

Freedom of Expression and the Internet in Sri Lanka

Centre for Policy Alternatives

August 2010

Friedrich Naumann
STIFTUNG **FÜR DIE FREIHEIT**

The Centre for Policy Alternatives (CPA) gratefully acknowledges the financing of the Friedrich Naumann Stiftung für die Freiheit (FNST) that supported the research reflected in this report. The Foundation's work focuses on the core values of freedom and responsibility. Through its projects FNF contribute to a world in which all people can live in freedom, human dignity and peace.



CENTRE FOR POLICY ALTERNATIVES
විකල්ප ප්‍රතිපත්ති කේන්ද්‍රය
மாற்றுக் கொள்கைகளுக்கான நிலையம்

The Centre for Policy Alternatives (CPA) is an independent, non-partisan organization 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

Map of Sri Lanka



Contents

Acronyms.....	6
Executive Summary	7
Global trends in Internet regulation	10
Physical Level.....	10
Connectivity level.....	14
Applications level.....	15
Content level	18
Private individuals and content restrictions	18
Government efforts to regulate content	19
Internet in Sri Lanka	23
Regulatory framework	23
The diminishing space for freedom of expression online	25
Shutting down websites	25
Attacks online journalists	27
Statements undermining freedom of expression	29
Surveillance.....	30
Efforts to regulate online content	31
The fight on pornography	35
Post war developments	36
Structural causes	38
Legal limits to freedom of expression in Sri Lanka	40
National Security Laws.....	40
Emergency Regulations	40
Prevention of Terrorism Act	43
General laws	43
Sri Lanka Press Council Law	43
Official Secrets Act	44
Defamation.....	45
Contempt of Court	45
Parliamentary Privilege	46
Penal Code	46
The Public Performance Ordinance	47
Obscene Publications Ordinance	47
Profane Publications Act	47

Enforcing content restricting laws to the online sphere	48
Freedom of expression in Sri Lanka.....	52
Constitutional texts	52
Restrictions	56
Application to the Internet	59
The Internet and Privacy	61
Constitutional Protection	64
Legislative Framework.....	65
Indian experiences	72
South Africa	73
Conclusion	75
Recommendations	77
List of works cited	79
Books	79
Case Law	79
Legislation.....	80
Internet sources	81
Reports	89
Newspaper Articles	89
Journal Articles	89
Correspondence	89

Acronyms

ACMA	Australian Communications and Media Authority
BBC	British Broadcasting Service
EPDP	Eelam People's Democratic Party
FCC	Federal Communications Commission (United States)
FMM	Free Media Movement
IP	Internet Protocol
IPTV	Internet Protocol Television
ISP	Internet Service Provider
JVP	Janatha Vimukthi Peramuna
LTTE	Liberation Tigers of Tamil Eelam
NDTV	New Delhi Television
NSA	National Security Agency (USA)
PSB	People's Security Bureau (China)
PTA	Prevention of Terrorism Act No 45 1979 (Sri Lanka)
SLT	Sri Lanka Telecom
TID	Terrorist Investigation Department (Sri Lanka)
TRC	Telecommunications Regulations Commission (Sri Lanka)

Executive Summary

The post war outlook for freedom of expression on the web and Internet in Sri Lanka is not bright. In Sri Lanka's recent history, freedom of expression both online and elsewhere has come under threat. Online journalists and bloggers have come under attack, censure and surveillance. Websites have been shutdown and media premises have been attacked. A strong culture of impunity prevails. The government continues to speak of the increasing need for surveillance systems and imposing greater regulation on online content providers.

What is important to note is that stifling content online is not something that is just happening in Sri Lanka. All over the world, regimes of all political persuasion, whether liberal, repressive or in between are finding it a challenge to strike a balance to preserve freedom of expression online. Liberal regimes such as Australia are proposing to use Internet filters to remove certain prescribed content. In Thailand authorities have banned thousands of websites that were deemed offensive to the monarchy. China is famous for its 'great wall' that blocks access to any site that the government deems is undesirable. In Saudi Arabia there is a government authority that determines which websites are acceptable and blocks all others. To date, a record 120 bloggers and Internet users remain imprisoned all over the world. Similarly, regimes of all political persuasion are implementing mechanisms that place Internet usage under surveillance. The French National Assembly have passed a law that allows the government to install software on an Internet user's computer that can collect and record key strokes from the computer. The British and Australian governments are currently considering proposals to require communication firms to hold user information and organize it in a manner that is more easily accessible by law enforcement agencies.

Measures such as the British and French surveillance scheme and the global trend towards stifling content online is worrying, especially when considered from a Sri Lankan perspective. These precedents from abroad, especially from developed 'liberal' governments can be opportunistically seized by regimes like Sri Lanka to legitimize their own actions to clamp down on dissent. In particular it is important to keep in mind the context in which these measures are being carried out. At least in places like Australia, France and the UK the proposed measures are announced publicly and debated vigorously. It is possible for civil society to lobby law makers and regulators and actually impact the policy making process. In contrast in countries like Sri Lanka, laws are made in a culture of secrecy, there is very little opportunity to meaningfully influence the law making process and worse often what is legal and permissible and what happens in reality are two different things.

In any event 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 as to the importance of free speech for a democracy, and how criticizing 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, at odds with comparative international jurisprudence, that allows over-broad national security legislation to trump civil liberties.

Further there are a host of legislative provisions that currently limit freedom of expression. These laws are not specifically targeted at online content; however their existence 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 and the PTA have been criticized often for their over broad nature, lack of specificity and their insufficient connection 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. However, this paper considers examples from foreign jurisdictions and discusses the novel ways these content restricting laws can be applied to the online sphere. Thus, highlighting that in Sri Lanka, though these laws haven't yet been enforced in the online sphere, their mere existence alone warrants concern.

Further given the increasing threats to privacy posed by the Internet, this paper 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 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.

Considering these shortcomings this paper proposes recommendations to improve freedom of expression online. Numerous steps can be taken both at a legal and a policy level. The Government in consultation with service providers, Internet users and bloggers should initiate significant law reform. Laws that restrict discussion of politically and socially relevant content should be repealed. The Government should take immediate steps to legislate for broad privacy protection. Service providers need to provide clear and accessible privacy policies so consumers are informed of their privacy rights. Efforts to block websites and filter content has to be catalogued and published. There needs to be 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 publicized so that users are aware of the limits to their privacy and freedom of expression online.

Global trends in Internet regulation

In January 2010 the U.S. Secretary of State Hillary Clinton announced that freedom of expression on the Internet is a top foreign policy goal of the United States. However, both at home in the U.S. and all over the world, governments are grappling with how to respond to the challenge of regulating the Internet. Broadly speaking, the Internet can be regulated at four levels. The first level is the physical level which concerns the physical infrastructure. The second level is the connectivity layer, which concerns how different devices connect. The third level is the application layer, which concerns the applications used to navigate the Internet. The fourth level is the content layer, which concerns what information is actually available on the Internet. An emerging trend from liberal democracies like the United States to impoverished repressive regimes like Burma, is towards restricting freedom of expression online in the interests of national security, political stability or cultural control. There are tensions between ensuring that users have reliable and unfettered access to the Internet; the interest of government in controlling what information the citizenry can access; and the business interests of the corporate players who own the infrastructure and tools that are being used to access and navigate the Internet.

Physical Level

The first level is the physical level, which is the point at which individuals have access to the Internet and other networked communication technologies. Many governments, especially in the developing world grapple with the challenge of building up sufficient infrastructure to allow individuals affordable and reliable access to the Internet. According to the United Nation's International Telecommunications Union, in 2009 sixty four percent of the developed world had access to Internet whereas only eighteen percent of the developing world had access to the Internet.¹ 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.² In this regard Sri Lanka is illustrative, as of 2009 only five and a half percent of the population has access to the Internet³ whereas over seventy percent of the population has access to mobile phones.⁴ Economic wealth, lack of basic infrastructure (e.g. lack of cheap, reliable accessible electricity), high cost of telecommunications, and lack of basic education and technical expertise all affect a government's ability to provide access to the Internet. In Sri Lanka, along with these factors its thirty year

¹ International Telecommunications Union, *Measuring the Information Society*, (2010), p 1.

²Ibid.

³ Internet World Stats Usage and Population Statistics <<http://www.internetworldstats.com/asia/lk.htm>> accessed 11 May 2010.

⁴ Telecommunications Regulatory Commission of Sri Lanka, June 2009 Statistics < <http://www.trc.gov.lk/information/statistics.html>> accessed 11 May 2010.

old civil war prevented the expansion of telecommunication infrastructure, especially to the northern and eastern parts of the country.

A common barrier hindering access at the physical level is government imposed Internet related licensing and registration requirements. In Iraq, citizens need a licence before installing a modem or a satellite dish.⁵ Similarly in China Internet cafes need to obtain a licence and report details of user activity to the People's Security Bureau (PSB).⁶ In Sri Lanka it was reported that the government planned to introduce a requirement that all online news websites register with the Telecommunications Regulations Commission (TRC).⁷ However, the government later announced that this was not going ahead.⁸

In developed countries, where there is widespread Internet access, an emerging issue is to what extent telephone companies allow competing Internet service providers to use their networks. For example in the United States, telephone companies are lobbying the government to allow them to close their networks to other service providers.⁹ If networks are only used by a limited number of service providers, then those that own the infrastructure will control what information people are able to access. There is an emerging debate about the principles that should underlie any regulation of the Internet. In the United States, the Federal Communications Commission (FCC), the chief regulator of Telecommunications and the Obama administration¹⁰ favor principles of Net Neutrality. The principle of Net Neutrality argues that neither Governments nor Internet Service Providers should place restrictions on content, platforms, modes of communication and the infrastructure used to bring the Internet to the consumer.¹¹ Similarly in Europe, there is a strong push towards Net Neutrality. However in Europe there is an argument being made that Net Neutrality can be achieved by permitting restrictions and simultaneously insisting on transparency.¹² Under European laws providers must provide full disclosure 'of any limitations they impose on access or on the user of services and applications'.¹³

⁵ Article 19, Background Paper on Freedom of Expression and Internet Regulation for the International Seminar on Promoting Freedom of Expression with Three Specialized International Mandates, (2001), p 8.

⁶ Thomas Lum, Internet Development and Information Control in the People's Republic of China CRS Report for Congress Updated 6 February 2010, p 4.

⁷ Lankanewsweb, Government to block Internet in Sri Lanka, 10 February 2010 < http://www.lankanewsweb.com/news/EN_2010_02_10_013.html > accessed 20 February 2010.

⁸ Bandula Sirimanna, 'President halts cyber censorship', The Sunday Times, 21 February 2010 <http://sundaytimes.lk/100221/News/nws_05.html> accessed 4 April 2010.

⁹ Andrew Puddapphatt, New Challenges to freedom of expression <<http://www.article19.org/speaking-out/new-challenges>> accessed on 30 April 2010.

¹⁰ New York Times, 'Editorial: Mr Obama's Internet Agenda', New York Times, 15 December 2008 <http://www.nytimes.com/2008/12/16/opinion/16tue3.html?_r=1> accessed 31 May 2010.

¹¹ Google, 'What do we mean by net neutrality', Google Public Policy Blog, 16 January 2007 <<http://googlepublicpolicy.blogspot.com/2007/06/what-do-we-mean-by-net-neutrality.html>> accessed 18 May 2010.

¹² Neelie Kroes, 'Net Neutrality in Europe address at ARCEP conference', Europa Press Releases Rapid < <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/153>> accessed 31 May 2010.

¹³ John W. Mayo, Mairus Schwartz, Bruce Owen, Robert Shapiro, Lawrence J White and Glenn Woroch, 'How to Regulate the Internet Tap', New York Times, 20 April 2010 < <http://www.nytimes.com/2010/04/21/opinion/21mayo.html>> accessed 31 May 2010.

Another practice increasingly adopted by governments is the surveillance of Internet usage by its citizens. There are worrying trends emerging from both countries with good records on human rights as well as those with poor records. For example under a new law reform package the French National Assembly has passed a law that provides for a state sanctioned online surveillance regime. The Law and Planning for the Performance of Homeland Security 2nd (LOPPSI 2) allows the French government to install software on an Internet user's computer that can "collect record save and transmit key strokes from computers" for a period of up to four months. A judge can extend this period for another four months.¹⁴ Worryingly President Sarkozy himself has expressed a desire to see ISPs play a greater role in clamping down on undesirable content.¹⁵ The bill also provides for the creation of a database known as "Pericles" that can pull together information from various existing databases to create profiles of individuals that would include an array of personal information. France has come under attack for proposing to give the State such unprecedented control over the Internet. To date the measure has only been approved by the French National Assembly; it is yet to pass through the French Senate.¹⁶ It is interesting to note despite's France's domestic initiatives, internationally France is pushing for anti Internet surveillance measures. In July 2010, France and Netherlands called for international guidelines to prevent private firms from exporting high-tech equipment that could be used for Internet censorship.¹⁷

In a similar vein the British government has proposed that a database be created that records every telephone call, e-mail and time spent on the Internet by the public.¹⁸ The government argued that the measures were needed as police and security services needed new powers to keep up with technology, in order to fight crime and terrorism.¹⁹ The proposal was mooted as part of larger plans to implement European Union standards of requiring telephone companies to store records of phone calls and text messages for a period of up to twelve months. Law enforcement agencies would be able to access these records with a warrant issued by the Courts. The British government proposed that the records be handed over to the government and stored in one database, to facilitate easier access for law enforcement

¹⁴ Nate Anderson, 'Next up for France: police key loggers and web censorship', Arts Technica, 19 March 2009 <<http://arstechnica.com/tech-policy/news/2009/05/next-up-for-france-police-keyloggers-and-web-censorship.ars>> accessed 19 May 2010.

¹⁵ Nate Anderson, 'Move over, Australia: France taking 'net censorship lead'', Arts Technica, 17 February 2010 <http://arstechnica.com/tech-policy/news/2010/02/move-over-australia-france-taking-net-censorship-lead.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss> accessed 11 May 2010.

¹⁶ Lepoint, 'Reviews LOPPSI two texts and the reform of criminal procedure carried', Lepoint.fr, 5 May 2010 <<http://translate.google.com/translate?hl=en&sl=fr&u=http://www.lepoint.fr/actualites-politique/2010-05-05/senat-la-reforme-de-la-procedure-penale-reportee/917/0/451385&ei=rCIETNGNBseXcZbY2dUB&sa=X&oi=translate&ct=result&resnum=1&ved=0CBUQ7gEwAA&prev=/search%3Fq%3DExamens%2Bdes%2Btextes%2BLoppsi%2B2%2Bet%2Bde%2Bla%2Br%25C3%25A9forme%2Bde%2Bla%2Bproc%25C3%25A9dure%2Bp%25C3%25A9nale%2Breports%26hl%3Den%26rls%3Dcom.microsoft:en-us>> accessed 11 May 2010 (Translated from French to English via Google Translator).

¹⁷ Yahoo, 'France, Netherlands seek to halt Internet censorship', Yahoo!, 8 July 2010 <http://news.yahoo.com/s/afp/20100708/tc_afp/francenetherlandsinternetpoliticsrights_20100708160333> accessed 8 July 2010.

¹⁸ Richard Ford, 'Big Brother' database for phones and e-mails', Times Online, 20 May 2008 <http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article3965033.ece> accessed 17 May 2010.

