor and regulate web content. Following the 2010 Presidential election, it was reported that new regulations would be drafted by the TRC, which would initiate a registration process for all news websites 'with the authority to obtain Internet Protocol addresses'.[144] An important point to note are the reasons given by the TRC and government about what sort of web content needed to be monitored and regulated. The Director General, Anush Palpita, stated that 'there should be a proper system of monitoring and regulating content…content – whether political, cultural, religious or pornographic – should be checked if they "create problems in society."'[145] A similar statement was made by Charitha Herath, an advisor to the Mass Media and Information Ministry, who stated that "our national interest has to be protected and therefore it is important to have a debate on the subject of content regulation."[146] An issue with regard to such vague statements is that it leads to the protection of partisan interests, which justify the monitoring and restriction of web content critical of the government as upholding the 'national interest' and protecting national security. This became quite clear after the police made several arrests in order to clamp down on text messages that were circulated by individuals accusing the government of electoral fraud following the result of 2010 Presidential election, and with rumours that the TRC was monitoring dissenting content published on Facebook and Twitter.[147]

It was further reported that the TRC would administer controls on Google's search engine.[148] Information Technology experts from China were to travel to Sri Lanka to assist the TRC to implement the new rules.[149] Further, funds from the World Bank were to be used to implement the censorship programme.[150] Subsequently the World Bank issued a statement asserting that there is no scope to utilise World Bank funds for an Internet censorship programme[151] following which the Sunday Times clarified that 'the plan was intended to impose Internet censorship on offensive news websites by introducing regulations on the issue of licences and a fee to operate websites.[152] However, it was also reported that the President has since ordered the suspension of the censorship programme.[153]

With regard to the role that the TRC was to play in any such programme, its Director General Anusha Palpita denied that he had received any directive to take control of news websites.

---

[143] 'Internet and Web Based Citizen Journalism in Sri Lanka,' ICT4Peace, http://ict4peace.wordpress.com/2009/02/25/internet-and-web-based-citizen-journalism-in-sri-lanka/, February 2009.

[144] Sri Lankan government prepares new Internet restrictions, WSWS, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml, 15th February 2010

[145] Ibid.

[146] Ibid.

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Ibid.

[151] B. Muralidhar Reddy, 'World Bank clarifies stand on Sri Lankan Telecom Body', The Hindu, 15 February 2010, http://beta.thehindu.com/news/international/article107208.ece

[152] Bandula Sirimanna, 'Chinese here for cyber censorship', The Sunday Times, 14 February 2010, http://sundaytimes.lk/100214/ News/nws_02.html

[153] Ibid.

However, alarmingly, Palpita acknowledged that 'monitoring could not be ruled out'.[154] Former Director General Rohan Samarajiva questioned the authority of the TRC to implement such a censorship programme. Samarajiva pointed out that under the Telecom Act, the TRC does not have the necessary legal authority. The TRC has at best the authority to licence ISPs. In issuing such licences, the TRC could introduce specific licence conditions about filtering and censorship; however, such conditions may violate the constitution and be the subject of challenge.[155]

Websites that were blocked during the war continue to be unavailable. Websites such as Lankanewsweb.com and tamilcanadian.com/news/ do not operate on Sri Lanka Telecom's ADSL connexion. It has been argued that unlike during the war, the motivations behind the ongoing blocking of such websites are different and exist namely to prevent 'exposure of corruption, abuse of power at the top, revelations of the antics of the royal dynasty, and to hide state atrocities'.[156] However, as with the court sanctioned blocking of pornographic websites, the actual process of blocking is haphazard and some websites though unavailable on an ADSL connexion continue to be available on HSPA.[157]

Surveillance

Disturbing evidence of a broad surveillance regime emerged over the past five years. In February 2009 LTTE air attacks on Colombo, Editor of the Tamil language newspaper Sudar Oli, Nadesapillai Vithyatharan was arrested for assisting the rebels to carry out the attacks.[158] The evidence alleged against Vithyatharan included *inter alia* a telephone conversation between Vithyatharan and his brother-in-law immediately after the air attack on Colombo, during which terms such as 'flight', 'airport', 'flight no', 'date of departure', 'time of departure' and 'arrival' were used.[159] Vithyatharan admitted that he did have a conversation with his brother-in-law where such terms were used. The incident raised interesting questions about the extent of surveillance by the government over Internet and mobile phone communications. How did the law enforcement agencies know the contents of Vithyatharan's telephone conversation? To what extent does the government monitor communications between individuals? What is the capacity of the government to store such information?

The obvious implication in this instance is that the authorities were tapping Vithyatharan's telephone conversations. Presumably Vithyatharan's phone was being tapped given the government's view that his newspaper was sympathetic to the LTTE. These questions are highly pertinent given ongoing speculation about the existence of Government 'hit lists' and plans to monitor any 'malpractice' of human rights activists, lawyers and journalists.[160]

In March 2010, Defence Secretary Gotabaya Rajapaksa responded to the question 'is it ethical for a government to infiltrate in to online privacy of Sri Lankan citizens by gathering information with regard to their political affiliations?' with the following statement:

---

[154] Ibid.

[155] [155] Rohan Samarajiva, 'Quo Warranto TRC?', Lirneasia, 14 February 2010, http://lirneasia.net/2010/02/quo-warranto-trc/

[156] Kumar David, above n 117.

[157] Sanjana Hattotuwa. 'Examples of on-going web censorship in Sri Lanka' ICT for Peacebuilding. 23 February 2010, http://ict4peace.wordpress.com/2010/02/23/examples-of-on-going-web-censorship-in-sri-lanka/

[158] Ravi Nessman, 'Nadesapillai Vithyatharan, Sri Lanka editor, Arrested and Accused of Aiding Rebel Strike', Huffington Post, 26 February 2009, http://www.huffingtonpost.com/2009/02/26/nadesapillai-vithyatharan_n_170168.html

[159] Nadesapillai Vithyatharan Fundamental Rights Application under s 126 of the Constitution, paragraph 35.

[160] BBC, 'Sri Lanka denies 'hit list' charge', BBC, 17 March 2010, http://news.bbc.co.uk/2/hi/south_asia/8571627.stm

> Actually if we could do that it would be good, however as a third world country we don't have that facility. But in all other developed countries they monitor emails, telephone conversations, SMS and people in the streets...Our ID card system is not effective, so we have to introduce a better system... We don't have a closed circuit television (CCTV) surveillance system in Colombo; whereas in all other big cities they are monitored...we can't monitor sms's or emails, we need to have such a system but we don't and are not doing it[161]

Throughout the course of 2010, there have been numerous reports that the Government is monitoring activity on social networking sites. In January 2010, it was reported that the TRC was monitoring Facebook activity as users were allegedly defaming prominent personalities and spreading false rumors about the government.[162] There were also reports that Sri Lankan Army intelligence officials and officers from N.I.B were infiltrating Facebook to collect information on supporters of General Sarath Fonseka and critics of Mahinda Rajapaksa.[163] The idea reportedly came from Defence Secretary Gotabaya Rajapaksa who had previously thought of using Facebook to collect information on foreign supporters of LTTE suspects.[164] In July 2010, it was reported that the Women and Child's Bureau of the Police had received over 50 complaints against Facebook.[165] Among the complaints were allegations that photos on Facebook were being stolen and being turned into 'indecent images'.[166] To date the TRC has responded by stating that they had not received any complaints concerning Facebook. Anusha Palpita, TRC Director General, went so far as to state that 'access to Facebook is a human right so we can't take measures to block the site... if we take measures to block the site, the Internet speed will reduce and this will affect the country's reputation in the technological aspect'.[167]