¹⁹ BBC, 'Giant database plan 'Orwellian'', BBC, 15 October 2008 <http://news.bbc.co.uk/2/hi/uk_politics/7671046.stm> accessed 11 May 2010.

agencies.²⁰ Critics of the move questioned both how the Government proposed to store and search literally billions of telephone calls, text messages and e-mails and piece together the relevant intelligence.²¹ The Shadow Home Ministry commented that “Given [ministers’] appalling record at maintaining the integrity of databases holding people’s sensitive data, this could well be more of a threat to our security than a support”.²² In particular it was pointed out that holding large collections of data is highly risky as there is increased risk that the data will be lost, traded or stolen.²³ Subsequently the plans for a government owned giant database was scrapped.²⁴ However the Government retained the original idea of asking communication firms, i.e. mobile phone networks, Internet services providers to hold user information and organize it in a manner that is more easily accessible by law enforcement agencies.²⁵ Further under the proposal only the contacts and not the content of communication will need to be retained. Requests to see the data would require top level authorization from a public body.²⁶ The Home Office to date was seeking further consultation on limiting the number of public authorities that can have access to the retained information.²⁷ Shadow Home Secretary commented at the time the larger issue is that the ‘government has built a culture of surveillance which goes far beyond counter terrorism and serious crime...too many parts of government have too many powers to snoop on innocent people and that’s really got to change’²⁸. Alarming, the Australian government has expressed a desire to bring its laws in conformity with European standards, and has announced that it is also planning to introduce a requirement that service providers retain a subscriber’s private Internet browsing history to assist law enforcement agencies.²⁹

In a highly disturbing example of gross abuse of surveillance, two whistle-blowers from the National Security Agency (NSA) in the United States claimed that the NSA frequently surveilled the phone calls of ‘ordinary Americans, journalists, aid workers, and military personnel who were living in the Middle East and calling friends and loved ones back in the US.’³⁰ Disturbingly, it was alleged that it was common practice to single

²⁰ Richard Ford, above n 20.

²¹ Sanjana Hattotuwa, ‘The rise of Big Brother in the UK’, ICT for Peacebuilding, 8 May 2008 <<http://ict4peace.wordpress.com/2008/05/28/the-rise-of-big-brother-in-the-uk/>> accessed 17 May 2010.

²² Richard Ford, above n 20.

²³ Ibid.

²⁴ Dominic Casciani, ‘Plan to Monitor all internet use’, BBC, 27 April 2009 <http://news.bbc.co.uk/2/hi/uk_news/politics/8020039.stm> accessed 17 May 2010.

²⁵ Ibid.

²⁶ Ibid.

²⁷ Ibid.

²⁸ Ibid.

²⁹ Ben Grubb, ‘Govt wants ISPs to record browsing history’, ZDNet, 11 June 2010 <<http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm?omnRef=NULL>> accessed 3 July 2010.

³⁰ Jon Stokes, ‘NSA eavesdropped on Americans, journalists in Baghdad’, Arts technica, 9 October 2008 <<http://arstechnica.com/old/content/2008/10/nsa-eavesdropped-on-americans-journalists-in-baghdad.ars>> accessed 17 May 2010.

out conversations that had no relation to national security issues, but had some novel or salacious content for ridicule and general discussion among the NSA staff.³¹

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 inherent difficulties. In such contexts details of such measures are crucial and especially in countries such as Sri Lanka where the government already has a poor record on freedom of expression and privacy.³² In particular it is important to keep in mind the context in which these measures are being carried out. At least in places like Australia, France and the UK the proposed measures are announced publicly and debated vigorously. It is possible for civil society to lobby law makers and regulators and actually impact the policy making process. In contrast in countries like Sri Lanka, laws are made in a culture of secrecy, there is very little opportunity to meaningfully influence the law making process and worse often what is 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 with poor records on civil liberties to be vigilant and if possible buck the trend.

Connectivity level

The connectivity level refers to the networks and codes that are used to relay information on the Internet. At present all data sent across the Internet is treated the same, thus websites of an individual blogger can be accessed just as easily as the website of a major news company. However an emerging debate in the United States is over the lobbying by cable and telephone networks to implement legislation that would enable them to transmit certain data faster than others. If the changes are implemented, it would create a two tiered internet. Those who pay an additional fee will be on the 'fast tier' and their content will be delivered faster to end users. Those who don't pay the fee will be on the 'slow tier'. Thus a situation could arise where a major news company could pay the network owner to transmit their web page faster than those of an individual blogger. The FCC is currently in favor of the principles of net neutrality, which seeks to ensure that Internet service providers should treat all sources of data equally. However in an April 2010 decision, a federal appeals court held that the FCC lacks the authority to require broadband providers to give equal treatment to all Internet traffic flowing over their networks.³³ The decision marks a setback for the FCC in their efforts to uphold Internet neutrality. Concerns about network neutrality are not limited to the Internet. Recently Apple was criticized over rejecting an iPhone application, Google Voice, (an Internet based telephone service that allow users to make low-cost calls without using traditional telephone services).³⁴ The reason for Apple's rejection was its exclusive arrangement for the iPhone with AT&T, America's largest telephone services provider. The decision was widely criticized as it restricted application choices of iPhone users and helped AT&T maintain its market share.

³¹ Ibid.

³² Ibid.

³³ Comcast Corporation v Federal Communications Commission and United States of America No 08-1291, Decided 6 April 2010.

³⁴ Andrew Heining, 'Why Apple axed the Google Voice iPhone app', The Christian Science Monitor, 28 July 2009 < <http://www.csmonitor.com/Innovation/Horizons/2009/0728/why-apple-axed-the-google-voice-iphone-app>> accessed 31 May 2010.

Applications 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 if a few applications monopolize 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 of 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 by forcing application owners to regulate the content. Browser and software owners themselves have their own terms and conditions both expressly disclosed and hidden which undermine the freedom with which users can navigate the Internet.

A notable example of a government's attempts to regulate these applications is the case of China and Google. In 2005 Google launched a Chinese language google.cn website. In March 2009 the Chinese government blocked access to the Google owned video sharing website, YouTube and other online Google services. In January 2010 citing cyber attacks on human rights activists; Google announced that it is no longer willing to censor searches in China. As of late March 2010 Google reroutes searches from mainland China to Hong Kong. Despite being part of the mainland, Hong Kong is regarded as a special administrative region and has independent judicial power vested within it and is not subject to most Chinese laws. For the moment the Chinese government hasn't banned Google websites in China.

However Google's record is far from clean. Faced with similar obstacles in Thailand, Google was more compliant. Google, as the parent company of YouTube struck a deal with the Thai authorities to censor all YouTube content that offended the Thai Monarchy.³⁵ As of April 2010 Google publishes daily updates on requests from government agencies to remove content from Google services or to provide information on users of Google services and products.³⁶

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 Geocities require users not to publish anything that is harmful, threatening, abusive, harassing or otherwise objectionable.³⁷ 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

³⁵ International Federation of Journalists, 'IFJ concerned over Google censorship deal', International Federation of Journalists, 5 September 2007 <<http://www.ifj.org/en/articles/ifj-concerned-over-google-censorship-deal-with-thailand>> accessed 18 May 2010.

³⁶ Google. Government requests directed to Google and YouTube <<http://www.google.com/governmentrequests/>> accessed 30 April 2010.

³⁷Article 19, above n 7.

including in Sri Lanka, allows third parties back door access to listen in on communications between users.³⁸ Following a meeting between Internet service providers and their Austrian regulator, it was reported that a high ranking official from the Austrian interior ministry had indicated that they had no difficulties listening in on Skype conversations.³⁹ In response Skype failed to expressly deny that such a feature existed on Skype.⁴⁰ In a separate news story, it was reported that the Chinese version of Skype (TOM-Skype) allows for Chinese authorities to monitor text communications between users.⁴¹ Allegedly TOM-Skype monitors all text communications for a list of prohibited words such as 'democracy', 'Falun Gong' and 'Taiwan independence'. The encrypted list of words inside TOM-Skype prevents text conversations containing prohibited words from being communicated. When the prohibited words are used personal information of the user is retained. It was suspected that Skype's Chinese joint venture partner managed the surveillance system with the assistance of the Chinese police.⁴² Skype responded explaining that the Chinese version of Skype in order to be able to operate had to comply with local laws that required communication companies to monitor and block instant messages containing 'offensive' words; however that the parent company was unaware that such messages were being stored and accessed by third parties.⁴³

In a similar story from India, it was reported that the government sought to have backdoor access to information passing through BlackBerry services in India. BlackBerry is a smart phone that offers advanced capabilities more similar to a personal computer rather than an ordinary mobile phone. When Tata Teleservices sought approval from the authorities to launch BlackBerry services in India, the Home Minister threatened to ban BlackBerry services unless the government was given unconditional access to information passing through BlackBerry services.⁴⁴ In particular it was reported that the Home Ministry was concerned over the fact that e-mails being received through the BlackBerry service couldn't be intercepted.⁴⁵ The officials allegedly requested that either a 'demand key' be provided in to data and e-mails sent from BlackBerry devices or that servers be set up that could be monitored by Indian law

³⁸ 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>> accessed 18 May 2010.

³⁹ Ibid.

⁴⁰ Ibid.

⁴¹ Amnesty International, 'Skype users monitored in China', Amnesty International, 7 October 2008 <<http://www.amnesty.org.au/china/comments/18073/>> accessed 18 May 2010.

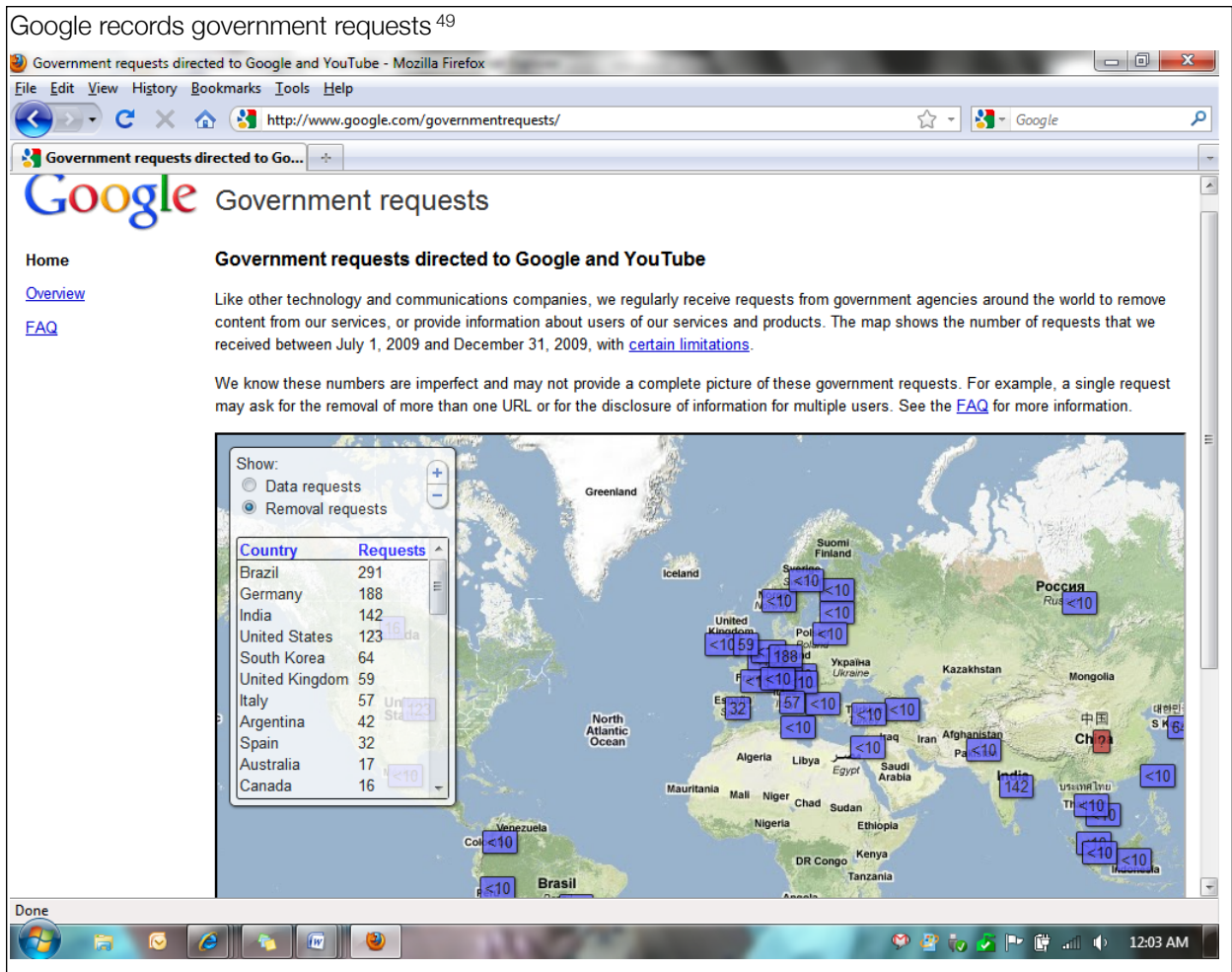
⁴² John Markoff, 'Surveillance of Skype Messages Found in China', New York Times, 1 October 2008 <http://www.nytimes.com/2008/10/02/technology/internet/02skype.html?_r=1&em> accessed 18 May 2010.

⁴³ Josh Silverman, 'Skype President Addresses Chinese Privacy Breach' The Big Blog, 2 October 2008 <http://blogs.skype.com/en/2008/10/skype_president_addresses_chin.html> accessed 18 May 2008.

⁴⁴ Joel Hruska, 'Rumours fly as RIM, India talk BlackBerry snooping, privacy', Arts technica, 27 May 2008 <<http://arstechnica.com/gadgets/news/2008/05/rumors-fly-as-rim-india-talk-blackberry-snooping-privacy.ars>> accessed 18 May 2010.

⁴⁵ Marin Perez, 'RIM Questions India's BlackBerry Encryption Worries', Informationweek, 2 June 2008 <<http://www.informationweek.com/news/security/encryption/showArticle.jhtml?articleID=208401643>> accessed 18 May 2010.

enforcement agencies.⁴⁶ At the time Ministry claimed that such access was necessary as BlackBerry's could be used to coordinate terrorist attacks.⁴⁷ However, not all communication firms have been resilient to pressures as BlackBerry. Recently Nokia Siemens admitted that it had made an error when it provided Iran the ability to lawfully intercept communications over its mobile networks.⁴⁸



⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ Alton Parish, 'EU Report Shows Internet Censorship Increasing; Sophisticated and Hidden Censorship Tools Mobilised by Enemies of Human Rights', Beforeitsnews, 14 June 2010 <http://beforeitsnews.com/news/78/338/EU_Report_Shows_Internet_Censorship_Increasing;_Sophisticated_and_Hidden_Censorship_Tools_Mobilized_by_Enemies_of_Human_Rights.html> accessed 4 July 2010.

⁴⁹ Google, 'Government Requests', Google, 2010 <<http://www.google.com/governmentrequests/>> accessed 31 May 2010.

Content level

The content layer refers to the actual information available on the Internet. Laws relating to hate speech, libel, defamation, intellectual property all affect the actual content that users of the Internet can upload on to the Internet. It is interesting to note that at this level of regulation, both governments and private entities have significant power to stifle online content. Private individuals can limit freedom of expression online by asserting their own rights for example to intellectual property and reputation. Governments can stifle content both expressly and under closed doors. The most common way is by enforcing laws that restrict content, such as anti hate speech, laws relating to obscenity and national security.

Private individuals and content restrictions

Private individuals and corporations can restrict content by pursuing legal action under intellectual property laws and under libel and defamation laws. In 2002 a UK Law Commission study found that some ISPs received over a hundred complaints a year from solicitors and individuals claiming that they hosted defamatory material. The Commission also found that the 'safest course of action for the recipients of letters was to remove the material without regard to public interest or truthfulness.'⁵⁰ In another infamous example in India, during the 2008 terrorists' attacks in Mumbai a blogger living in the Netherlands wrote a blog post criticizing an Indian television channel, New Delhi Television (NDTV) and its group editor Barkha Dhatt's reporting of the attacks.⁵¹ The blogger was critical of Dhatt's sensationalist coverage and in particular how NDTV aired information about remaining hostages and their locations during the crisis, thus further endangering them. Subsequently and without explanation the blogger took down his post and offered an unconditional apology.⁵² It was later confirmed that the blogger was served with a libel suit by NDTV.⁵³ The blogger, a lone individual confronted with a law suit from a large media organization chose to back away.

⁵⁰ Gus Hosein, *Politics of the Information Society: The Bordering and Restraining of Global Data Flows*, (2004), p 29.