In consideration of the above, the growth of social media has had a relatively positive impact for freedom of expression in Sri Lanka. With mobile penetration at 80 per cent, it was estimated in March 2011 that of the total number of users accessing the Internet through a mobile device, 42 per cent access Facebook.[168] As noted below, Internet penetration stands at roughly around 13-14 per cent of the population (over 1.7 million users) and there are over 900,000 users on Facebook in Sri Lanka with a majority (78 per cent) in the 18 to 34 age group.[169] The primary assumption when examining the data and trends above is that social media are providing citizens with more means of expression in Sinhala, Tamil and English. However, it is important to note that at the same time social media enables governments to benefit from and implement open source surveillance, particularly if privacy restrictions are not enabled by users in order to prevent the monitoring of content. Nevertheless, the cumulative effect of social media has resulted in the government finding it more difficult to suppress online dissent given the sheer popularity of social

---

[161] 'It's OK for the government to infiltrate online privacy of Sri Lankan citizens?,' ICT4Peace, http://ict4peace.wordpress.com/2010/04/17/its-ok-for-government-to-infiltrate-online-privacy-of-sri-lankan-citizens/, April 2010

[162] Rathindra Kuruwita, 'Facebook users come under scrutiny', Lankanewspapers.com, 31 January 2010 < http:// www.lankanewspapers.com/news/2010/1/53532_space.html

[163] Sri Lankan Guardian, 'Sri Lankan Intelligence Infiltrates Facebook – Gota Behind the Move', Sri Lankan Guardian, 24 February 2010, http://www.srilankaguardian.org/2010/02/sri-lankan-intelligence-infiltrates.html

[164] Ibid.

[165] Indika Sri Aravinda, 'Complaints against Facebook', Daily Mirror, 13 July 2010, http://www.dailymirror.lk/index.php/news/5055- complaints-against-facebook-.html

[166] Ibid.

[167] Ibid.

[168] 'Sri Lanka mobile internet usage poised for growth: Nielsen,' http://www.lbr.lk/fullstory.php?nid=201103041615077468, 4th March 2011

[169] Ibid

networking sites and availability of circumvention tools to access them if there were to be a block. As mentioned earlier, following a brief block on citizen journalism site Groundviews, the site was able to immediately launch emergency protocols that included the activation of a mirror site on WordPress.com, alerting the readership through email, Twitter and Facebook of the site block and immediately switching RSS feeds to a different network architecture that allowed the full content on the site, including comments, to be read even if the SLT ADSL block continued to be in place, and indeed, spread to other ISPs as well.[170] While social media allows for some degree of resistance to restrictions, it does not ameliorate the real threat of governments that might - as a last resort - use physical violence to suppress dissent and other drastic measures such as complete control of ISPs and regulators in order to implement a broader system for monitoring web content and restrict known sources of dissent on the web.

The discussion of the future trends of media highlights the eventual merging of new media and citizen media with mainstream media sources online. In addition, the nature of consumption and production will transform radically into what has already begun with citizens becoming producers of news, audiences fragmenting and news becoming a conversation. Even if the there is a consistent threat to the freedom of expression from the government through intimidation, legal restrictions and arbitrary blocking of web content, the long-term impact of new media on the freedom of expression cannot be discounted. Firstly, there is already an emphasis on communicative rights, where citizens have a right to produce and access a wide and diverse range of information that inform them on the main issues of the day. Secondly, information will eventually be treated as a public good.[171] Thirdly and in congruence with the first point, freedom of expression should not be considered as the right of the media to simply publish or produce, but instead as the ability and right of any individual or organisation to *participate*.[172]

---

[170] Groundviews blocked and unblocked, ICT4Peace, http://ict4peace.wordpress.com/2011/06/22/groundviews-blocked-and-unblocked/, 22nd June 2011

[171] Media Trends and Training in Sri Lanka, http://www.slideshare.net/yajitha/media-trends-and-training-in-sri-lanka, October 2009

[172] Ibid

5. Disconnecting Users from Internet Access, Including on the Basis of Intellectual Property Law

According to CERTCC, there were no cases of cyber crimes associated with the violation of the Intellectual Property Act in 2007. Since then, it is unclear whether CERTCC has been able to act upon cases where intellectual property law has been violated and it is impossible to confirm whether the National Intellectual Property Office of Sri Lanka (NIPO)[173] and the TRC have disconnected users from Internet access on the basis of intellectual property law or for other reasons. However, the broad provisions of the Intellectual Property Act No. 36 of 2003 do allow for the Court to prevent infringement by granting an injunction against an offender or provide the 'necessary' order for preventing an act of intellectual property right infringement from being committed. They key aspects of the legislation are highlighted below:

> (2)(a) The Court shall have power and jurisdiction—
>
> (i) to grant such injunctions to prohibit the commission of any act of, infringement or the continued commission of such acts of infringement of any right protected under this Part;
>
> (e) Where there is a danger that acts of infringement may be continued, the court shall make such orders as may be necessary prevent such acts being committed.
>
> (f) The provisions of Chapter XXXV of this Act relating to infringement and remedies shall apply, *mutatis mutandis,* to rights protected under this Part.
>
> (g) Any person who infringes or attempts to infringe any of the rights protected under this Part shall be guilty of an offence and on conviction be liable to any penalty as provided for in Chapters XXXVIII and XLI of the Act.[174]

It is worth noting that the Act does not provide for an explicit disconnection of Internet access as a penalty for infringement, and instead favours the payment of damages to an aggrieved party in such an instance of intellectual property right infringement. However, due to the broad nature of the provisions of the Act, any developments with regard to injunctions and penalties imposed for the violation of the Act should be closely monitored. If cases of intellectual property right infringement occur in the future on the Internet, it would be beneficial if NIPO and the TRC as well as other relevant government authorities consider a method of intellectual property rights enforcement that does not make disconnection of Internet access a final penalty, and instead abides by international standards of enforcement with the ultimate priority being the recognition of Internet access as a fundamental human right.