⁵¹ Gaurav Mishra, 'Indian Blogosphere condemns NDTV's bullying of blogger Chyetanya Kunte over criticism of Barkha Dutt'. Gauravonomics. < <http://www.gauravonomics.com/blog/indian-blogosphere-condemns-ndtvs-bullying-of-blogger-chyetanya-kunte-over-criticism-of-anchor-barkha-dutts-sensationalistic-coverage-of-the-1126-mumbai-terror-attack/>> accessed 31 May 2010.

⁵² Rezwan, 'India: blogger silenced', *Global voices*, 30 January 2009 < <http://globalvoicesonline.org/2009/01/30/india-blogger-silenced/>> accessed 1 June 2010.

⁵³ *Ibid.*

Government efforts to regulate content

Government's can restrict online content by implementing filtering and blocking software, enforcing criminal obscenity laws, hate speech and so on. At times laws not specifically aimed at restricting online content can have restrictive consequences on the online sphere. In an example of how laws unrelated to the Internet can have unintended consequences, under current French law it is an offence to film or broadcast acts of violence by people other than professional journalists. French civil liberties group has criticized the law as it could result in the imprisonment of citizen journalists who film acts of violence or operators of web sites that publish the images.⁵⁴ The law was part of a legislative effort to outlaw delinquent acts. The offence in question was created to criminalize acts of 'happy slapping', where violent acts are filmed by accomplices for the amusement of an attacker's friends. In other quarters the law has been criticized as being a 'classic instance' where an overbroad definition of a specific problem serves to undermine freedom of expression and media freedom.⁵⁵

Interestingly, regimes of all political persuasion, whether liberal, repressive or in between are finding it a challenge to strike a balance to preserve freedom of expression online. Australia is a classic example. The Australian Communications and Media Authority (ACMA) is currently empowered to issue takedown notices against ISPs hosting certain prescribed materials. However there have been concerns about the efficacy of this method, as the ACMA can only issue notices against content that is uploaded in Australia.⁵⁶ Thus, the Australian Parliament is soon expected to pass a new measure that requires mandatory ISP level filtering of prescribed materials.⁵⁷ Prescribed materials include among other things, content classified as 'refused classification' (RC) or X 18+ materials. The Government explained these measures as an effort to protect Australian families, from websites containing sexual violence, bestiality and child pornography.⁵⁸ Critics of these laws point to the fact what these measures really amount to is an effort to impost family values as determined by the Government on the citizenry. Others point to the fact that RC material could include socially and politically controversial material for example content relating to drug use, abortion and euthanasia. In this regard, Google has voiced its concerns, noting that the Australian constitution does not

⁵⁴ Peter Sayer, 'France bans citizen journalists from reporting violence', Macworld, 6 March 2007 <<http://www.macworld.com/article/56615/2007/03/franceban.html>> accessed 18 May 2010.

⁵⁵ Sanjana Hattotuwa, 'A step backwards for Citizen Journalism – France bans citizen journalism from reporting violence', ICT for Peacebuilding, 7 March 2007 <<http://ict4peace.wordpress.com/2007/03/07/a-step-backwards-for-citizen-journalism-france-bans-citizen-journalists-from-reporting-violence/>> accessed 18 May 2010.

⁵⁶ Information Policy, 'Australia: Measures to Improve Safety of the Internet for Families', Information Policy, 2 July 2010 <<http://www.i-policy.org/2010/07/australia-measures-to-improve-safety-of-the-internet-for-families.html>> accessed 4 July 2010.

⁵⁷ Ibid.

⁵⁸ Ibid.

provide for a general freedom of expression guarantee, and only protects a limited freedom of political speech, thus 'there is a significant risk that filtering of RC content could readily be extended to other content whether or not the content is related to sex or violence.'⁵⁹ The Australian Government has responded to these criticisms by proposing to introduce a more transparent process for classifying RC content.⁶⁰

Moreover, implementing filtering or blocking mechanisms or requiring that Internet service providers (ISPs) do so is one of the most controversial ways to restrict access to content online. Generally it is done by creating a database of specific words and phrases whose appearance on a website will cause the website to be blocked. However a key problem with this method is that it blocks unrelated material. For example AOL had to tell some British users to misspell the name of their own home town, 'Scunthorpe' as the name was automatically excluded from its inbuilt censor, owing to the string of four letters in its name.⁶¹ In Sri Lanka the government passed the Private Television Station Broadcasting Regulations of 2007 which required ISPs monitor proscribed video content.⁶² However, owing to various other objections the Supreme Court issued an interim order suspending the Regulations. In another example closer to home, there appears to be an emerging trend in Asia to implement Internet filters to protect religious values. Recently in Pakistan, a court ordered that a host of popular websites sites such as Facebook, Flickr, and Wikipedia be banned as they violated Pakistani blasphemy laws.⁶³ However on appeal, the Court restored access to most sites as '[it] couldn't block access to information'.⁶⁴ In its judgment the Court encouraged the Pakistani government to consider implementing a national censorship program that limits hate content similar to those in UAE and Saudi Arabia.⁶⁵ In aftermath of this decision, the Pakistani Ministry of Information Technology announced that it will start monitoring seven websites including Google and Yahoo for content that may be offensive to Muslims.⁶⁶ Following the example from Pakistan, weeks later Afghanistan

⁵⁹ Google, 'Mandatory ISP Level Filtering - submission to the Department of Broadband, Communications and Digital Economy', Arts technica < http://www.dbcde.gov.au/submissions/20100316_11.34.55/256-Google%20ISP%20filtering%20submission%20Feb%202010.pdf> accessed 18 May 2010.

⁶⁰ Information Policy, above n 36.

⁶¹ Gus Hosein, *Politics of the Information Society: The Bordering and Restraining of Global Data Flows*, (2004), p 29.

⁶² Sanjana Hattotuwa, 'Significant issues arising out of the Private Television Broadcasting Regulations of 2007 for bloggers and new media producers in Sri Lanka', *ICT for Peacebuilding*, 24 November 2008 < <http://ict4peace.wordpress.com/2008/11/24/significant-issues-arising-out-of-the-private-television-broadcasting-station-regulations-of-2007-for-bloggers-and-new-media-producers-in-sri-lanka/>> accessed 18 May 2010.

⁶³ Adam E. Ellick, 'Pakistani court orders access to facebook restored', *New York Times*, 31 May 2010 <<http://www.nytimes.com/2010/06/01/world/asia/01pstan.html>> accessed 1 June 2010.

⁶⁴ *Ibid.*

⁶⁵ *Ibid.*

⁶⁶ BBC, 'Pakistan to monitor Google and Yahoo for 'blasphemy'', *BBC*, 25 June 2010 < http://news.bbc.co.uk/2/hi/south_asia/10418643.stm > accessed 3 July 2010; Zeeshan Haider, 'Pakistan to monitor Google, others for blasphemy', *Reuters*, 25 June 2010 < <http://in.reuters.com/article/id/INIndia-49655320100625?feedType=RSS&feedName=everything&virtualBrandChannel=11709>> accessed 3 July 2010.

announced that it too will be filtering the popular sites Google, Facebook, Twitter as they may contain content that is 'immoral and against the traditions of Afghani people'⁶⁷

In other parts of the world Governments are taking more straightforward to banning content. In the United States the Army has ordered soldiers to stop posting on personal blogs or sending email messages without the permission of a superior officer.⁶⁸ In Thailand over 43,000 websites have been blocked for containing contents that were insulting of the Monarchy⁶⁹ and over 17,000 websites have been blocked for national security reasons.⁷⁰ In Malaysia, despite the Government's promises not to censor the Internet as part of promoting the country's burgeoning ICT industry, authorities requested that all nineteen ISPs in the country block the controversial political website Malaysia Today.⁷¹ When pressed with the inconsistency of its promises and actions, government claimed that the promise was subject to interpretation.⁷² In Indonesia officials are considering proposals to block Internet websites that are deemed to violate 'public decency'.⁷³ In Singapore rather than banning the content, the authorities punish the authors of online content. In the high profile case of Gopalan Nair, a lawyer that criticized a Singaporean judge in an online blog post was jailed.⁷⁴ Nair's blog posts criticizing the judge remained online; however, Nair's experiences no doubt served to instill fear and self censorship on fellow bloggers.

Unsurprisingly in Fiji the military junta are not only banning anti junta blogs but also jailing their authors.⁷⁵ China is famous for its 'great wall' that blocks access to any sites the government deems undesirable. Among the prohibited content are well known news websites such as BBC, CNN, Time and PBS. There are similar systems in Saudi Arabia where there is a government authority that determines what websites are acceptable and blocks all others.⁷⁶ All web traffic is forwarded to a central authority and information considered harmful to 'Islamic values' are barred. In Jordan the Press and Publications Law has been

⁶⁷ Rebekah Heacock, 'Afghanistan begins Internet filtering with Gmail, Facebook', Opennet, 28 June 2010 <<http://opennet.net/blog/2010/06/afghanistan-begins-internet-filtering-with-gmail-facebook/>> accessed 4 July 2010.

⁶⁸ Brad Linder, 'Army tells soldiers to stop blogging', Download Squad, 2 May 2007 <<http://www.downloadsquad.com/2007/05/02/army-tells-soldiers-to-stop-blogging/>> accessed 18 May 2008.

⁶⁹ Komsan Tortermvasana, 'Websites face new crackdown', Bangkok Post, 18 June 2010 <<http://www.bangkokpost.com/news/local/38943/websites-face-new-crackdown>> accessed 4 July 2010.

⁷⁰ Achara Ashayagachat, 'Web block adds controversies to laws', Bangkok Post, 6 May 2010 <<http://www.bangkokpost.com/breakingnews/177092/website-blockade-add-controversies-to-lese-majeste-cyber-laws>> accessed 4 July 2010.

⁷¹ Lee Min Keong, 'With site block, Malaysia seems to break promise', CNet News, 2 September 2009 <http://news.cnet.com/8301-13578_3-10030325-38.html> accessed 18 May 2010.

⁷² Ibid.

⁷³ Presi Mandari, 'Indonesia looks to block', AFP, 16 February 2010 <<http://www.google.com/hostednews/afp/article/ALeqM5hac4JRd2Zm2itcNWDH7JG3bynuCQ>> accessed 18 May 2010.

⁷⁴ Mark 'Rizzin' Hopkins, 'Freedom of Speech, Not Freedom of Consequences', Mashable, 2009 <<http://mashable.com/2008/06/05/truth-and-consequences/#more-27552>> accessed 18 May 2010.

⁷⁵ Patrick O' Conner, 'Fijian military junta targets bloggers', World Socialist Web Site, 24 May 2007 <<http://www.wsws.org/articles/2007/may2007/blog-m24.shtml>> accessed 18 May 2010.

⁷⁶ Article 19, above n 7, p 9.

amended to allow government control over online content.⁷⁷ Under the law Internet content in Jordan comes under the purview of Department of Publications and Publishing. The law permits authorities to prosecute or impose fines on journalists, bloggers and editors for publishing online material that may be 'deemed offensive or imply criticism of the Government, national unity or the economy'.⁷⁸ Under the law a former MP was given a two year prison sentence for publishing news considered harmful to the government's reputation.⁷⁹ The law has been criticized for increasing pressure from the state for journalists to exercise self censorship. Further, Internet Café owners in Jordan are required to register the IP number of the Café, and the user's personal data, time of use and data of the Web sites explored.⁸⁰ Internet Cafés are required to install censorship programs to prevent access to websites containing pornographic, drug or tobacco related and anti religious content.⁸¹

As will be seen in the third section of this Report, Sri Lanka is not far behind many of these global developments. What is important to note is that what is happening in Sri Lanka cannot be viewed in isolation. It must be understood in the context of this emerging global trend. All over the world countries with good human right records, as well as those with poor records are acting in ways that restrict freedom of expression online. In some cases like France, there is an incongruence between their international efforts to push for greater freedom of expression and their domestic efforts to limit it. What is worrying about this trend is that, examples from foreign jurisdictions can be used by governments to legitimize their own efforts to limit freedom of expression online. A response that seeks to preserve freedom of expression online needs a global consensus where governments commit to uphold freedom of expression both abroad and at home, both online and otherwise.

⁷⁷ Article 19, Press Release Jordan: Courts Extend Law to Curb Internet Freedoms, 13 January 2010 <<http://www.article19.org/pdfs/press/jordan-courts-extend-law-to-curb-internet-freedoms.pdf>> accessed 18 May 2010.

⁷⁸ Ibid.

⁷⁹ Open Net Initiative, Jordan, 6 August 2009 <http://opennet.net/research/profiles/jordan#footnote13_st2wukl> accessed 18 May 2010.

⁸⁰ Ibid.

⁸¹ Ibid.

Internet in Sri Lanka

Regulatory framework

Internet service providers 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. At present the President is responsible for the Ministry of mass communications, thus secretary to the President, Lalith Weeratunga chairs the TRC.

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.⁸² 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.⁸³ However, the Minister may reject such recommendations and grant a license under his or her own discretion.⁸⁴ Applications for licenses are to be in writing and in a manner required by the TRC.⁸⁵ Further a fee must be paid for each license⁸⁶ and the Minister may impose conditions on a license.⁸⁷

Interestingly, regimes of all political persuasion, whether liberal, repressive or in between are finding it a challenge to strike a balance to preserve freedom of expression online.

When issuing such licenses, the TRC can impose specific license conditions. Terms and conditions of a license can relate to any of the following:

⁸² Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(2).

⁸³ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(5).

⁸⁴ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(2).

⁸⁵ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(4).

⁸⁶ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(6)(a).

⁸⁷ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 17(6)(c).

- 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:
 - a. 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;
 - b. To keep the TRC informed of the practices followed by the ISP in the routing of national and international traffic; and
 - c. To ensure that compensation is paid to persons affected by the running of underground cables or overhead lines;
- h) Conditions requiring an operator to:
 - a. To comply with any direction given by the TRC as to any matter specified in the licence;
 - b. To act with the consent of the TRC when doing things that are required to be done under the licence; and;
 - c. 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 actions of the TRC must be those permitted by 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 actions of the TRC infringes upon constitutional rights, then a fundamental rights case may be brought against the TRC before the Supreme Court. It is notable that following reports that the Government planned to introduce regulations to require news websites to register with the TRC, it was pointed out

that the TRC has no authority to require or to maintain a register of news websites.⁸⁸ Further, any such action could potentially be the subject of a writ or fundamental rights application.⁸⁹

The diminishing space for freedom of expression online

Over the past five years freedom of expression online has come under severe threat. During the war and especially towards its last stages, websites were blocked and online journalists were killed and attacked. Those websites that had the resources to withstand such impunity survived, whilst others voluntarily shut down their operations. Officials repeatedly undermined the work of journalist both online and otherwise, accusing them of unpatriotic, treacherous behavior. There were open calls for censorship and vilification of journalists. Disturbing evidence emerged of state sanctioned surveillance on media personnel and citizens generally. Even in the post war period there were reports of state sanctioned surveillance on social networking websites. There were unsuccessful efforts to regulate online video content, which if successfully enforced would have had resulted in wide scale censorship of online content. The Government also made lukewarm efforts to ban online domestically produced pornographic content.

Shutting down websites

During the latter part of the war websites that purported to provide alternative war coverage 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.⁹⁰ The website was generally regarded as having a LTTE slant and the Government accused it of being a propaganda instrument of the LTTE. To date, the government has denied any knowledge of the unavailability of Tamilnet.com. At the time, then government spokesperson and current Media Minister Keheliya Rambukwella denying any government involvement in the blocking of Tamilnet.com added that ‘the government is looking to hire hackers to disable Tamilnet but could not find anyone yet’.⁹¹

Article 19, an international Human Rights group, condemned the government for cutting off an important source of independent and alternative views.⁹² Local media watchdog Free Media Movement criticized the government as follows:

⁸⁸ Rohan Samarajiva, ‘Quo Warranto TRC?’, Lirneasia, 14 February 2010 < <http://lirneasia.net/2010/02/quo-warranto-trc/>> accessed 4 April 2010.

⁸⁹ Ibid.