---

[173] National Intellectual Property Right Office of Sri Lanka, http://www.nipo.gov.lk/about.htm

[174] Intellectual Property Right Act No. 36 of 2003, p. 22-3

6. Cyber-attacks

The number of cyber threats in Sri Lanka is on the rise with 151 incidents reported in 2010 and 681 incidents that were reported so far this year.[175] Most of these incidents involve privacy breaches on social media and email accounts, and CERT CC (Computer Emergency Readiness Team and Coordination Centre) - a subsidiary of the ICT Agency of Sri Lanka (ICTA) established to respond to cyber-attacks and strengthen existing security systems against potential attacks - stated that the threats include,

> malware (viruses), phishing (automated targeted emails, SMSs, Skype, faxes and other channel abuse where users are directed to malicious sites), abuse of or infringing on the privacy of personal online accounts, defacement of websites, scams such as Green Card lottery emails, etc., threatening or hate mail, and unauthorised access at places of business.[176]

At present CERT CC consider the rise to be in line with international trends and indicated that emphasis should be placed on ensuring secure networks for financial transactions in order to prevent fraud and identity theft. It has been proposed that a separate emergency response team should be established, which would monitor cyber threats to the financial sector so as to 'share vulnerabilities that come up with the entire industry.'[177] Even though Sri Lanka's cyber-security strategy is focussed on maintaining a robust 'defensive' capability[178] in order to pre-empt potential attacks, it is unclear whether CERT CC have plans in the future to track down sources of cyber-attacks in cooperation with international cyber-action teams and other global strategic initiatives for cyber security.[179]

The most reported cases of cyber-attacks in Sri Lanka have been largely linked to politically motivated attacks and the battle against cyber terrorist networks, which has - at least to a certain extent - been repositioned as an external rather than an internal threat after the end of the war. In February 2011, the Sri Lankan Army Commander, Lieutenant General Jayasuriya, revealed that during the latter stages of the war against the LTTE, the website of the Sri Lankan Army had encountered what was described as a 'web defacement attack' and that there are continued efforts to hack into security networks, which have been prevented.[180] An important development in the present post-war period has been the need to ensure an adequate shift in defensive capability from physical to cyber-space in order to prevent what is described as 'false propaganda' disseminated by 'anti-Sri Lankan and LTTE activists'. The government has recognised the 'possibility of attacks on the computers with vital information such as financial networks of the country' as well as the need to 'maintain updated security systems and to continuously monitor those systems externally and internally to ensure that there are no loopholes or vulnerabilities.'[181]

---

[175] 681 SL cyber security incidents so far in 2011, The Sunday Times, http://www.sundaytimes.lk/111016/BusinessTimes/bt31.html, 16th October 2011

[176] Ibid.

[177] Ibid

[178] Ibid.

[179] Federal Bureau of Investigation (FBI), Cyber security, http://www.fbi.gov/about-us/investigate/cyber/cyber

[180] Sri Lanka Army commander says Cyber War still continues, http://www.colombopage.com/archive_11/Feb22_1298388902CH.php, 22nd February 2011

[181] Ibid

Following the emergence of Anonymous[182] 'hacktivists' during the Egyptian revolution and the launch of DDoS attacks against the websites of various Egyptian ministries and institutions[183], in August 2011 the Sri Lankan branch of Anonymous claimed to have hacked into the DNS servers of Symantec, Facebook, Apple, Microsoft and various other international organisations.[184] In addition, the group also claimed to have carried out several DNS attacks against 'agencies in Sri Lanka, including the nation's Parliament, military, and largest telecom provider.' CERT CC[185] responded by stating that the claims of Anonymous were unfounded as the organisation had not provided any evidence to suggest that 'DNS poisoning attacks' had been carried out against the specific severs of state institutions.[186] The reasons behind the alleged attack are not dissimilar to the case detailed above with regard to the attempted hacking of the Army's network. Anonymous Sri Lanka highlighted social, political and economic exploitation and corrupt establishments among many other issues as the *raison d' etre* of its group.[187]

Even if the claims above are questionable, the activities of such groups present a clear threat to the freedom expression, particularly if they target social media websites and communication tools - such as Skype - that have assisted in strengthening the freedom of expression, and opposition to authoritarian politics in the country. It also presents the government with an added reason to build-up more sophisticated surveillance systems in order to monitor web activity and strengthen security systems, which might have an adverse impact if manipulated in order to suppress dissent in the country. There is also nothing to prevent the establishment of counter-organisations/ movements that would lead to the risk of cyber-warfare and another risk is that the websites of organisations that work on human rights, justice and corruption could face cyber-attacks as well. As the Special Rapporteur's report notes,

> …determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult…it should be noted that States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression.[188]

While cyber-attacks violate the provisions of the Computer Crimes Act, which are examined in Chapter 6, the principle of proportionality and necessity would apply to any action undertaken by the government or law enforcement agency. In this regard, Jayantha Fernando of ICTA notes that,

> Any criminal investigation interferes with the rights of others, whether the person is the subject of an investigation or a related third party. In a democratic society any such interference must be justifiable and proportionate to the needs of society sought to be protected. However, the growth of network-based crime has raised difficult issues in respect of the appropriate balance between the needs of those investigating and

---

[182] For further information, on the Anonymous 'hacktivist group,' please visit http://en.wikipedia.org/wiki/Anonymous_(group)

[183] Anonymous 'hacktivists' attack Egyptian websites, MSNBC, http://www.msnbc.msn.com/id/41280813/ns/technology_and_science-security/t/anonymous-hacktivists-attack-egyptian-websites/#.To61J-v8_Kw, 26th January 2011

[184] Anonymous claims DNS attacks against Symantec, Apple, Microsoft, CNet News, http://news.cnet.com/8301-1009_3-20099841-83/anonymous-claims-dns-attacks-against-symantec-apple-microsoft/, 31st August 2011

[185] For further information on CERT|CC and its constituency, please visit http://www.cert.lk/cons.html

[186] Fake hacking incidents reported. CERT|CC, http://www.cert.lk/news.html

[187] Anonymous Sri Lanka goes public – Press Release, http://pastebin.com/WZsgSniV, 31st August 2011

[188] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations Human Rights Council (UNHRC), Seventeenth Session, 16th May 2011

prosecuting crime, and the rights of users of such networks.[189]

[189] Jayantha Fernando, 'Cybercrime Legislation – Sri Lankan Update,' ICTA

7. Inadequate Protection of the Right to Privacy and Data Protection

The Internet along with other information communication technologies has increased the possibility of information or data being intercepted and being placed in the hands of unintended parties.[190] As a result, it is necessary to have strong privacy laws to protect users of the Internet and other information communication technologies. Under the Roman Dutch common law of Sri Lanka, the Courts have recognised a right to privacy in limited circumstances. Various legislative enactments that prohibit surveillance and other forms of intercepting communications also provide some legal basis for protecting individual privacy. However, the Sri Lankan Constitution does not provide for a right to privacy. Nonetheless, it may be possible to read a right of privacy in to the Sri Lankan Constitution through a broad interpretation of other closely related rights such as freedom of expression and freedom of movement. In this regard, the jurisprudence of India is considered, where despite the lack of express recognition of a right to privacy, the Indian Courts have recognised such a right under the right to liberty. In addition, jurisprudence from South Africa is considered where there is both a common law right and a constitutional right to privacy.

It is important not to underestimate the possibilities of surveillance. Currently mobile phone users cannot only fall prey to someone snooping in to the contents of their mobile phones but also using their mobile phones to discover where they are at any given moment of the day. Worse still, such information is not just available to government authorities or telecommunication service providers. Almost anyone can access information, especially information with regard to an individual's location at any given point. In England, for a prescribed fee, a company allows individuals to monitor the movements of 'your friends and family' on your own computer.[191] 'Consent' is obtained by getting the person who is being subject to the surveillance to send a text message approving a request to be traced.[192] No further efforts are made to see if in fact the actual owner of the mobile phone did consent, or some third party agreed to the request to be traced.[193] More worryingly, there are surveillance expert companies that are developing ways to better investigate and analyse the content of information communicated, and are selling this technology to governments around the world regardless of concerns about their human rights record.[194]

Privacy is not a constitutionally protected right in Sri Lanka. However, the Courts have recognised a right to privacy under the common law of Sri Lanka. Under the Roman Dutch law individuals can bring an action for injury under the *actio iniuriarum*. The Courts have recognised a right to household privacy among adjoining landowners to protect his fence with the covering of ola leaves.[195] Similarly the courts have recognised that an owner of an estate or a superintendent has no right to enter the labourer's lines and invade his privacy. The Supreme Court in an appeal[196]

---

[190] Althaf Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective', Scripted 5(3): 553-574, p 558.

[191] Daniel Soar, 'Short Cuts', London Review of Books, 14 August 2008, http://www.lrb.co.uk/v30/n16/daniel-soar/short-cuts

[192] Ibid.

[193] Ibid.

[194] Sanjana Hattotuwa, 'Deciding which mobile phone to bug and how: the incredible flipside of the growth of mobile phones'. ICT for Peacebuilding. 25 August 2008, http://ict4peace.wordpress.com/2008/08/25/deciding-which-mobile-phone-to-bug-and-how-the- incredible-flip-side-of-the-growth-of-mobiles/

[195] Chinnapa et al v Kanakar et al 13 NLR 157 at 158-160.

[196] A.M.K. Azeez v W.T. Senevirathne (SI Police) 69 NLR 209, 210.

from a Magistrates' Court where a husband and wife were convicted of insulting police officers who had entered their house, reduced the sentence of the appellants taking into consideration the circumstance in which the comments were made (namely that the police entered well after midnight and the privacy and the sleep of the appellants were disturbed).[197]

In Sinha Ratnatunga v The State (2001) 2 SLR 172, the editor of the Sunday Times was indicted on two counts for defamation under s 480 of the Penal Code and s 15 of the Sri Lanka Press Council Law. Sunday Times reported that the President had attended the birthday part of a male Member of Parliament in a prominent Colombo hotel and that she stayed until the early hours of the morning. In its reasoning, the Court recognised the importance of the right to privacy as follows:

> The press should not think they are free to invade the privacy of individuals in the exercise of their constitutional right to freedom of speech and expression, merely because the right to privacy is not declared a fundamental right of the individual[198]
>
> ...The press should not seek under the cover of exercising its freedom of speech and expressions make unwarranted intrusions in to the private domain of individuals and thereby destroy [his] right to privacy. Public figures are no exception. Even a public figure is entitled to a reasonable measure of privacy. Therefore Her Excellency the President even though she is a public figure is entitled to a reasonable measure of privacy to be left alone when she is not engaged in the performance of any public functions.
>
> There is a no entry zone which the press must not trespass. The case in hand is one where the press has attempted to enter that no entry zone.[199]

However, recognition of the right to privacy in these limited circumstances is not sufficient to cover the numerous ways the Internet can breach a user's privacy. Furthermore, in order to bring an *actio iniuriarum* action many requirements must be satisfied making it a restrictive means of redress. It has been suggested that Sri Lanka expand its privacy jurisprudence by interpreting other closely related fundamental rights to include a concept of privacy.[200] For example, the right to freedom of expression could be expanded to include a right to privacy.[201] If an individual only intends to communicate with a selected recipient then third parties should not have access to the contents of the communication.[202] To take an Internet example, if a website only permitted access to those whom had been given permission to do so, a hacker that gains unauthorised access would be violating the 'privacy' of the website owner.[203] Alternatively it could be argued that privacy is inherent in the right to freedom of movement, and surveillance mechanisms inhibit one's freedom to move.[204] Using such reasoning it has been suggested that an Internet user should also have a right to free movement (to surf the web) freely and without fear, and mechanisms such as spyware, web bugs, cookies would impede this right of 'movement.'[205]

---

[197] Althaf Marsoof, above n 300, p 558.

[198] Sinha Ratnatunga v State, 2 SLR 172, at 212.

[199] Sinha Ratnatunga v State, 2 SLR 172 at 213.

[200] Althaf Marsoof, above n 300, p 570.

[201] Althaf Marsoof, above n 300, p 571.

[202] Ibid.

[203] Ibid.

[204] Ibid.

[205] Althaf Marsoof, above n 300, p 571.

Legislative Framework

To date the government has not introduced any specific legislation that protects individual privacy or collection of personal information. The Telecom Act and Computer Crimes Act No 27 of 2007 touch on these two areas, and both are in turn considered below. There have been two other pieces of legislation the Information and Communication Technology Act No 27 of 2003 (ICT Act) and the Electronic Transactions Act No 19 of 2006 (Electronic Transactions Act) that concern information communication technologies. The ICT Act provides for the establishment of the Information and Communication Technology Agency (ICTA). ICTA is given chief responsibility for implementing a national policy on ICTs. The Electronic Transactions Act seeks to facilitate transactions related to e-commerce.

In addition to these legislative measures, the government has also sought to launch an 'e-Sri Lanka programme' which seeks "to adopt ICT in all its aspects to make government more efficient and effective, improve access to government services and create a more citizen centric government."[206] The government has been criticised for attempting to introduce such a programme in absence of a data protection law or privacy protection for individuals.[207] In any event, the 'e-Sri Lanka program' seeks to adopt the EU data protection regime in the form of a 'Data Protection Code of Practice' with the possibility that the Code be replaced by regulations issued under the ICT Act.[208]

Telecom Act

In Sri Lanka privacy protection prohibiting surveillance can be found in several legislative enactments. Section 47 of the Telecom Act, *inter alia*, makes it an offence for any person with intent to prevent or obstruct the transmission of any message; or interrupt or acquaint themselves with the content of any message. 'Message' is defined broadly to include any communication sent or received or made by telecommunication.[209] 'Telecommunication' is defined as the making of any transmission, emission or reception of signs, signals, wilting, images, sound or intelligence of any nature by optical means or by wire or radio waves or any other electromagnetic system.[210] The section clearly encompasses text messages and telephone conversations, and it may also apply to email messages. Section 52 of the Telecom Act makes it an offence for any person, without lawful authority, to intrude, interfere or unlawfully learn the contents of any message or its usage information. Section 53 makes it an offence for any person to willfully seek to intercept and improperly learn the contents of any telecommunication transmission. Section 54(1) makes it an offence for telecommunications officers or any person with official duties in connexion with a telecommunication system to intentionally intercept a message or disclose the contents of any message or its usage information. However, it is not an offence if messages are intercepted or their contents are disclosed pursuant to a direction given by the Minister. Under s 54(3) it is an offence for a telecommunication officer to reveal to any person the contents of a statement of account specifying what telecommunication services are provided to any other person. However, it is not an offence to do so where such details are revealed in connexion with a criminal investigation.[211] For the purposes of Sections 52 and 54, 'usage information' means information relating to the identity of calling or called subscriber.