⁹⁰ Groundviews, ‘Sri Lanka blocks TamilNet’, Groundviews, 19 June 2007 < <http://www.groundviews.org/2007/06/19/sri-lanka-blocks-tamilnet/>> accessed 1 June 2010.

⁹¹ BBC, ‘Tamil Net Blocked in Sri Lanka’, BBC < http://www.bbc.co.uk/sinhala/news/story/2007/06/070620_tamilnet.shtml> accessed 4 April 2010.

⁹² 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>> accessed on 4 April 2010.

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 expression⁹³

Though not completely blocked during the latter part of the war the website of Human Rights Watch remained regularly inaccessible.⁹⁴ Other websites such as TamilCanadian.com, Lankanewsweb.com, Nidahasa.com, and Lankaenews.com were also blocked.⁹⁵ Though not shut down, 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'.⁹⁶

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.⁹⁷ The sites were inaccessible from Sri Lanka's main ISP, the government owned Sri Lanka Telecom (SLT).⁹⁸ However the sites were accessible by the privately owned ISP Dialog WiMax. It was further reported that according to a source who worked for SLT that 'verbal directives were given' to block the websites. Complaints were made to the electoral commission who had in turn referred the complaints to SLT. SLT however refused to answer any questions. Reporters without Borders condemned the government, 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...⁹⁹

⁹³ 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> accessed 4 April 2010.

⁹⁴ Reporters Without Borders, Internet Enemies – Countries under surveillance: Sri Lanka, 12 March 2009 < <http://www.unhcr.org/refworld/docid/4a38f97c.html>> accessed 4 April 2010.

⁹⁵ 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>> accessed 18 May 2010.

⁹⁶ The Bottom Line, 'Plans to kill TNA website?', The Bottom Line, 9 April 2008 <<http://www.thebottomline.lk/2008/04/09/B38.htm>> accessed 3 July 2010.

⁹⁷ BBC, 'Sri Lanka news websites 'blocked'', BBC, 27 January 2010 <http://www.bbc.co.uk/sinhala/news/story/2010/01/100127_lankaenews_rsf.shtml> accessed 18 May 2010.

⁹⁸ 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>> accessed 18 May 2010.

⁹⁹ Ibid.

Attacks online journalists

Before its blocking, in 2005 the editor of Tamilnet, Dharmaratnam Sivaram “Taraki” was murdered because his coverage of political and military situation was seen as hostile by the government. In 2007, another editor of a Tamil website E-thalaya.org, Kumudu Champika Jayawardena was the target of an ambush of pro government militia. J.S. Tissainayagam, editor of the now defunct www.outreachsl.com and North Eastern Monthly, was detained under the Prevention of Terrorism Act No 48 1979 (PTA) on 7 March 2008, held and interrogated for over 180 days without any formal charge by the Terrorist Investigation Department (TID).

In April 2008, JVP guards attempted to intimidate and expel a journalist from ‘Lanka E News’ who was attempting to report a JVP party press conference in Colombo.¹⁰⁰ The defence ministry called the reports of the Sinhala service of the BBC World service ‘diabolical lies’.¹⁰¹ The BBC journalists were accused of being accomplices in Tamil Tiger propaganda.¹⁰² Indika Gamage, Editor of the Lanka Dissent website alleged in May that the website was subject to hacking attempts. Gamage stated that

The Defence Ministry recently set up an electronic media observation unit at a building adjacent to Standard Chartered Bank in front of the President’s House in Colombo to monitor websites reporting on the situation in Sri Lanka. LD learns through reliable sources that this particular unit staffed with electronic and IT experts, is experimenting on how to disrupt websites.¹⁰³

The Ministry of Defence denied the allegations and demanded a retraction. However Gamage several months later again complained that the e-mail inbox was hacked into, and the websites’ email address was

Measures such as the British, French and American surveillance scheme have been criticized as such precedents from developed ‘liberal’ governments will be opportunistically seized by more repressive regimes to legitimize their own surveillance mechanisms to clamp down on dissent.

¹⁰⁰ Sanjana Hattotuwa, ‘2008: Celebrating the growth of media freedom and the freedom of expression in Sri Lanka’, ICT for Peacebuilding, 4 March 2009 < <http://ict4peace.wordpress.com/2009/03/04/2008-celebrating-the-growth-of-media-freedom-and-the-freedom-of-expression-in-sri-lanka/> > accessed 1 June 2010.

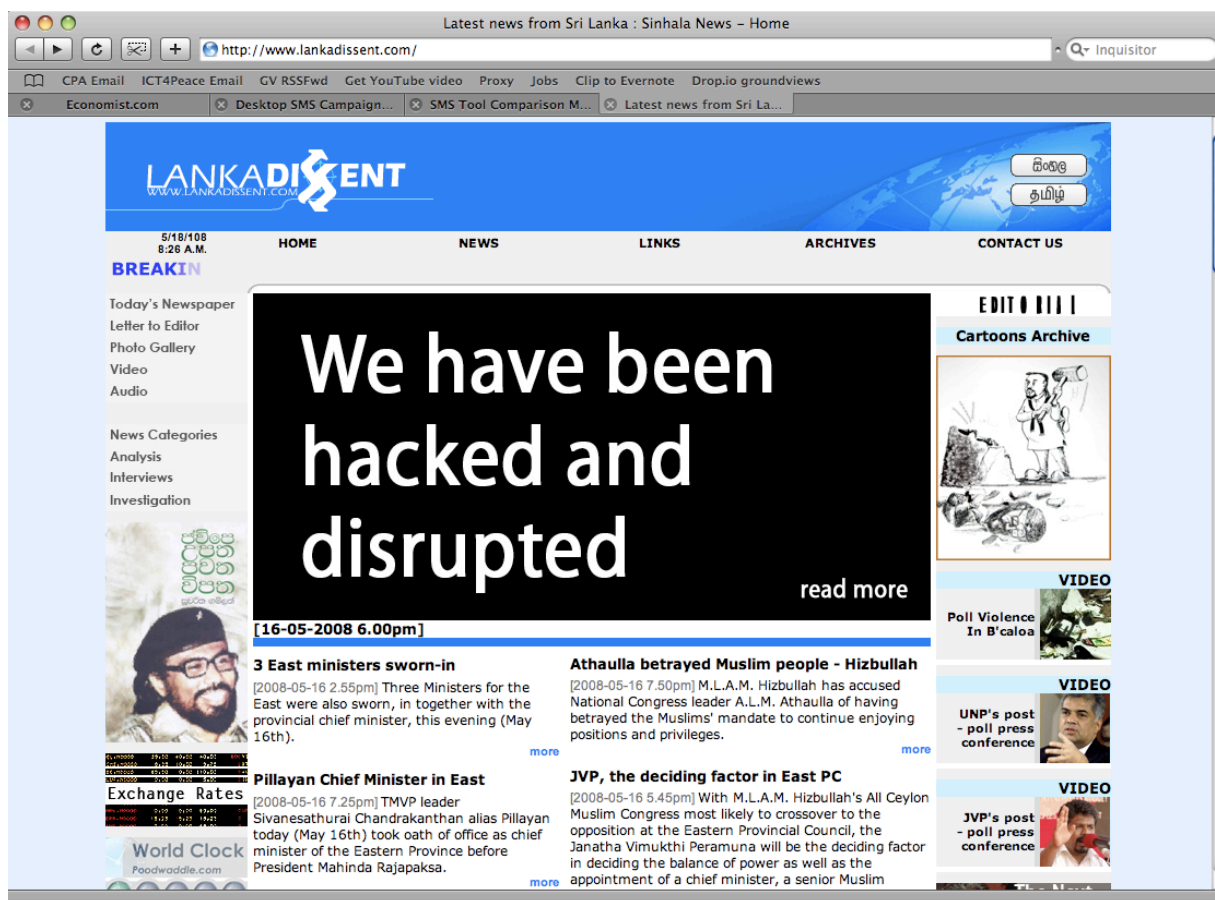
¹⁰¹ Ministry of Defence, ‘WFP apology for BBC falsehood on Sri Lankan IDPs’, Ministry of Defence, 12 December 2008 < http://www.defence.lk/new.asp?fname=20081210_08 > accessed 1 June 2010.

¹⁰² Ibid.

¹⁰³ The Nation, ‘Unidentified groups attack Mangala’s news website’, The Nation on Sunday, 18 May 2008 <<http://www.nation.lk/2008/05/18/news11.htm>> accessed 3 July 2010.

used to threaten and insult third parties.¹⁰⁴ Further the site was blocked and even the administrator's were not able to have access to it.¹⁰⁵

In November 2009, the Daily Mirror reported that a young blogger was arrested by the Criminal Investigations Department and ordered to be detained by a Matale Magistrate for making offensive comments regarding the President and Secretary of Defense on the web.¹⁰⁶ Days later it was reported that the individual arrested was not a blogger, but that he had sent a 'derogatory email containing five nude photos' to the President and the Defense Secretary.¹⁰⁷ No further reporting of the story has been done and it remains unclear whether there were any offensive blog posts.



¹⁰⁴ Free Media Movement, 'After 365 Days it's now a crawl for survival – LankaDissent', Free Media Movement, 21 July 2008 < <http://freemediasrilanka.wordpress.com/2008/07/21/after-365-days-it%E2%80%99s-now-a-crawl-for-survival-lankadissent/>> accessed 3 July 2010.

¹⁰⁵ Ibid.

¹⁰⁶ Sanjana Hattotuwa, 'Blogger arrested in Sri Lanka for 'offensive' comments regarding President and Defense Secretary?', ICT for Peacebuilding, 1 November 2009 < <http://ict4peace.wordpress.com/2009/11/08/the-arrest-of-the-%e2%80%98blogger-%e2%80%99-in-sri-lanka-crowd-sourcing-trumps-traditional-media-follow-up/>> accessed 18 May 2010.

¹⁰⁷ Sanjana Hattotuwa, 'The arrest of the 'blogger' in Sri Lanka: Crowd-sourcing trumps traditional media follow up', ICT for Peacebuilding, 8 November 2009 < <http://ict4peace.wordpress.com/2009/11/08/the-arrest-of-the-%e2%80%98blogger-%e2%80%99-in-sri-lanka-crowd-sourcing-trumps-traditional-media-follow-up/>> accessed 18 May 2010.

On the eve of the Presidential election, when the Lankaenews.com was blocked, at one point its premises was surrounded by police and its director received a death threat.¹⁰⁸ Further staff from Lankaenews.com had received threatening phone messages with comments such as 'we are coming to deal with you'.¹⁰⁹ Political analyst and cartoonist Prageeth Eknaligoda, journalist for the news site Lankaenews has been reported missing since the night of 24 January 2010.¹¹⁰ RSF reported that on the eve of his disappearance, Prageeth had confided in a colleague that he was being threatened because of his political analyses.¹¹¹

Statements undermining freedom of expression

During this period the government and other key actors were most forthcoming in their disregard for media freedom and freedom of expression. There were repeated statements threatening journalists, bloggers and anyone else who dared to provide an alternative coverage of social and political events in Sri Lanka. During the war both the Commander of the Army General Sarath Fonseka and Defense Secretary Gotabaya Rajapaksa were virulent in their criticism of alternative coverage of the war. In January 2008, General Fonseka repeatedly called independent journalists 'traitors'.

The biggest obstacle is the unpatriotic media. I am not blaming all journalists. I know 99 percent of media and journalists are patriotic and doing their jobs properly. But unfortunately, we have a small number of traitors among the journalists. They are the biggest obstacle. All other obstacles we can surmount.¹¹²

In the same month in an interview Gotabaya Rajapaksa stated that media has to be censored and criminal defamation brought back.¹¹³ Threats to the media also came from non-government quarters. In November the leader of the opposition threatened senior journalist from the Daily Mirror and its Editor.¹¹⁴ The Eelam People's Democratic Party (EPDP) in November wrote to the FMM asking that it retract allegations made by the Uthayan newspaper that armed cadre of the group was intimidating and harassing journalists.¹¹⁵ The

¹⁰⁸ Reporters Without Borders, 'Countries under surveillance 2010- Sri Lanka', Reporter Without Borders, 18 March 2010 <<http://www.unhcr.org/refworld/docid/4c21f668c.html>> accessed 5 July 2010.

¹⁰⁹ Ibid.

¹¹⁰ Ibid.

¹¹¹ Ibid.

¹¹² Sanjana Hattotuwa, above n 123.

¹¹³ Ibid.

¹¹⁴ Ibid.

¹¹⁵ EPDP, 'EPDP advisory to free media movement', Free Media Movement, 1 November 2008 <<http://freemediasrilanka.wordpress.com/2008/11/17/epdp-advisory-to-free-media-movement/>> accessed 1 June 2010.

JVP also threatened journalists on many occasions during the year.¹¹⁶ Inevitably local media groups exercised a high degree of self censorship. The significant civilian impact of the last phase of the war and humanitarian fall out of the war went unreported.

Organizations with the infrastructure and financial security to withstand the government's attacks such as the BBC continued to operate and offer their alternative coverage of events in Sri Lanka. However, other smaller local website operators, ceased to operate. For example, following the brutal assassination of one of the country's leading newspaper editor Lasantha Wickrematunga the news website lankadissent.com ceased to operate.

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 carry out the attacks.¹¹⁷ 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.¹¹⁸ 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 surveil 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 over the existence of Government 'hit lists' and plans to monitor any 'malpractice' of human rights activists, lawyers and journalists.¹¹⁹

As recently as March 2010 Defence secretary Gotabaya Rajapaksa responded to the question on '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?' he responded as follows:

¹¹⁶ Sanjana Hattotuwa, above n 123.

¹¹⁷ 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> accessed 18 May 2010.

¹¹⁸ Nadesapillai Vithyatharan Fundamental Rights Application under s 126 of the Constitution, paragraph 35.

¹¹⁹ BBC, 'Sri Lanka denies 'hit list' charge', BBC, 17 March 2010 < http://news.bbc.co.uk/2/hi/south_asia/8571627.stm> accessed 18 May 2010.

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 it¹²⁰¹²¹

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.¹²² Subsequently there were 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.¹²³ Reportedly the idea came from Defence Secretary Gotabaya Rajapaksa who had previously thought of using Facebook to collect information on foreign supporters of LTTE suspects.¹²⁴ In July 2010, it was reported that the Women and Child's Bureau of the Police had received over 50 complaints against Facebook.¹²⁵ Among the complaints were allegations that photos on Facebook were being stolen and being turned in to 'indecent images'.¹²⁶ To date the TRC has responded that they had not received any complaints concerning Facebook. Anusha Palpitya, the 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'.¹²⁷

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 broadcasting stations. From the outset civil society groups were highly critical of the Regulations given the negative implications it

120

¹²¹ Dianne Silva, 'USA only sympathetic towards Fonseka: Gota', Daily Mirror 1 March 2010, p A7.

¹²² Rathindra Kuruwita, 'Facebook users come under scrutiny', Lankanewspapers.com, 31 January 2010 < http://www.lankanewspapers.com/news/2010/1/53532_space.html > accessed 16 July 2010.

¹²³ 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> > accessed 4 April 2010.

¹²⁴ Ibid.

¹²⁵ Indika Sri Aravinda, 'Complaints against Facebook', Daily Mirror, 13 July 2010 < <http://www.dailymirror.lk/index.php/news/5055-complaints-against-facebook-.html> > accessed 16 July 2010.

¹²⁶ Ibid.

¹²⁷ Ibid.

had for freedom of expression in Sri Lanka. Some of the measures the subject of criticism included a requirement that only Sri Lankan citizens can apply for television broadcasting licences; political parties be prohibited from obtaining a television broadcasting licence; any licence granted be only for one year duration; any licence may be cancelled by the Minister for failure to comply with content restrictions; there be a committee to advise on the administration of television broadcasting appointed by the Minister; the Regulations required all kinds of organizational information 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.¹²⁸ Various civil society groups and private media institutions challenged the Regulations and were successful in getting the Supreme Court to grant an interim order suspending the Regulations.¹²⁹

Despite the fact that the laws were never 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.¹³⁰ 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’.¹³¹ 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.¹³²

The Regulations did not seek to distinguish between the vastly different models of television delivery using the Internet and Mobile telephones.¹³³ In particular there is an important distinction between the transmission of TV over IP networks (IPTV) and delivering TV generally over the open Internet.¹³⁴ 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.¹³⁵ To date Sri Lanka has had only one IPTV service, ‘PEO’ provided by Sri Lanka Telecom. Usually such services are delivered over an exclusive network managed by a

¹²⁸ Free Media Movement, ‘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/>> accessed 18 May 2010.