---

[206] Information Communication Technology Agency (Sri Lanka) (ICTA). Policy and Procedures for ICT Usage in Government (e- Government Policy), 2 December 2009 <http://www.icta.lk/attachments/759_ICT_Policies_and_Procedures_for_Government_V_9_English_Jan_08_2010.pdf>

[207] Privacy International, 'Republic of Sri Lanka', Privacy International, 18 December 2007 <http://www.privacyinternational.org/ article.shtml?cmd[347]=x-347-559488#[21]>

[208] ICTA, above n 319.

[209] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 73.

[210] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 73.

[211] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54(4).

However, the Telecom Act has also been the subject of criticism as several provisions potentially serve to undermine privacy. For example, there are several offences in the Telecom Act that make it an offence for an employee of a telecommunication service provider to *inter alia* interfere with the contents of any message,[212] or intercept any message.[213] However, the Act provides that it is a defence to these offences if the employee were to do so in the 'pursuance of official his duty'[214], 'as directed by a court'[215], under 'a direction of the Minister'[216], 'in connection with the investigation of any criminal offence'[217] or 'for the purpose of any criminal proceeding'[218]. Critics have raised questions about the ambit of these defenses. For example, what are the permitted circumstances under which an employee of a telecommunication service can intercept or interfere with the contents of messages?[219] Under what circumstances can a Minister issue a direction to interfere or intercept a message?[220] What guidelines inform a Minister's decision? Do employees of a telecommunication service have any capacity to refuse a Minister's direction? [221] Especially if such a direction appears to be an unreasonable intrusion into an individual's privacy, serving no particular public purpose? Is there any way to challenge a Minister's direction? Who can issue directions to employees of telecommunication services in connexion with the investigation of any criminal offence or for the purpose of any criminal proceedings?[222] What level of authority would be required? Do such directions have to be in writing or merely verbal?[223] Can employees of telecommunication services, for the purpose of criminal proceedings or investigation of any criminal offence, intercept or interfere with messages of their own accord?[224] Finally, to what extent are customers adequately informed that their communications might not be private?[225]

In light of these questions, there have been calls for the Government together with the TRC to formulate regulations, guidelines and best practices to direct service providers to uphold the privacy of consumers.[226] Disclosure policies and any amendments to such policies should be made public so that consumers are fully informed.[227] Circumstances where a Minister may issue directions to intercept or interfere with communications must be clarified to operators and

---

[212] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 49.

[213] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54.

[214] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 49(c).

[215] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 49 (C).

[216] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54(3).

[217] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54(3).

[218] Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54 (3).

[219] Chandra Jayaratne, An extract of a note on protecting personal information, Email Message to Sanjana Hattotuwa, sent 4 April 2010.

[220] Ibid.

[221] Ibid.

[222] Ibid.

[223] Ibid.

[224] Ibid.

[225] Ibid.

[226] Chandra Jayaratne, Guest Column Article for Daily FT on Law promotes wire taps and cyber crimes! Business privacy at risk?, [Email] Message to Sanjana Hattotuwa, sent 7 May 2010.

[227] Ibid.

published in the gazette so that consumers are fully informed of the limits to their privacy.[228] Similarly, circumstances where employees of telecommunication service providers may make disclosures in connexion with criminal investigations or criminal proceedings should be published, and actual instances of cooperation should be notified to the TRC.[229] A further recommendation was that the TRC should monitor and/or enforce such regulations and guidelines in order ensure privacy of consumers.[230]

Computer Crimes Act No.24 of 2007

Further, the Computer Crimes Act introduced numerous offences to protect computer users from unauthorised access to computers and unlawful interception of data. Provisions of the Computer Crimes Act apply where,

a) A person commits an offence while being present or outside of Sri Lanka;
b) The computer, computer system or information affected or information which was to be affected was in or outside of Sri Lanka;
c) The facility or service including any computer storage or data or information processing service, used in the commission of an offence was present in or outside of Sri Lanka; or
d) Loss or damage caused by the offence is caused to a person in or outside of Sri Lanka.

Section 3 of the Computer Crimes Act makes it an offence to hack into a computer. The section provides that where a person intentionally secures access to a computer or any information held in any computer knowing or having reason to believe that he has no lawful authority to secure such access commits an offence. Under this section, sending out a virus that gathers information on a person's computer or programme and reports it back would amount to a hacking offence.[231] As noted above, using cookies to collect information can be an infringement of privacy. Under this section it will also be an offence to send a cookie to a computer through the Internet and gather information held in a computer (such as the user's liking or disliking of websites) where it happens without the authority of the user. However, most web designers get around this by inserting a disclaimer clause, which states that the user must agree to in order to access the website.[232] Section 4 of the Computer Crimes Act makes it an offence to 'hack' in to a computer. Section 4 applies where,

a) a person secures access to a computer or any information held in any computer;
b) knowing or having reason to believe that he has no lawful authority to secure such access; and
c) does so with the intention of committing an offence under the Computer Crimes Act commits an offence.

Under this section activities such as phishing would be made illegal.[233]

Section 5 makes it an offence to cause a computer to perform a function without lawful authority. Section 5 provides that it is an offence for a person to cause a computer to perform any function, intentionally and without lawful authority, with the knowledge or having reason to believe that the function will cause unauthorised modification or damage of any computer, computer system or programme. The Computer Crimes Act provides that examples of unauthorised modification or damage or potential damage to any computer include the following:

---

[228] Ibid.

[229] Ibid.

[230] Ibid.

[231] Sunil Abeyaratne, Introduction to Information and Communication Technology Law (2008), p 94.

[232] Ibid, p 95.

[233] Ibid.

1. a) impairing the operation of any computer, computer system or the reliability of any data or information held in any computer; or
2. b) destroying deleting or corrupting or adding moving or altering any information held in any Computer; or
3. c) makes use of computer service involving computer time and data processing for the storage or retrieval of data; or
4. d) introduces a computer program which will have the effect of malfunctioning of a computer or falsifies the data or any information held in any computer or computer system.[234]

Further, the Act provides that for the purposes of any of the scenarios envisaged above, it is immaterial whether the consequences were of a temporary or permanent nature. Viruses or botnets transmitted over the Internet would fall foul of this section.

Section 8 provides that it is an offence to knowingly and without lawful authority intercept any subscriber information, traffic data, or any communication to, from or within a computer or any electromagnetic emissions from a computer that carries any information.[235] Subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its service. Service provider is defined as a public or private entity, which provides for the ability for its customers to communicate by means of a computer system and any other entity that processes or stores computer data or information on behalf of that entity or its customers.[236] Traffic data means 'data that relates to attributes of a communication by means of a computer system; data generated by a computer system that is part of a service provider; and which shows communication origin, destination, route, time, data, size, duration or details of subscriber information'.[237] Therefore, anyone who monitors an Internet user could be in violation of the Act. Computer is defined so broadly and covers any electronic device with information processing capabilities. Thus, it has been suggested that a service provider of a mobile phone who intercepts any transmissions from the mobile phone would be committing an offence under the Act.[238]

Further, the Act makes it an offence for any person - without legal authority - to use any device including a computer, computer program, a computer password, access code or similar information to commit an offence under the Computer Crimes Act. It is also an offence for any person to disclose any information that enables the access to a service provided by a computer without express authority.[239]

However, there have been numerous criticisms of the Computer Crimes Act. Former Chief Justice Silva has stated that more than three quarters of cases under the Act end up without convictions or not being investigated.[240] Chief Justice Silva criticised the ability of the police to detect and investigate computer crimes.[241] Many judges themselves are computer illiterate, but it is understood that training programmes were underway to improve computer literacy.[242] Ironically, certain investigative provisions under the Computer Crimes Act have been criticised for intruding

---

[234] Ibid.

[235] Computer Crimes Act No 24 of 2007 (Sri Lanka), s8.

[236] Computer Crimes Act No 24 of 2007 (Sri Lanka), s38.

[237] Computer Crimes Act No 24 of 2007 (Sri Lanka), s38.

[238] Sunil Abeyaratne, Introduction to Information and Communication Technology Law (2008), p. 102

[239] Computer Crimes Act No 24 of 2007 (Sri Lanka), s 10.

[240] Lanka Business Online, 'Crime Alarm', Lanka Business Online, 29 January 2009, http://www.lankabusinessonline.com/ fullstory.php?nid=257786312

[241] Ibid.

[242] Ibid.

on individual privacy. Section 18 allows an expert or a police officer involved in an investigation under the Act to tap any 'wire or electronic communication' or obtain any information (including subscriber information and traffic data) from any service provider. A warrant is required from a magistrate to authorise the tapping. However, it has been suggested that this is not a sufficient safeguard given that first, 'warrants are available for the asking'[243] and second, the requirement of a warrant can be dispensed with in cases of urgency.[244]

[243] Sunil Abeyaratne, Introduction to Information and Communication Technology Law (2008), p. 558

[244] Computer Crimes Act No 24 of 2007 (Sri Lanka), s 1

8. Internet Access

Physical level

According to the United Nation's International Telecommunications Union, in 2010 there were 71.6 Internet users per 100 inhabitants in developed States whereas only 21.1 Internet users per 100 inhabitants in the developing states.[245] Similarly just over fifty percent of the developing world had access to a mobile phone in comparison to the developed world where nearly a hundred percent of the population had access.[246] In this regard Sri Lanka is illustrative - as of 2009 only five and a half percent of the population has access to the Internet[247] whereas over seventy percent of the population has access to mobile phones.[248] Economic wealth, lack of basic infrastructure (e.g. lack of cheap, reliable accessible electricity), high cost of telecommunications, and the lack of basic education and technical expertise all affect a government's ability to provide access to the Internet. In addition to these factors, Sri Lanka's thirty-year-old civil war prevented the expansion of telecommunication infrastructure, especially to the northern and eastern parts of the country.

It is worth noting that the TRC recently unveiled a programme to launch WiFi zones across the country in order to increase local accessibility to the Internet. Director General of the TRC highlighted that the specific WiFi zones will be located in 'Colombo City, the area around the Bandaranaike International Airport as well as the routes to Colombo, the coastal areas between Beruwala and Hambantota, and Arugam Bay and Trincomalee."[249] The programme marks a positive step towards fulfilling universal access to Internet and providing the necessary infrastructure to narrow the gap presented by the digital divide. As the cross-regional statement at the HRC notes,

> Recognizing the global nature of the Internet, we share the key objective of universal access. Internet is a formidable force in generating development and promoting economic, social and cultural rights, and the present digital divide must be bridged to enable participation of all.
>
> All users, including persons with disabilities, should have greatest possible access to Internet-based content, applications and services, whether or not they are offered free of charge. In this context, network neutrality and openness are important objectives. Cutting off users from access to the Internet is generally not a proportionate sanction.[250]

---

[245] "Key Global Telecom Indicators for the World Telecommunication Service Sector," International Telecommunication Union, 21 October 2010.

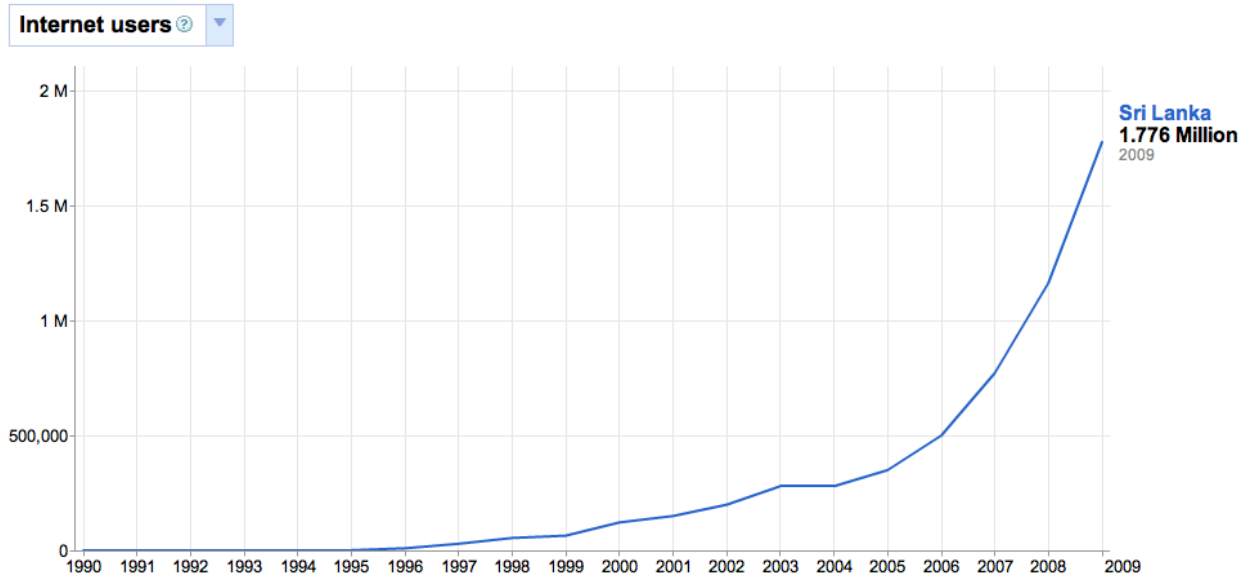
[246] Ibid.

[247] Internet World Stats Usage and Population Statistics, http://www.internetworldstats.com/asia/lk.htm

[248] Telecommunications Regulatory Commission of Sri Lanka, June 2009 Statistics, http://www.trc.gov.lk/information/statistics.html

[249] Lanka to get WiFi zones, Sunday Times, http://sundaytimes.lk/110731/News/nws_14.html, 31st July 2011

[250] Freedom of Expression on the Internet, Cross-regional Statement, Human Rights Council 17th session, 10th June 2011



Source: Google Public Data Explorer; Data from World Bank, World Development Indicators

As the Special Rapporteur's report notes,

> …without Internet access, which facilitates economic development and the enjoyment of a range of human rights, marginalized groups and developing States remain trapped in a disadvantaged situation, thereby perpetuating inequality both within and between States… The Internet offers a key means by which such groups can obtain information, assert their rights, and participate in public debates concerning social, economic and political changes to improve their situation.