¹²⁹ ‘Draft paper formulated’, 3 April 2009 <<http://www.thefreelibrary.com/Draft+paper+formulated-a0199262018>> accessed 18 May 2010.

¹³⁰ Free Media Movement, above n 153.

¹³¹ Sanjana Hattotuwa, above n 65.

¹³² Free Media Movement, above n 153.

¹³³ Sanjana Hattotuwa, above n 65.

¹³⁴ Ibid.

¹³⁵ New Media Glossary. <<http://www.sag.org/content/new-media-glossary>> accessed 18 May 2010.

telecommunications company.¹³⁶ 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.¹³⁷ The latter essentially refers to video sharing websites YouTube, Vimeo and any other instances where Internet users upload videos for viewing by other users. Thus given that the Regulations doesn't 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 interest¹³⁸

Further the Regulations require 'Internet based television broadcasting stations' to a) have a ISP license or b) to enter in to an agreement with an ISP for the 'use of such network facilities required for the establishment and maintenance of such a broadcasting station'.¹³⁹ 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 in to 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'.¹⁴⁰ 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.¹⁴¹ 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 that an ISP or Telephony Network provider to monitor online video content. Moreover it could force ISPs to enter in to 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.¹⁴²

Moreover, the Regulations provide that a license for broadcasting television may be cancelled among other circumstances for broadcasting programs that are detrimental to the interests of national security, inciting

¹³⁶ Sanjana Hattotuwa, above n 65.

¹³⁷ Sanjana Hattotuwa, above n 65.

¹³⁸ 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>>

¹³⁹ Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 9.

¹⁴⁰ Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 10.

¹⁴¹ Sanjana Hattotuwa, above n 65.

¹⁴² Sanjana Hattotuwa, above n 65.

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.¹⁴³ 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 has blocked a host of websites, without any public acknowledgement of doing so, it is likely that ISPs will act even more cautiously and act to limit Internet content even further. More 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. 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 contents, it is often the case that other users can comment and provide responses to the video content. It was entirely questionable how an ISP would monitor such user generated comments to video content to comply with content restrictions on the Regulations. The Regulations also required that licence holders keep electronic copies of all materials broadcasted for a minimum period of sixty days.¹⁴⁴ 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.¹⁴⁵

The Regulations also prohibited the broadcasting of transmission which originated outside the territory of Sri Lanka unless permission had been granted by the Minister.¹⁴⁶ 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 that ISPs may have to block every website and Internet location containing video content originating outside the territory of Sri Lanka.¹⁴⁷

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

¹⁴³ Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 13(e).

¹⁴⁴ Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 16 (b).

¹⁴⁵ Sanjana Hattotuwa, above n 65.

¹⁴⁶ Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 26(1)(b).

¹⁴⁷ Sanjana Hattotuwa, above n 65.

channels that can be broadcast over the Internet.¹⁴⁸ 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.¹⁴⁹

The Regulations also prohibited any political party from holding a license for a private television broadcasting station or a network.¹⁵⁰ However given the unclear meaning of 'Internet based broadcasting stations' it is unclear whether political parties can use the Internet to disseminate video content. Further 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. Further given 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, potentially cutting off vital video content that can educate and inform them.

The Regulations are illustrative of the law maker's lack of understanding of the dynamics of the Internet and their complete disregard for freedom of expression both online and otherwise. 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 undermined the freedom of expression of end-users, including citizen journalists, professional media personnel and human rights activists.¹⁵¹

The fight on pornography

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.¹⁵² 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 of 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 connection. In June 2009 on an application brought by the Inspector General of Police, 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

¹⁴⁸ Sanjana Hattotuwa, above n 65.

¹⁴⁹ Sanjana Hattotuwa, above n 65.

¹⁵⁰ Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka), s 6.

¹⁵¹ Sanjana Hattotuwa, above n 65.

¹⁵² Daily News, 'TRC directed to filter obscene websites', Daily News, 2 August 2008 < <http://www.dailynews.lk/2008/08/02/news11.asp> > accessed 4 April 2010.

effective than the unofficial ban on websites such as Tamilnet.com. Four of the twelve banned pornographic websites continue to be available through a Dialog Internet connection.¹⁵³

In the post war context the government's concern over pornography has not lessened. Recently it was reported that the Women and Child's Bureau within the Police has formally requested from the TRC that pornography websites be banned from mobile phones.¹⁵⁴ Reportedly up to 400 websites could be banned under such a request.¹⁵⁵ Director General of the TRC has confirmed that it had received such a request, but has advised that to date it is waiting on Cabinet approval prior to implementing such a ban.¹⁵⁶

As critics at the time noted, protecting children from pornography is a worthy policy objective. However, question remains whether banning all pornography, even from adults is the appropriate response? It is a question that even other jurisdictions have grappled with. In Australia, when a similar move was mooted, the Internet service providers pointed to the unfeasibility and unworkability of such a broad filtering regime.¹⁵⁷ In America, 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.¹⁵⁸ Critics of the Chinese attempts to block pornography have pointed out that, the Chinese government under the auspices of 'blocking vulgarity' has also blocked other social and political content that is critical of Chinese government.¹⁵⁹

Post war developments

In the post war environment the government has not shown any signs of easing its stance on freedom of expression. In February 2010 it was reported¹⁶⁰ in the press that the TRC was to introduce new laws that would require all news websites to register with the TRC and that such sites would need to acquire internet protocol (IP) addresses from the TRC. It was further reported that the TRC would administer controls on the

¹⁵³ Sanjana Hattotuwa, 'Banning Sri Lankan porn online: a couple of month after', ICT for Peacebuilding, 31 January 2010 <<http://ict4peace.wordpress.com/2010/01/31/banning-sri-lankan-porn-online-a-couple-of-months-after/>> accessed 4 April 2010.

¹⁵⁴ Daily Mirror, 'Police seek mobile porn ban', Daily Mirror, 12 May 2010 <<http://srilankanewsfirst.com/politics/17315.html>> accessed 3 July 2010.

¹⁵⁵ Ibid.

¹⁵⁶ Ibid.

¹⁵⁷ James Kirby, 'The Net- Overseas pornography will filter through', Business Review Weekly, 12 November 1999 <<http://www.brw.com.au/stories/19991112/4092.htm>> accessed 4 April 2010.

¹⁵⁸ ACLU v Reno 535 U.S. 1 (2002).

¹⁵⁹ 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_bahrain_s_censorship_efforts_run_into_the_cute_cat_theory> accessed 4 April 2010.

¹⁶⁰ Bandula Sirimanna, 'Chinese here for cyber censorship', The Sunday Times, 14 February 2010 <http://sundaytimes.lk/100214/News/nws_02.html> accessed 4 April 2010.

Google search engine.¹⁶¹ Information Technology experts from China were to travel to Sri Lanka to assist the TRC to implement the new rules.¹⁶² Further, funds from the World Bank were to be used to implement the censorship program.¹⁶³ Subsequently the World Bank issued a statement asserting that there is no scope to utilize World Bank funds for an Internet censorship program.¹⁶⁴ 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.’¹⁶⁵ However it was also reported that the President has since ordered the suspension of the censorship program.¹⁶⁶

As to the role that the TRC was to play in any such program, its Director General Anusha Palpitiya denied that he had received any directive to take control of news websites. However alarmingly, Palpitiya acknowledged that ‘monitoring could not be ruled out’.¹⁶⁷ Former Director General Rohan Samarajiva questioned the authority of the TRC to implement such a censorship program. Samarajiva pointed out that under the Telecom Act does not provide the TRC with 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.¹⁶⁸

Websites that were blocked during the war continue to be unavailable. Websites such as Lankanewsweb.com and tamilcanadian.com/news/ does not operate on Sri Lanka Telecom’s ADSL connections. It has been argued that unlike during the war the motivations behind the ongoing blocking of such websites are different, 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’.¹⁶⁹ However as with the court sanctioned blocking of pornographic websites, the actual blocking is haphazard; some websites though unavailable on an ADSL connection continue to be available on HSPA.¹⁷⁰

Going in to the Presidential election the President released a Manifesto where he promised to address media freedom in the following manner:

¹⁶¹ Ibid.

¹⁶² Ibid.

¹⁶³ Ibid.

¹⁶⁴ 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>> accessed 4 April 2010.

¹⁶⁵ Bandula Sirimanna, above n 10.

¹⁶⁶ Ibid.

¹⁶⁷ Ibid.

¹⁶⁸ Rohan Samrajiva, above n 110.

¹⁶⁹ Kumar David, above n 117.

¹⁷⁰ 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/>> accessed 18 May 2010.

I will operationalise a mechanism which gives priority to produce accurate information and portray a true picture of the country to the rest of the world and thereby uplift the reputation of the country, instead of the current practice of certain media institutions which strive to tarnish the image of the country by portraying Sri Lanka as a state with an unsatisfying track record¹⁷¹

Such statements have been criticized as reflecting the government's intolerance for alternative and or dissident voices. After its win at the polls, the Government sought to signal an easing on media restrictions. It eased some emergency regulations and granted a pardon to the incarcerated journalist J. S. Tissainayagam.¹⁷² These moves are surely to be welcomed. However, as noted by observers the Government has a long way to go ensure freedom of expression both generally and online.

Structural causes

Finally it is important to make a note about the general culture within which freedom of expression operates in Sri Lanka. In particular there is a highly polarized political and social culture that has made it a difficult place to express not only political dissent but all forms of expression both online and otherwise. Those that agree with the status quo, whether political, social or cultural are branded patriots and those that don't are branded traitors. Even content that have remote connections to any identified public ill can become the subject of censure. Two recent examples are illustrative. First, in April 2010 American hip hop artist Akon was scheduled to perform in a concert sponsored by Maharajah Television. The concert was announced in the midst of the general election campaign and initial ticket sales soared. However soon after announcing the concert, a furor broke out over Akon's video clip 'sexy chic', which contained a pool party scene where a swim wear clad model is seen dancing in front of a decorative Buddhist statue.¹⁷³ The government refused to grant a visa to Akon and his concert in Sri Lanka was cancelled. The Cabinet ratified the decision to cancel the singer's visa on the basis that allowing the rapper to perform in Sri Lanka would be disrespectful to Buddhism.¹⁷⁴ Sections of civil society endorsed the Cabinet move; Facebook groups were created and thousands of supporters expressed their approval.¹⁷⁵ Thugs widely speculated to be

¹⁷¹ Ibid.

¹⁷² B Muralidhar Reddy, 'Pardon for Tissainayagam', The Hindu, 4 May 2010 < <http://www.hindu.com/2010/05/04/stories/2010050455871700.htm>> accessed 3 July 2010.

¹⁷³ Krishan Francis, 'Buddha uproar halts Akon show', MSNBC.com, 28 March 2010 < <http://www.msnbc.msn.com/id/36020442/ns/entertainment-music/>> accessed 18 May 2010.

¹⁷⁴ Indika Sri Aravinda, 'Pop star Akon in Cabinet', Daily Mirror, 24 March 2010 < <http://www.dailymirror.lk/index.php/news/2600-pop-star-akon-in-cabinet.html>> accessed 18 May 2010.

¹⁷⁵ One group was called Akon who disgraced Buddhism – Stop Sri Lanka Concert! (with 5125 supporters) and Akon! Don't insult any Religion & we don't want you to be in Sri Lanka! (with 3222 supporters).

sponsored by Minister Mervin Silva stoned Maharaja Television studios.¹⁷⁶ Ironically Minister Silva went on to win the General Election and was briefly appointed as the new Deputy Minister for Media. In a similar vein, in the same month, a Sri Lankan who was born a Buddhist that converted to Islam was arrested for writing a book about her religious conversion.¹⁷⁷ The author, Sarah Malanie Perera was a Bahraini resident and was travelling in Sri Lanka at the time of her arrest.¹⁷⁸ Perera was detained by the Defence Ministry under emergency powers for allegedly insulting Buddhism.¹⁷⁹ At present she has been released on bail however her trial is pending.¹⁸⁰

These examples are illustrative of both the culture of impunity that prevails and the hyper sensitivity of the authorities to anything that is seen to be (even remotely) undermining national security and or national identity. In the context of the Akon example, it is also illustrative of civil society's own intolerance and how easily it can be mobilized to support government's own views. Attempts to condemn such hypersensitivity is seen as unpatriotic and an effort driven by 'foreign / Western / NGO / dollar / kroner/ Terrorist / LTTE interests.'¹⁸¹ The result of such an environment is inevitably widespread self censorship in online media and other forums.

¹⁷⁶ Lasanda Kurukulasuriya, 'The Sirasa attack: Was Akon just an excuse?', Sunday Times, 28 March 2010 < http://sundaytimes.lk/100328/News/nws_79.html> accessed 18 May 2010.

¹⁷⁷ Islamic Human Rights Commission, 'Alert: Sri Lanka – Sri Lankan Muslim convert to be tried under Emergency Law Tomorrow', Islamic Human Rights Commission, 14 May 2010 < <http://www.ihr.org.uk/activities/alerts/9313-alert-sri-lanka-sri-lankan-muslim-convert-to-be-tried-under-emergency-law-tomorrow>> accessed 18 May 2010.

¹⁷⁸ Ibid.

¹⁷⁹ Ibid.

¹⁸⁰ Ibid.

¹⁸¹ Sanjana Hattotuwa, 'Freedom of Expression in Singapore vs Sri Lanka', ICT for Peacebuilding, 7 June 2009 <<http://ict4peace.wordpress.com/2008/06/07/freedom-of-expression-in-singapore-vs-sri-lanka/>> accessed 18 May 2010.

Legal limits to freedom of expression in Sri Lanka

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. Currently there are a host of laws that currently limit the full exercise of freedom of expression in Sri Lanka. Broadly these laws can be grouped in to two categories: national security laws and general laws. General laws are all laws that do not pertain to national security. Examples include 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 not just those that are communicated on the Internet. To date, these laws haven't been enforced with respect to online content in Sri Lanka. However their presence has to be considered as first and foremost they limit what can be discussed online. Second, these laws when applied to the online sphere can have novel and often unintended consequences. This section first 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 in the online sphere.

National Security Laws

There are three main problems with national security laws: they are often vague so their scope is difficult to determine; they are often over-broad, so that they cover matters that are insufficiently connected with national security to warrant censorship; and they impose harsh penalties that encourage self censorship. Broadly 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

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 doesn't 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.¹⁸² An

¹⁸² Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2).

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 essential to the life of community, the President may declare an Emergency.¹⁸³ There is no requirement of an 'exceptional threat' that is generally understood to be a condition precedent to the valid declaration of an emergency.¹⁸⁴ The discretion afforded to the President and allowing expediency to be factor is at odds with international standards, which require the 'life of the nation to be under threat' prior declaring a state of emergency.¹⁸⁵ Once an Emergency is in operation, the President is empowered to make such regulations as 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.¹⁸⁶

Emergency Regulations come in to force the moment they are made by the President¹⁸⁷ and have the legal effect of overriding all laws except provisions of the Constitution.¹⁸⁸ However, the Constitution itself permits emergency regulations to restrict certain constitutional provisions including article 14(1)(a) which guarantees freedom of expression.¹⁸⁹ Emergency Regulations do not have a permanent nature; their duration is limited to a period of one month from the date of coming in to effect.¹⁹⁰ However, they may be revoked before the end of the one month period or extended before or at the end of that period.¹⁹¹

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.¹⁹² Further, within fourteen days the proclamation must be approved by resolution in Parliament.¹⁹³ If Parliament does not approve a proclamation then the emergency ceases to be valid.¹⁹⁴

Sri Lanka has been under emergency rule almost uninterrupted for over three decades. During the cease fire period of 2001, emergency rule lapsed. However, once the government recommenced the

¹⁸³ Ibid.