A common barrier hindering access at the physical level is government imposed Internet related licensing and registration requirements. As noted previously, it was reported that the government planned to introduce a requirement that all online news websites register with the Telecommunications Regulations Commission (TRC).[251] However, the government later announced that these plans were not going to be implemented.[252]

In July 2011, it was revealed that China's telecommunications and software corporation, ZTE, was awarded a contract by Sri Lanka Telecom's mobile subsidiary, Mobitel, for the 'deployment of 4G Long-Term Evolution mobile broadband infrastructure.'[253] The possibility of ZTE's involvement in Sri Lanka's network infrastructure development does, however, raise concerns over more pervasive surveillance techniques, and the possibility of better, more coordinated, network command and control expertise transfer from mainland China. At a very basic level, it would allow the Government of Sri Lanka to listen into and precisely locate subscribers to the service. In short, though China's involvement in Sri Lanka's network development does not make mobile communications any less secure than it already is and will bring broadband to millions who do not currently enjoy it, it will make it that much easier for any Government to use - with impunity - increasingly sophisticated ways to listen in, and if necessary, censor and curtail what is perceived to be 'unpatriotic' communications, dissenting narratives published online and target websites, blogs and social networks utilised by opposition groups to organise dissent against the Government.

---

[251] Lankanewsweb, Government to block Internet in Sri Lanka, 10 February 2010 http://www.lankanewsweb.com/news/ EN_2010_02_10_013.html

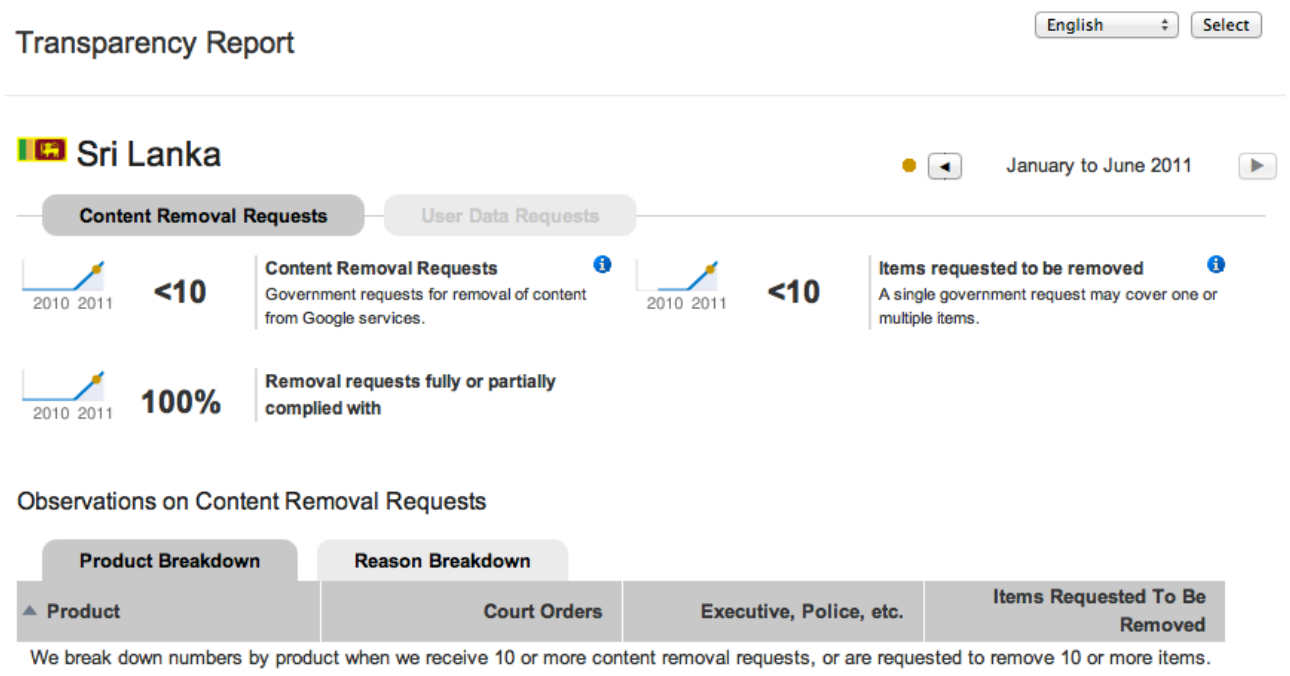
[252] Bandula Sirimanna, 'President halts cyber censorship', The Sunday Times, 21 February 2010, http://sundaytimes.lk/100221/News/ nws_05.html

[253] ZTE secures Sri Lankan LTE deal, TeleGeography, http://www.telegeography.com/products/commsupdate/articles/2011/07/19/zte-secures-sri-lankan-lte-deal/, 19th July 2011.

The case for monitoring and imposing restrictions on Internet and web communications in the interests of protecting public order and national security though entirely justified is not without its inherent difficulties. In such contexts, details of such measures are crucial and especially in countries like Sri Lanka where the government already has a poor record on freedom of expression and privacy. In particular, it is important to keep in mind the context in which these measures are being carried out. In Sri Lanka, laws are made in a culture of secrecy and there is very little opportunity to meaningfully influence the law making process. A disconcerting trend in the country is that what is often legal and permissible and what happens in reality are two different things. Given the growing global trend towards greater regulation, it is important for countries like Sri Lanka with poor records on civil liberties to be vigilant and if possible buck the trend.

Application level

The applications layer refers to the applications; for example, software and search engines that are used to navigate the Internet. For example, search engines such as Google and computer software like Internet Explorer or Firefox fall within this category. A key issue is that if a few applications monopolise the market then they are given a significant amount of influence over the content that is accessed by users. For example, Google is the most widely used search engine in the world, thus it exercises disproportionate influence on what information is accessed by users on its search mechanism. These applications are being regulated by both Governments and the applications themselves. Governments around the world are attempting to regulate these applications by placing surveillance on their use and forcing application owners to regulate the content. Browser and software owners themselves have their own terms and conditions both expressly disclosed and hidden that undermine the freedom with which users can navigate the Internet.



Screenshot from http://www.google.com/transparencyreport/governmentrequests/LK/

The screenshot above detailing the number of content and item removal requests by the Sri Lankan Government to Google is quite revealing with respect to the sharp rise from mid-2010 to 2011, which is line with reportage from that period detailing the Government's own efforts to increase regulation, monitor online content and filter content that is considered offensive. It is worth stressing that further monitoring of Google's Transparency Report is required in order to respond to a potential rise in take down requests by the Government in the future. This would enable civil society organisations to ensure that there is a sustained effort to find out what content

was removed and carry out adequate reportage on the matter, particularly if there is an exponential increase in requests.

Other than under direct government requests, browsers and software applications themselves have their own terms and conditions, which users must comply with. For example Yahoo's Geocites require users not to publish anything that is harmful, threatening, abusive, harassing or otherwise objectionable.[254] More worryingly there can be hidden features or terms and conditions that are not expressly disclosed that can undermine the freedom with which a user can navigate the Internet. For example, there has been speculation that Skype (an Internet based telephone service), widely used by human rights activists including in Sri Lanka, allows third parties back door access to listen in on communications between users.[255] This was followed by news reports in July 2010 that Skype's ultra-secret and complicated encryption protocols had allegedly been hacked into,[256] which immediately led to concerns that any compromise in Skype's security architecture would have significant implications for those human rights activists and journalists working on research, advocacy and activism on human rights violations and information with regard to corruption within the government in Sri Lanka. Despite the threat that this represents to human rights activists who use Skype to relay sensitive information, it is still extremely complicated, though not entirely impossible, for the Government of Sri Lanka to build a surveillance programme based on encryption protocols that are made public. Skype still remains the most secure means of communication currently available, particularly when dealing with sensitive information, and a vital tool for human rights work in the country.

---

[254] Article 19, above n 7.

[255] Daniel AJ Sokolov, 'Speculation over back door in Skype', The H, 24 July 2008 <http://www.h-online.com/newsticker/news/item/ Speculation-over-back-door-in-Skype-736607.html>

[256] Skype's Innermost Security Layers Claimed to be Reverse-Engineered, TechCrunch, http://techcrunch.com/2010/07/08/skypes-innermost-security-layers-claimed-to-be-reverse-engineered/, 8th July 2010

Conclusion

In Sri Lanka, the censorious attitudes towards media freedom and the freedom of expression more generally are increasingly evident in the online sphere. The insidious attempts to regulate online content; block websites; the attacks on journalists over content published or republished online and repeated statements from government officials threatening those who provide alternative and dissenting views do not bode well for the future of online freedom of expression in the country. Further, despite the end of war, freedom of expression in Sri Lanka remains weak, and under siege. To date, there has been no satisfactory response from law enforcement agencies to any of the attacks on online journalists or websites. Attempts by human rights organisations and media watchdogs to condemn such violence and other moves that restrict freedom of expression have been dismissed as the work of 'western' agents, conspirators, terrorists and traitors.

Internet, mobile and web consumers need to be cautious of attempts to ban online pornography and more general bans on 'indecent advertising' as concerns about 'decency' could be the start of a slippery slope towards a wider and more invasive censorship programme. Internet filters established at the level of Internet Service Providers (ISPs) to remove pornography today can be used to curtail and censor political dissent tomorrow. It is important that consumers remain vigilant about such possibilities given the existing socio-political climate that has little tolerance for alternative views or values. Further, the concerns about decency and morality ultimately represent an effort by the government to impose certain kinds of values on the citizenry. The concerns about decency and morality are part of a larger debate about 'culture' and 'family values' as defined by the government. Rather than enforcing 'values' as determined by the government, what is more important is that citizens have the freedom to choose whatever values that best suit them and are provided the right to participate in policy-making, including via online participatory platforms.

The restrictive legal framework in Sri Lanka compounds the impact of this culture of intolerance and impunity. The Sri Lankan Constitution, despite providing a freedom of expression guarantee, is subject to numerous limitations. These restrictions need not be 'reasonable' or 'necessary' as is the standard under the ICCPR. Moreover, Article 16 of the Sri Lankan constitution undermines the protection afforded by the any of the constitutional rights, as it provides that all other laws, though inconsistent with the Constitution, shall remain valid and operative. This is especially worrying in the context of the freedom of expression guarantee, as there are a host of laws that currently restrict the discussion of socially and politically relevant content. Despite being the subject of international condemnation, draconian legislation like the PTA continues to be tool of oppression that criminalises political dissent.[257][258] Similarly, other legislation like the Parliamentary Privileges Act and the Press Council Law inhibit discussion of vital policy-making by the government. The application of such laws to the online sphere has not yet been tested in Sri Lanka. However, a growing number of global examples illustrate that these laws can often have unintended consequences for the online sphere. Therefore, the mere existence of legislation that may be potentially used to restrict the freedom of expression warrants concern.

To date, the Courts have not had an opportunity to decide on the application of the freedom of expression guarantee to the online sphere. Thus, there is uncertainty as to the extent to which freedom of expression in the online sphere is constitutionally protected in Sri Lanka. The Supreme Court has recognised that free speech applies regardless of the mode used to express one's ideas. The Court has also recognised that the free speech guarantee protects traditional journalists from arbitrary interference and physical attacks. These decisions can be used to base an argument that freedom of expression guarantee can be applied to the online sphere. In

---

[257] CPA Statement On The Termination Of The State Of Emergency, http://cpalanka.org/cpa-statement-on-the-termination-of-the-state-of-emergency/, 28th August 2011

[258] CPA Statement on the new Regulations under the Prevention of Terrorism Act, http://cpalanka.org/cpa-statement-on-the-new-regulations-under-the-prevention-of-terrorism-act/, 23rd September 2011

particular, decisions concerning the rights of journalists can be used to argue that online journalists who publish in the online sphere should also be protected.[259] However, it remains to be seen whether bloggers will receive the same protection. A larger concern is that Sri Lankan Courts have a poor record when it comes to interpreting national security legislation that restrict fundamental rights. Too often in the past, the Courts have allowed national security concerns to limit freedom of expression. Thus, despite the protection afforded by the Constitution, it remains constrained by the constitutional text itself and conservative interpretations by the Courts.

Finally, despite the growth of ICTs in Sri Lanka, the government has failed to provide adequate privacy protection for those who use these new mediums. Currently there is no constitutional right to privacy in Sri Lanka. There is a weak legislative framework that protects users from instances of surveillance. However, these laws also grant significant power to law enforcement agencies, service providers and the relevant Minister to intercept communications. There are no guidelines, or procedures as to how and when these powers can be exercised.

In consideration of the specific cases and practices with regard to online freedom of expression and regulation as well as legislation in Sri Lanka examined in this report, it is apparent that the country is failing to abide by international freedom of expression standards as well as its commitment to ensure that the right to the freedom of expression is upheld as guaranteed by Article 19 of the UDHR and ICCPR. In line with the broader objectives of this project as well as the clear global standards and recommendations for addressing freedom of expression on the Internet, it is important that a framework for action focuses on two specific short-term policy goals that would be followed – after successful deliberation with stakeholders – by a long-term action plan for monitoring regulation and other government actions with respect to freedom of expression on the Internet.

Firstly, advocacy should focus on ensuring that information with regard to restrictive legislation, regulation and practices is effectively disseminated to the public, legislators, regulators, and media rights organisations. This should be followed up with additional regional and international advocacy, which would require consultation with the UN Special Rapporteur and key international media rights organisations in order to ensure that there is sustained external pressure on the government to implement legal reforms that respect fundamental rights and ensure that regulators comply with international freedom of expression standards. Secondly, a multi-stakeholder initiative must be launched for broad consultation on and design of policy and legal alternatives pertaining to the protection of the right to freedom of expression, transparency, and privacy and data protection so as to ensure that both user and intermediary perspectives are incorporated into the design of legislation and regulatory standards. An inability to achieve necessary reform and policy responses from the government would have severe implications for the future of freedom of expression on the Internet in Sri Lanka and strengthen existing moves towards surveillance, regulation and restrictive arbitrary action.

---

[259] 2008 Colombo Declaration on Media Freedom and Social Responsibility, http://ict4peace.wordpress.com/2009/03/16/2008-colombo-declaration-on-media-freedom-and-social-responsibility/, May 2009