¹⁸⁴ Asanga Welikala. A state of permanent crisis constitutional government, fundamental rights and states of emergency in Sri Lanka (2008), p199.

¹⁸⁵ Ibid.

¹⁸⁶ Public Security Ordinance No 25 of 1947 (Sri Lanka), s (5)(1).

¹⁸⁷ Public Security Ordinance No 25 of 1947 (Sri Lanka), s (11).

¹⁸⁸ Public Security Ordinance No 25 of 1947 (Sri Lanka), s (7).

¹⁸⁹The Constitution of the Democratic Socialist Republic of Sri Lanka 1978, s 15.

¹⁹⁰ Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2)(2).

¹⁹¹ Ibid.

¹⁹² Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2)(3).

¹⁹³ Public Security Ordinance No 25 of 1947 (Sri Lanka), s (2)(4).

¹⁹⁴ Ibid.

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.¹⁹⁵ 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 extraordinary powers.¹⁹⁶ As a result the public has become accustomed to the government's expanding role and less likely and willing to question the government.¹⁹⁷

Emergency regulations most commonly limit freedom of expression by either imposing a complete prohibition on the reporting of certain subjects and or requiring that news reports 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.¹⁹⁸

Even more than one year after the war Sri Lanka continues to be in a state of emergency.¹⁹⁹ However as of May 2010 many of the emergency regulations have been relaxed. Emergency Regulations relating to holding meetings and gatherings, curfews, printing literature and providing householder's names to the police was relaxed.²⁰⁰ However the military continues to enjoy wide police powers to investigate suspected terrorist activities.²⁰¹

¹⁹⁵ 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/>> accessed 1 June 2010.

¹⁹⁶ Ibid.

¹⁹⁷ Ibid.

¹⁹⁸ Article 19, War of Words: Conflict and Freedom of Expression in South Asia Thematic Reports, (May 2005), p 66.

¹⁹⁹ Extraordinary Gazette Notice no 1651/24 (Sri Lanka), 2 May 2010.

²⁰⁰ Colombo Page, 'Sri Lankan government relaxes emergency regulations', Colombo Page, 4 May 2010 < http://www.colombopage.com/archive_10/May1272987911JV.php> accessed 1 June 2010.

²⁰¹ Ibid.

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.²⁰² 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. These decisions are considered in the following section.

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 operations as part of the Government's commitment not to arrest anyone under the PTA. However, with the resumption of the war, and 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 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 in to force as a means of regulating the press. It establishes a Press Council to regulate the press.²⁰³ The council is constituted by the Director for Information and six other members appointed by the President.²⁰⁴ The objects of the council are inter alia to ensure freedom of the press and ensure high standards of journalistic ethics.²⁰⁵ 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

²⁰² Public Security Ordinance No 25 1947 (Sri Lanka), s 3.

²⁰³ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s2.

²⁰⁴ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s3.

²⁰⁵ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s8.

has been published in a newspaper or where there has been a breach of journalistic ethics.²⁰⁶ After such an inquiry the council has the power to order a correction, censure the proprietor, editor or journalist or order an apology be tendered.²⁰⁷ An order made by the Council is deemed final and cannot be questioned in a court of law.²⁰⁸

A 'newspaper' is defined in the Act as 'any paper containing public news, intelligence or occurrences printed or published in Sri Lanka...'²⁰⁹ 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 in to the following broad categories: obscenity and profanity,²¹⁰ government decision making,²¹¹ fiscal policy²¹² and official secrets.²¹³ Section 16(1) makes it an offence to publish any proceeding of a cabinet meeting without prior approval of the secretary of 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 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 a legal action within the specified time frame.²¹⁴

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 unauthorized person.²¹⁵ An official secret is widely defined to including any

²⁰⁶ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s9.

²⁰⁷ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s9(1)(a)-(c).

²⁰⁸ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s9(5).

²⁰⁹ Sri Lanka Press Council Law No.5 of 1973, s 33.

²¹⁰ Sri Lanka Press Council Law No 5 of 1973 (Sri Lanka), s15(1)(a),(d).

²¹¹Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s16(1),(2),(5).

²¹² Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s16(4).

²¹³ Sri Lanka Press Council Law No 5 of 1973(Sri Lanka), s16(3).

²¹⁴ 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.

²¹⁵ Official Secrets Act No 32 of 1955 (Sri Lanka), s 7.

information relating to any arm of the armed forces; any implements of war maintained for use in the service of the country; any equipment, organization 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 defenses of Sri Lanka.²¹⁶ Similar to the Press Council Laws this Act has not been used that widely. However, critics argue that by its mere presence, laws such as these have a ‘chilling’ effect.

Defamation

In 2002 Sri Lanka repealed laws relating to criminal defamation. Civil defamation can be established if the publication is ‘malicious’.²¹⁷ 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 to a defamation case.

Contempt of Court

The courts have defined what constitutes contempt in a very conservative fashion. Contempt has been found in publications that suggested judges were responsible for a serious breach of duty in taking unauthorized holidays by going to race meets and thereby contributing to arrears of work.²¹⁸ In the *Ceylon Daily News*²¹⁹ case a deputy editor was imprisoned for six months for commenting that a judge’s criticism of 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 of 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 untrammelled 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 ‘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 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

²¹⁶ Official Secrets Act No 32 of 1955 (Sri Lanka), s 27(1).

²¹⁷ *Jayawardane v Aberan* (1964) Ramanathan Reports.

²¹⁸ *Re Hulugalle* 39 NLR 294.

²¹⁹ *Re Hulugalle* 39 NLR 294.

rule has the capacity to seriously impede the discussion of matters of public interest.²²⁰ In *A.M. E. Fernando v Attorney General* (2003) 2 SLR 52, a human rights activists 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 courts and court of appeal to punish for contempt. There are no procedures to regulate the contempt of court inquiries. Section 136 of the Constitution, authorizes 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 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 per with other legislation, there are overbroad 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

²²⁰ Human Rights Commission, *Contempt of Court the need for substantive cum procedural definition and codification of the law in Sri Lanka* (2005), p 11.

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 in to 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, dramas and other entertainments.²²¹ Under the power to make regulations, the Minister can issue, withdraw or suspend permits for the exhibition of such performances.²²²

Obscene Publications Ordinance

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.²²³ However the Act doesn’t 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.²²⁴ 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.²²⁵ There is an inbuilt defence by way of ‘fair comment and fair criticism’.²²⁶

²²¹ Public Performances Ordinances No 7 of 1912 (Sri Lanka), s 3.

²²² Public Performances Ordinances No 7 of 1912 (Sri Lanka), s 3(e).

²²³ Obscene Publications Ordinance No 4 of 1927 (Sri Lanka), s 2.

²²⁴ Profane Publications Act No 41 of 1958 (Sri Lanka), s 2.

²²⁵ Profane Publications Act No 41 of 1958, s 5.

²²⁶ Profane Publications Act No 41 of 1958 (Sri Lanka), s 2.

Enforcing content restricting laws to the online sphere

The preliminary issue with respect to such laws and the Internet is jurisdiction. There is currently a heated debate both in academia and in court rooms around the world as to how to establish jurisdiction when online content falls foul of what is deemed to be legally acceptable. The Internet allows for content that is uploaded in one jurisdiction to be available in another, and what is permissible in one jurisdiction may not be in another. In the much publicized case of *Dow Jones v Gutnick* (2002) HCA 56, an online publication owned by the Dow Jones publishing firm, contained an article titled *Unholy gains* which made several references to Joseph Gutnick. The article was uploaded in New Jersey, United States and it was accessible by Internet users all over the world. Gutnick alleged that the references were defamatory and sued the Dow Jones company in a court in Australia. Joseph Gutnick is a world famous, Australian based mining entrepreneur. The Australian court held that, though the offending article wasn't published in Australia, it had jurisdiction to hear the matter. The Australian court held that given that Australia is Gutnick's primary place of residence that was where damage to his reputation occurred. The decision was highly criticized especially in the United States, as the content in question was legally permissible in New Jersey owing to the very strong constitutional free speech guarantees in the United States. The Gutnick case ultimately went on to be settled out of court, with Dow Jones agreeing to pay Gutnick damages. However, had the Court made the ruling that Dow Jones fell afoul of Australian defamation laws and ordered that content be taken down, it would have potentially had the catastrophic consequence that what is not permissible in Australia, be not available to Internet users all around the world. Currently there is no solution to this issue. Each country has its own rules as to when it can establish jurisdiction. Until governments around the world come to a global consensus as to how jurisdiction can be found in such cases disparities such as that in *Dow Jones v Gutnick* will continue.

The second key consequence of such laws is that they limit what can be written or published about in the online sphere. Governments are currently grappling with how best to enforce these laws and police online content. At its worst, some of these laws can result in criminal penalties. To date a record number of 120 bloggers and Internet users are behind bars all over the world.²²⁷ In a much publicized case from Italy, a court held that a video uploaded to YouTube in Italy, offended Italian privacy laws.²²⁸ However, controversially the Court went on to find that, three executives from Google (YouTube's parent company) were criminally responsible for the failure to monitor the content uploaded on its website.²²⁹ There was much criticism of the decision; Google argued that 20 hours of video content is uploaded on to YouTube every minute thus, it is an impossible feat for it to monitor and censor offending content.²³⁰

²²⁷ Lucie Morillon and Jean-Francois Julliard, 'Web 2.0 versus Control 2.0', Reporters Without Borders, 2 June 2010 <<http://www.europarl.europa.eu/document/activities/cont/201005/20100527ATT75115/20100527ATT75115EN.pdf>> accessed 28 June 2010.

²²⁸ Rachel Donadio, 'Larger threat is seen in Google case', New York Times, 24 February 2010 <<http://www.nytimes.com/2010/02/25/technology/companies/25google.html>> accessed 1 June 2010.

²²⁹ Ibid.

²³⁰ Ibid.

Other than direct prosecution of individuals, governments attempt to police online content by requiring ISPs or individual users to monitor content. In South Africa, the government has inquired from the South African Law Reform Commission whether it could legislate a requirement that service providers block pornography on the Internet, mobile phones and television.²³¹ As noted above Australia is proposing to soon pass a law that requires ISPs to filter certain prescribed materials.

Also unlike other modes of publication and speech, publication through the Internet can raise novel fact scenarios, that traditional legal doctrines aren't necessarily best equipped to solve. And at times there can be unique and unintended consequences when such laws are applied to the online sphere. In a classic example from Briton, a young man was arrested after joking on twitter that he would blow Robin Hood Airport 'sky high' if his flight was delayed.²³² The offender was convicted under s 127 of Briton's Communications Act, which prohibits obscene, indecent or menacing messages.²³³ The accused was ordered to pay £1000 and court costs. The decision was criticized as a criminal conviction was considered too severe a punishment for such behavior.²³⁴

²³¹ BBC, 'Porn ban on net and mobiles mulled by South Africa', BBC, 28 May 2010 < <http://news.bbc.co.uk/2/hi/technology/10180937.stm>> accessed 1 June 2010.

²³² Robert Mackey, 'Briton convicted for 'Menacing tweet against Robin Hood Airport'', New York Times, 10 May 2010 < <http://thelede.blogs.nytimes.com/2010/05/10/briton-convicted-for-menacing-tweet-against-robin-hood-airport/>> accessed 1 June 2010.

²³³ Ibid.

²³⁴ Ibid.

Case study

Recently in Sri Lanka the police arrested two men over the content of their text messages. In January 2010, during the Presidential election, a man was arrested over an attempt to 'disgrace the government'.²³⁵ The man in question was also reported to be a supporter of the Opposition (UNP).²³⁶ In June 2010, another man was arrested after he sent a prank SMS to his wife claiming that LTTE suicide bombers were going to attack Anuradhapura.²³⁷ The wife was in Anuradhapura at the time on a pilgrimage.²³⁸ The SMS warned that at least twelve LTTE suicide bombers were in Anuradhapura.²³⁹ The police claimed that the SMS had caused panic in the area. (See footnote 240)

These arrests illustrate several points about how these content restricting laws can apply to the online sphere. Similar arrests could easily take place over the similar messages sent over Twitter, Facebook or even via email. In the context of the first message, it is unclear what the content of the message was, or even how the Police came to know of its contents. It is unclear whether an attempt to disgrace the government was mere political criticism or whether it was something more sinister.

With regards to the prank SMS, on the one hand, (especially given Sri Lanka's past) the Police were well within their duties to investigate claims about a future terrorist attack. If they hadn't investigated the SMS, it could even be argued that they were derelict in their duties. On the other hand it is also possible to argue as with the British twitter example, that there ought to be civil penalties rather than criminal penalties for these unintended breaches of the law.

Finally as noted before, much of what restricts freedom of expression in Sri Lanka, are extralegal actions. Even in these two cases the basis for the arrests are unclear. It is possible that the arrests were made under any number of laws including the PTA, Penal Code or under an Emergency Regulation. It is also important to keep in mind, that often in the past the Police have not identified a clear legal basis prior to an arrest. In such instances the Attorney General's department has retroactively created a legal basis which courts have been fully willing to accept.

Another important consideration with respect to such laws and the Internet, is that though such laws are difficult to detect and enforce in the online world, once detected, the veneer of anonymity afforded on online platforms can be easily stripped away to hold account those that offend the laws. In an example from India, 22 year old Rahul Krishnakumar Vaid posted an obscene message about Congress Party Leader, Sonia Gandhi on an Orkut community called I hate Sonia Gandhi.²³⁵ A Congress party activist saw the message and alerted the authorities.²³⁶ The authorities asked Google to provide them with the IP address

²³⁵ Tech2, 'Obscene Orkut Post Lands Youth in Prison', Tech2.in, 20 May 2008 <<http://tech2.in.com/india/news/internet/obscene-orkut-post-lands-youth-in-prison/36611/0>> accessed 18 May 2010.

²³⁶ Ibid.

of the person who posted the message.²³⁷ Google released the information to the police and Vaid was arrested from his home and charged under s 67 of the Information Technology Act 2000 (India) and s 292 of the Indian Penal Code.²³⁸ Section 67 of the Information Technology Act 2000 makes it an offence to publish information that is obscene in an electronic form. Section 292 of the Indian Penal Code makes it an offence to inter alia publish or distribute obscene material. Article 19(1)(a) of the Indian Constitution guarantees to all citizens the right to 'freedom of speech and expression'. However Article 19(2)(a) of the Indian Constitution provides that reasonable restrictions can be imposed including in the interests of inter alia 'decency' and 'morality'. The Indian Supreme Court has held that s 292 of the Indian Penal Code is a permissible restriction on the freedom of expression as it seeks to promote public decency and morality.²³⁹

Orkut is owned by Google. When an individual signs up for an Orkut account, he or she agrees to accept Google Terms of Service, Orkut Additional Terms and the Google Privacy Policy.²⁴⁰ The Google Privacy Policy expressly provides that it will share personal information where Google has good faith belief that sharing of the personal information is necessary inter alia to "satisfy any applicable law, regulation, legal process or an enforceable governmental request."²⁴¹ Thus, Orkut faced by a demand from law enforcement agencies or a subpoena from an individual seeking to press a defamation claim, would be well within its rights to disclose the identity of its users.

These examples from foreign jurisdictions are illustrative of the novel ways these content restricting laws can be applied. In Sri Lanka, though these laws haven't yet been enforced in the online sphere, their mere existence alone warrants concern. In particular, the emergency regulations and the PTA combined with the culture of violence against those who speak out, has created a far more effective culture of self censorship that limit freedom of expression. Both Internet users and Regulators need to be aware that existing content restricting laws can have challenging application to the online sphere.

²³⁷ Ibid.

²³⁸ Michael Arrington, 'Hit pause on the evil button: Google assists in arrest of Indian man', Washington Post, 19 May 2008 <<http://www.washingtonpost.com/wp-dyn/content/article/2008/05/18/AR2008051800657.html>> accessed 18 May 2010.

²³⁹ Ranjit v Udeshi v State of Maharashtra AIR 1965 SC 881.

²⁴⁰ Orkut, Orkut Account Creation < <http://www.orkut.com/PreSignup>> accessed 18 May 2010.

²⁴¹ Google, Google Privacy Policy < <http://www.google.com/privacypolicy.html>> accessed 18 May 2010.

Freedom of expression in 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 or its exceptions meet 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 International Covenant on Civil and Political Rights (ICCPR). To date, the Supreme Court has not had an opportunity to consider the applicability of the guarantee to the Internet. However, the Court's rulings on right to publish cases can be illustrative. The court has recognized that it is a per se permissible exercise of the freedom of speech to support or criticize the government, political parties and policies of the government. Further it is not permissible to impose unequal governmental controls on private publications. However, 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.

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 and unwritten laws shall be valid and operative notwithstanding any inconsistency with the fundamental rights declared and

recognized by the Constitution. This significantly undermines the protection of the constitutional rights guaranteed and the supremacy of the constitution.²⁴² 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 where by 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 favor the State in constitutional rights cases, especially in cases that deal with restrictions imposed under emergency laws.²⁴³

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.'²⁴⁴ Unlike, the ICCPR under the Sri Lankan Constitution there is no express requirement that restrictions on constitutional rights be 'reasonable or necessary'.²⁴⁵ 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) 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.

Relevantly the Court held that the Internet enjoys full protection under the first amendment free speech guarantee.²⁴⁶ 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

²⁴² 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.

²⁴³ *Sunila Abeysekara v Ariya Rubesinghe and Others* (2000) 1 SLR 314; Rohan Edrisinha & Asanga Welikala, above n 280, p 133.

²⁴⁴ Rohan Edrisinha & Asanga Welikala, above n 280, p 131.

²⁴⁵ *Malagoda v AG* (1982) 2 SLR. 777.

²⁴⁶ *ACLU v Reno* 521 U.S. 844 (1997), 869.

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'.²⁴⁷

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. 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,²⁴⁸ and non speech forms of political protest²⁴⁹ 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 doubts 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.²⁵⁰

In numerous subsequent judgments 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 criticized 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 were breached. Though the court didn't 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 that the freedom protects not only speech that we agree with but also speech that we find repulsive.²⁵¹ Similarly in *Amaratunga v Sirimal (1993) 1 SLR 264* the right to support or criticize the Government, political parties, policies and programs is per se a permissible exercise of the freedom of speech and expression under Article 14 of the Constitution.

²⁴⁷ Ibid.

²⁴⁸ *Karunathilaka v Dayanand Dissanayake (No. 1) (1999) 1 SLR 157.*

²⁴⁹ *Amaratunga v Sirimal (1993) 1 SLR 264.*

²⁵⁰ *Joseph Perera v AG (1992) 1 SLR 199, at 202 per Sharvananda CJ.*

²⁵¹ *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.*

Further 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 guilty²⁵²

In that 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.²⁵³

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 regards to article 14(1)(a) the Court held that had the news item been broad casted 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.

²⁵² *Victor Ivan v Sarath N. Silva Attorney General and Others* (1998) 1 SLR 340, 347 per Fernando J.

²⁵³ *Victor Ivan Majuwana Kankanamge v Sri Lanka CCPR/C/81/D/909/2000* at para 9.4.

The court has also recognized 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 government broadcasted educational program challenged the government's actions when the program was arbitrarily stopped from being aired. The petitioner argued that he was not only a regular listener but also participated in the program on several occasions. The Court held that the freedom of speech of the petitioner qua participatory listener has been infringed, because the stoppage of the program prevented further participation by him.²⁵⁴

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. However, for the private sector broadcasters 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 the media publications the freedom of speech and expression enshrined in the Constitution were impinged upon. However in deciding that freedom of expression was impinged, the Court went to quote from earlier judgments 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'.

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 allowing 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 *Joseph Perera* still concluded that overbroad and vague national security laws can restrict constitutional rights.

In *Visvalingam v Liyanage* (1984) (2) SLR 305 the Petitioner complained against prohibition of the publication of the publication of "Saturday Review" a regional newspaper published in Jaffna. Though, censorship was

²⁵⁴ Fernando J at 180.

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 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 apprehension 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 there 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 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 that²⁵⁵

²⁵⁵ [2000] 1 SLR 314, 337.

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 using 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 organizers 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 '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 decision is especially significant as it was the first time that the Court recognized 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 screening of the film *Purahanda Kaluwara* (Death on a Full Moon Day) would be a violation of the Emergency Regulation 14 (same as that considered in the *Abeysekera* case above). 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 regards to the Minister's direction, the Court held it to be invalid as the relevant Act only authorized the Minister to give general directions related to policy. Further under the relevant emergency regulation only certain kinds of persons were prohibited from publishing, they 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 cases²⁵⁶ however even in those cases the decisions were criticized for the Court's failure to appropriately balance the competing interests. In *Abeysekera v Rubesinghe* an emergency regulation prohibited the publication of military operations in the North and the 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 authorized by the commander in chief to assist in the preserving national security. The petitioner, a human rights activist alleged that the regulation was overbroad 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

²⁵⁶ *Abeysekera v Rubesinghe* (2000) 1 SLR 314; *Wickremabahu v Herath* (1990) 2 SLR 348.

between the competing interests of national security and freedom of expression. The Court held that the Regulation in question was not overbroad, 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 speech²⁵⁷.

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 recognized 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.

Further 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 program would infringe the freedom of speech of the listener, it is possible to argue that arbitrarily blocking websites would infringe the freedom of speech of the reader. Further the Court has held that imposing unequal controls 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 the freedom of speech guarantees. The *Joseph Perera Case* may have special application in the context of websites. Requiring websites to register or a website licensing scheme would amount to the sort of pre 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 *Joseph Perera* it would be necessary 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.

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

²⁵⁷ *Abeysekera v Rubesinghe* (2000) 1 SLR 314, 378 per Amersainghe J.

protect their sources the same way traditional journalists can.²⁵⁸ 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 in a court in New Jersey held that traditional journalists who publish in the online sphere are entitled to be considered as journalists; however not so bloggers.²⁵⁹ The court held that the blogger could not be protected as a journalists as she “exhibited none of the recognized qualities or characteristics traditionally associated with the news process, nor has she demonstrated an established connection or affiliation with any news entity.”²⁶⁰

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 yet be developed in 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 recognizes 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

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

²⁵⁸ Jason O’Grady v Apple Computer Inc, Court of Appeal of the State of California, Sixth Appellate District.

²⁵⁹ 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>> accessed 1 June 2010.

²⁶⁰ Ibid.

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 newspapers²⁶¹

However it is important to note that what rights that 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 news print, 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, that allows over-broad national security legislation to trump civil liberties.

The Internet and Privacy

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.²⁶² Therefore 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 recognized 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 broader 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 recognized such a right under the right to liberty. Additionally 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 such information is not just available to government authorities or telecommunication service providers. Almost anyone can access information, especially such information as locating 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

²⁶¹ Colombo Declaration on Media Freedom and Social Responsibility, October 2008 < http://ict4peace.files.wordpress.com/2009/03/declaration_eng.pdf> accessed 15 July 2010.

²⁶² Althaf Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective', *Scripted* 5(3): 553-574, p 558.

your own computer.²⁶³ '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.²⁶⁴ 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.²⁶⁵ More worryingly there are surveillance expert companies that are developing ways to better snoop and also to analyze the content of information communicated, and selling this technology to governments around the world, regardless of their records on human rights.²⁶⁶ In this regard, (as noted in the first section) it is important to note that French and Dutch governments are proposing international guidelines to stop private firms from exporting Internet surveillance technologies.²⁶⁷

Before delving into the current limitations of Sri Lankan privacy laws, it is first helpful to understand the way in which the Internet can undermine an individual's privacy. Outlined on the next page are few of the common ways privacy can be undermined through the Internet.

²⁶³ Daniel Soar, 'Short Cuts', London Review of Books, 14 August 2008 < <http://www.lrb.co.uk/v30/n16/daniel-soar/short-cuts>> accessed 1 June 2010.

²⁶⁴ Ibid.

²⁶⁵ Ibid.

²⁶⁶ 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/>> accessed 1 June 2010.

²⁶⁷ Yahoo!, Above n 17.

Common ways privacy can be undermined on the Internet

Cookies	A text file that will be created in the computer each time a user accesses certain websites. It stores information about the user. For example, it may store information about certain preferences shown by the user such as which part of the website the user frequently accesses, the time spent on the websites and the user's preferred content. Cookies can be disabled in Internet Explorer and Netscape Navigator. However then the user cannot access websites that require cookies. Websites can record information about the user's preferences and adapt according to the user. For example pop-up advertisements can be generated based on information gathered through cookies.
Web bugs	Another mechanism through which a user's movements online can be traced. It traces the movements of the mouse and cursors. A simple example is they can be forwarded with emails and it can be determined if the email has been read or forwarded by the recipient.
Spyware	A program that installs itself without the user's permission. Spyware can then gather information and communicate it to third parties such as manufacturers, retailers and market research firms.
Botnets	A Botnet is a network of zombie computers, consisting possibly of thousands of computers which can automatically send out messages, possibly destructive ones that could cause a computer to cease functioning.
Social Networking websites	Social networking websites such as Facebook and MySpace allow individuals to share significant amount of personal information online. This information can be easily stolen or misappropriated.
Phishing	A process whereby sensitive information such as usernames, passwords and credit card details are acquired by posing as a trustworthy entity. Typically an e-mail is sent out, directing the user to enter details at a fake website that looks identical to the legitimate website. Emails purporting to be from popular social web sites (Youtube, Facebook) banks, IT Administrators (Yahoo, Google) are commonly used to acquire information from unsuspecting users.

Constitutional Protection

Broadly speaking, privacy has four aspects, information privacy (rules relating to collection and handling of personal data e.g. credit information), bodily privacy (protection of the individual's physical selves), privacy of communication (privacy of email, telephones, text messages etc) and territorial privacy (setting limits on intrusion in to the domestic and other environments).²⁶⁸

Privacy is not a constitutionally protected right in Sri Lanka. However the Courts have recognized 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 recognized a right to household privacy among adjoining landowners to protect his fence with the covering of ola leaves.²⁶⁹ Similarly the courts have recognized 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 appeal²⁷⁰ 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).²⁷¹

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 recognized 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 individual²⁷²

...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.

²⁶⁸ Althaf Marsoof, above n 300, p 558.

²⁶⁹ Chinnapa et al v Kanakar et al 13 NLR 157 at 158-160.

²⁷⁰ A.M.K. Azeez v W.T. Senevirathne (SI Police) 69 NLR 209, 210.

²⁷¹ Althaf Marsoof, above n 300, p 558.

²⁷² *Sinha Ratnatunga v State*, 2 SLR 172, at 212.

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.²⁷³

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.²⁷⁴ For example the right to freedom of expression could be expanded to include a right to privacy.²⁷⁵ If an individual only intends to communicate with a selected recipient then third parties should not have access to the contents of the communication.²⁷⁶ To take an Internet example, if a website only permitted access to those who had been given permission to do so, a hacker that gains unauthorized access would be violating the 'privacy' of the website owner.²⁷⁷ 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.²⁷⁸ Using such reasoning it has been suggested that an Internet user should also have a right to free movement (to surf) freely and without fear, and mechanisms such as spyware, web bugs, cookies would impede this right of 'movement.'²⁷⁹

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 touches 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 program' which seeks "to adopt ICT in all its aspects to make government more efficient and effective,

²⁷³Sinha Ratnatunga v State, 2 SLR 172 at 213.

²⁷⁴ Althaf Marsoof, above n 300, p 570.

²⁷⁵ Althaf Marsoof, above n 300, p 571.

²⁷⁶ Ibid.

²⁷⁷ Ibid.

²⁷⁸ Ibid.

²⁷⁹ Althaf Marsoof, above n 300, p 571.

improve access to government services and create a more citizen centric government.”²⁸⁰ The government has been criticized for attempting to introduce such a program in the of absence of a data protection law or privacy protection for individuals.²⁸¹ 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.²⁸²

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.²⁸³ ‘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.²⁸⁴ 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 connection 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 connection with a criminal investigation.²⁸⁵ For the purposes of sections 52 and 54 ‘usage information’ means information relating to the identity of calling or called subscriber.

However the Telecom Act has also been the subject of criticisms as several provisions potentially serve to undermine privacy. For example there are several offences in the Telecom Act that makes it an offence for an employee of a telecommunication service provider to inter alia interfere with the contents of any

²⁸⁰ 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> accessed 1 June 2010.

²⁸¹ Privacy International, ‘Republic of Sri Lanka’, Privacy International, 18 December 2007 <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559488#\[21\]](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559488#[21])> accessed 1 June 2010.

²⁸² ICTA, above n 319.

²⁸³ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 73.

²⁸⁴ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 73.

²⁸⁵ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54(4).

message,²⁸⁶ or intercept any message.²⁸⁷ 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'²⁸⁸, 'as directed by a court'²⁸⁹, under 'a direction of the Minister'²⁹⁰, 'in connection with the investigation of any criminal offence'²⁹¹ or 'for the purpose of any criminal proceeding'²⁹². 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?²⁹³ Under what circumstances can a Minister issue a direction to interfere or intercept a message?²⁹⁴ What guidelines inform a Minister's decision? Do employees of a telecommunication service have any capacity to refuse a Minister's direction?²⁹⁵ 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 connection with the investigation of any criminal offence or for the purpose of any criminal proceedings?²⁹⁶ What level of authority would be required? Do such directions have to be in writing or merely verbal?²⁹⁷ 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?²⁹⁸ Finally, to what extent are customers adequately informed that their communications might not be private?²⁹⁹

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 privacy of consumers.³⁰⁰ Disclosure policies and any amendments to such policies be made public so that consumers are fully

²⁸⁶ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 49.

²⁸⁷ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54.

²⁸⁸ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 49(c).

²⁸⁹ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 49 (C).

²⁹⁰ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54(3).

²⁹¹ Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54(3).

²⁹² Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended), s 54 (3).

²⁹³ Chandra Jayaratne, An extract of a note on protecting personal information, Email Message to Sanjana Hattotuwa, sent 4 April 2010.

²⁹⁴ Ibid.

²⁹⁵ Ibid.

²⁹⁶ Ibid.

²⁹⁷ Ibid.

²⁹⁸ Ibid.

²⁹⁹ Ibid.

³⁰⁰ 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.

informed.³⁰¹ Circumstances where a Minister may issue directions to intercept or interfere with communications be clarified to operators and be published in the gazette so that consumers are fully informed of the limits on their privacy.³⁰² Similarly circumstances where employees of telecommunication service providers may make disclosures in connection with criminal investigations or criminal proceedings be published, and actual instances of cooperation be notified to the TRC.³⁰³ Further that TRC monitor enforce such regulations and guidelines in order ensure privacy of consumers.³⁰⁴

Computer Crimes Act

Further the Computer Crimes Act introduced numerous offences to protect computer users from unauthorized 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 in to 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 program and reports it back would amount to a hacking offence.³⁰⁵ 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 the user must agree to in order to access the website.³⁰⁶ Section 4 of the Computer Crimes Act makes it an offence to 'crack' in to a computer. Section 4 applies where,

- a) a person secures access to a computer or any information held in any computer;

³⁰¹ Ibid.

³⁰² Ibid.

³⁰³ Ibid.

³⁰⁴ Ibid.

³⁰⁵ Sunil Abeyaratne, Introduction to Information and Communication Technology Law (2008), p 94.

³⁰⁶ Sunil Abeyaratne, above n 344, p 95.

- 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.³⁰⁷

Section 5 makes it an offence to cause a computer to perform a function without lawful authority. Section 5 provides 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 unauthorized modification or damage of any computer, computer system or program. The Computer Crimes Act provides that examples of unauthorized modification or damage or potential damage to any computer include the following:

- a) impairing the operation of any computer, computer system or the reliability of any data or information held in any computer; or
- b) destroying deleting or corrupting or adding moving or altering any information held in any Computer; or
- c) makes use of computer service involving computer time and data processing for the storage or retrieval of data; or
- 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.³⁰⁸

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.³⁰⁹ 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.³¹⁰ 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,

³⁰⁷ Ibid.

³⁰⁸ Ibid.

³⁰⁹ Computer Crimes Act No 24 of 2007 (Sri Lanka), s8.

³¹⁰ Computer Crimes Act No 24 of 2007 (Sri Lanka),s 38

destination, route, time, data, size, duration or details of subscriber information'.³¹¹ Therefore, anyone who surveils an Internet user could be in violation of the Act. Computer is defined so broadly, it 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.³¹²

Further the Act makes it an offence for any person, without law 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.³¹³

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.³¹⁴ His Honor criticized the police's ability to detect and investigate computer crimes.³¹⁵ Many judges themselves are computer illiterate, though training programs were underway to improve computer literacy.³¹⁶ Ironically, certain investigative provisions under the Computer Crimes Act have been criticized for intruding 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 authorize the tapping. However it has been suggested that this is not a sufficient safeguard given that first, 'warrants are available for the asking'³¹⁷ and second, the requirement of a warrant can be dispensed with in cases of urgency.³¹⁸

These examples from foreign jurisdictions are illustrative of the novel ways these content restricting laws can be applied. In Sri Lanka, though these laws haven't yet been enforced in the online sphere, their mere existence alone warrants concern.

³¹¹ Computer Crimes Act No 24 of 2007 (Sri Lanka), s38.

³¹² Sunil Abeyaratne, above n 344, p 102.

³¹³ Computer Crimes Act No 24 of 2007 (Sri Lanka), s 10.

³¹⁴ Lanka Business Online, 'Crime Alarm', Lanka Business Online, 29 January 2009 <<http://www.lankabusinessonline.com/fullstory.php?nid=257786312>> accessed 25 May 2010.

³¹⁵ Ibid.

³¹⁶ Ibid.

³¹⁷ Sunil Abeyaratne, above n 344, p 558.

³¹⁸ Computer Crimes Act No 24 of 2007 (Sri Lanka), s 18(2).

Case Study: Presidential New Year Message

On 1 January 2010 all five mobile phone service operators (Operators) sent a text message to all mobile phone subscribers in Sri Lanka, purporting to be a message of good wishes from President Mahinda Rajapaksa.

The message stated “Kiwu paridi obata NIDAHAS, NIVAHAL RATAK laba dunnemi. Idiri anagathaya sarwapparakarayenma Wasanawantha Weva! SUBA NAWA WASARAK WEVA! Mahinda Rajapaksa” (As I promised, I gave you a free independent country. May your future be successful in all ways. Happy New Year!)

On 1 January 2010, Daily Mirror Online reported that one Operator had sent the SMS to all their subscribers pursuant to a request from the President's Office. On 2 January 2010 Weekend Financial Times reported that ‘...the Telecommunication Regulatory Commission instructed all five operators to transmit an SMS containing President's New Year Wish to all 12 million subscribers’. According to the Weekend Financial Times one of the operators, Dialog Telekom had stated that the New Year Message was sent based on instructions received from the TRC and in line with prior practice with respect to the transmission of a message as instructed by the Commission, Dialog did not levy any charge from the Commission for the transmission of the message.

When a subscriber contacted Dialog and requested to opt out from any further subscriptions the subscriber was told they could not do so as the message came from the President. It raises important questions about the responsibilities of a Telephone company *vis a vis* the personal information they collect and record from their customers. In particular what right if at all does an Operator have to pass on the private telephone numbers of their customers for non-essential, partisan communications?

In the broader context of elections the text message raises further questions about use of state resources, election funds and good governance. At the time the President was a candidate in the presidential election along with 21 other candidates. In effect the President, while serving his office, used his powers to instruct a government body (the TRC), to send out text messages that advance his presidential campaign, free of charge. The TRC is a public body and its broad mandate is to regulate and arbitrate telecommunication issues in the public interest. It is run with tax payer money. It is entirely questionable whether advancing partisan causes is within its mandate? If one were to examine the Sri Lanka Telecommunications Act No. 25 of 1991 (As amended) and the TRC's stated objects and powers, it would be easy to conclude that such actions are far beyond the legal purview of the TRC.

At one rupee per message, to 12.6 million subscribers, the cost of the text message comes to approximately USD\$110,000. Given that the President did not pay for the text message, the mass SMS amounts to a USD\$110,000 campaign donation on behalf of the Operators. Moreover, one of the Operators, Mobitel is half owned by the Government, thus New Year messages received by Mobitel subscribers, were partially paid for by the Sri Lankan tax payer.

Indian experiences

In India where the Constitution is also silent when it comes to a constitutional right to privacy, the Court has interpreted a right to privacy using other fundamental rights. In *Kharak Singh v the State of Uttar Pradesh and Others* AIR 1963 (SC) 1295 the Indian Supreme Court held that a concept of privacy can be read in to the right to liberty. Later in the case of *Rajapogal alias R.R. Gopal and another v State of T.N. and others* 1995 S. C. 264 Indian Supreme Court read a concept of privacy under Article 21 of the Indian Constitution. Article 21 provides that 'no person shall be deprived of his life or personal liberty except according to procedure established by law'. To date the Court has refused to define a concept of privacy holding that 'as a concept it may be too broad and moralistic to define it judicially... whether a right to privacy can be claimed or has been infringed in a given case would depend on the facts of each case.'³¹⁹

There are no cases under which the court has considered how a right to privacy can apply for users of the Internet. However, there are a series of cases dealing with privacy and tapping of telephones which may by analogy applied in cases relating to the Internet. In *R. M. Malkani v State of Maharashtra* the Indian Supreme Court held that telephone conversations of innocent person would be protected by the court against wrongful or high handed interference by tapping of the conversation by the police.³²⁰ In *People's Union for Civil Liberties v Union of India* AIR 1997 SC 568 the Court held that once the facts in a case constitute a right to privacy, Article 21 (right to life and personal liberty) is attracted and the right cannot be limited 'except according to procedure established by law'. Thus, unless telephone tapping permitted under a procedure established by law it would infringe Article 21. Any such procedure must be 'just, fair and reasonable'.

The Indian Supreme Court has also held that telephone tapping may also violate Article 19(1) (a) of the Indian Constitution, which protects freedom of expression.³²¹ When a person is talking on the phone he is exercising his right to freedom of speech and expression. Thus, unless telephone tapping comes under the compass of permissible restrictions under article 19 it may violate the individual's freedom of expression. Under Article 19(2)(b) freedom of expression may be limited inter alia to protect the following interest: sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, for preventing incitement to commit of an offence.

Tapping of telephones in India is also regulated under the Telegraph Act 1885 (India). Section 5(2) of the Telegraph Act lays down circumstances under which telephones may be tapped. The circumstances envisaged in section 5(2) are in conformity with article 19(2)(b). The Court has held that the procedure for exercising powers under s5(2) must be fair, just and reasonable. Further the Court has held that powers under section 5(2) may not be exercised except by the Home Secretary, Government of India and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer not

³¹⁹ *Dr. Tokugha Yephthomi v. Apollo Hospital Enterprises Ltd* AIR 1999 SC 495.

³²⁰ M. P. Jain. *Indian Constitution Law*(2006, 5th edition) p 1135.

³²¹ *People's Union for Civil Liberties v Union of India and Others* AIR 1997 SC 568.

below the rank of Joint Secretary. Further there is a review committee consisting of the Cabinet Secretary, Law Secretary and the Secretary of Telecommunications at the Central and State Level to ensure that is no contravention of section 5(2).

However recent reports indicate that Indian authorities are taking steps to increase its surveillance role. In particular, it was reported that the government is employing new more advanced technology to snoop in to the contents of both international and domestic SMS, data and email, including draft emails.³²² Reportedly the Indian Department of Telecommunications is requiring service providers to install upgraded equipment to ensure consistency and quality in the surveillance programs.³²³

South Africa

In South Africa the right to privacy is protected in terms of both the common law and under s 14 of the Constitution. Section 14 of the of the Constitution provides that everyone has a right to privacy which includes the right not to have their person or home searched, their property searched, their possessions seized or the privacy of their communications infringed. The South African Courts have recognized that article 14 protects informational privacy.³²⁴ Section 36 of the South African Constitution limits constitutional rights in the following manner:

The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including,

- a. the nature of the right;
- b. the importance of the purpose of the limitation;
- c. the nature and extent of the limitation;
- d. the relation between the limitation and its purpose; and
- e. less restrictive means to achieve the purpose.

Under the Constitution an action for privacy needs to establish the following: the law or conduct in question infringed the right to privacy and that such an infringement is not justifiable in terms of the limitations of article 36. The plaintiff will have to establish that she had a subjective expectation of privacy which was objectively reasonable. Then the expectation of privacy will be weighed against other rights of the community, such as freedom of expression or the right to information.

³²² Shalini Singh, 'Govt widens interceptions to cover SMS, data & email', The Times of India, 27 April 2010 <<http://timesofindia.indiatimes.com/india/Govt-widens-interceptions-to-cover-SMS-data-email/articleshow/5861899.cms>> accessed 1 June 2010.

³²³ Ibid.

³²⁴ *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).

The Roman Dutch common law of South Africa also protects informational privacy. For a common law action for invasion of privacy (an *actio iniuriarum*) to succeed the plaintiff must establish the following: impairment of the plaintiff's privacy, wrongfulness and intention. Under the common law invasion of privacy is regarded as an impairment of dignity of the person under *actio iniuriarum*. Wrongfulness is established by looking at the reasonableness of the conduct and the expectations of the community (*boni mores*) i.e. countervailing community interests such as freedom of expression and access to information. In terms of intent, a plaintiff must establish that the wrongdoer directed his will to violate the privacy of the prejudiced party or that the wrongdoer knew that his actions could violate the privacy of the prejudiced party. Defenses to a common law action include consent to injury, necessity, private defence, impossibility, public interest and performance in a statutory or official capacity.

Despite the existence of a constitutional right to privacy and a common law privacy action which protects personal information of individuals, the South African Law Reform Commission recommended the enactment of comprehensive data protection laws. In particular the Commission noted that the courts do not have sufficient opportunity to extensively develop the law relating to protection of data. Such a comment is equally applicable to Sri Lanka, where privacy laws are still at their infancy and where no constitutional right to privacy exists. The only effective way to remedy this gap is by way of new legislation. In 2009 the South African Government introduced a draft bill The Protection of Personal Information Bill 2009. To date the bill has not yet been passed through parliament. The bill incorporates the recommendations of the South African Law Reform Commission and it seeks expressly to provide the necessary legislative framework for the effective enforcement of the underlying constitutional right to privacy.

Conclusion

The global outlook for freedom of expression online is mixed at best. All over the world, governments of all political persuasion are finding it difficult to strike a balance between freedom of expression and other countervailing interests such as national security, political stability and cultural control. Governments with poor records on human rights as well as those with good records are taking more and more measures that are undermining the privacy of Internet users. These trends are especially worrying, as countries with mixed human rights records like Sri Lanka can use these examples from abroad to justify their own actions to limit freedom of expression and privacy online.

In Sri Lanka, the impunity shown towards media freedom generally is being extended to the online sphere. The half hearted attempts to regulate online content; block websites; attacks on journalists and repeated statements from government officials threatening those who provide alternative views does not bode well for the future of online freedom of expression in Sri Lanka. Further, despite the end of war there appears to be little signs of any improvements to freedom of expression in Sri Lanka. To date there have been no satisfactory response from law enforcement agencies to any of the attacks on online journalists or websites. Attempts to condemn such violence and other moves that restrict freedom of expression have been dismissed as the work of 'western' agents, conspirators, terrorists or traitors.

Internet users need to be weary 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 censorship program. Internet Filters that are established to remove pornography today can be used to remove political dissent tomorrow. Sri Lankans need to be especially vigilant about such possibilities given the existing socio political climate that has little tolerance for alternative views or values. Concerns about decency and morality ultimately represent an effort by the government to impose certain kinds of values on the citizenry. These 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 the citizens have the freedom to choose whatever values that best suits them.

The impact of this culture of intolerance and impunity is compounded by the restrictive legal framework in Sri Lanka. The Sri Lankan Constitution despite providing for 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 criminalizes political dissent. Similarly other legislation like the Parliamentary Privileges Act and the Press Council Law inhibits discussion of vital policy making by the government. Their application to the online sphere hasn't yet been tested in Sri Lanka. However, a growing number of examples from abroad illustrate that these laws can often have unintended consequences to the online sphere. Thus, their mere existence 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. To date the Supreme Court has recognized that free speech applies regardless of the mode used to express one's ideas. The Court has also recognized 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 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. However, it remains to be seen whether bloggers will receive the same protection. Further, a larger concern remains 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 surveillances. 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.

Recommendations

Significant law reform is required in order to facilitate greater freedom of expression in Sri Lanka both online and otherwise. Firstly, as has been recommended many times elsewhere, the Government can reform and repeal the many content restricting laws currently in place. In particular, provisions of the Parliamentary Privileges Act, Press Council Law and Official Secrets Act that prohibit discussion of socially and politically relevant content should be repealed. Contempt of court laws should be codified and brought in to line with other jurisdictions that permit reasonable criticism of the court's conduct. Current mechanisms for declaring emergencies should be amended, to require a higher threshold prior to declaring an emergency. The PTA should be repealed and new legislation that conforms to international standards should be enacted. Current jurisprudence that protects the freedom of journalists should be strengthened and extended to the online sphere. In particular, bloggers should be given protection to retain their anonymity and protect their sources in appropriate circumstances.

Where governments or private individuals request that ISPs take down, alter or otherwise monitor online content, ISPs should be required to catalogue all such requests. Such requests should be made publicly available similar to Google requests, so that users are aware of threats to their online freedom of expression. Where blocks on Internet sites are administered there needs to be transparency, such that it is clear why content is prohibited. In this regard, it has to be noted that attempts by the Centre for Policy Alternatives to gain access to the 2008 Colombo Magistrates Court judgment that ordered the TRC to block twelve pornography websites were unsuccessful.

Given the complete absence of data protection laws and the limited privacy protection in place, the Government should take immediate steps to provide meaningful privacy protection to Internet users. This is especially so given the government's plans to rely more on ICTs to provide government services. The Government should implement data protection laws and specifically legislate to ensure that ISPs and website operators protect the privacy of data generated by users. The Government should hold ISPs and Telecommunication Operators to be accountable to their customers on how they manage their network traffic. There should be tighter regulation of legally sanctioned instances of surveillance. Where law enforcement agencies or any other Government official request to see user information from an ISP, there should be a clearly defined legal process for doing so. The process should at minimum identify the circumstances, the level of personnel, and the method of making such a request. That process should be publicized and explained to users, so they are aware of the limits to their privacy.

At a soft law level, ISPs and other Telecommunication service providers should have clearly defined privacy policies. Currently the two main ISPs in Sri Lanka, SLT and Dialog do not have a privacy policy regarding

the provision of Internet services available on their websites. It is unclear whether privacy policies are available once a customer signs up for Internet services. ISPs should take immediate steps to make their privacy policies available to both their existing customers and potential new ones. It should be possible for an independent regulator to assess whether the companies are diligent in implementing such policies. The regulator should also assess whether such policies are effective in overcoming threats to privacy and freedom of expression, and make recommendations where there are gaps. Where ISPs fail to adhere to their own policies, breaches in their conduct should be publicized so Internet users are aware of the quality of the service they are using.

Short of such reform, bloggers, Internet users and cyber activists in Sri Lanka may have to resort to uploading content from foreign jurisdictions. In this regard two recent initiatives are important. The first is the 'anti censorship shelter' launched by Reporters Without Borders (RSF).³²⁵ As part of its new initiative, RSF has set aside a room in its Paris headquarters for fugitive journalists and bloggers from abroad, who can use the room to access the Internet via a secure connection that preserves their online anonymity.³²⁶ The initiative also allows select bloggers to remain in their country and still access a free, secure and anonymous online connection.³²⁷ RSF admits that determined governments could find ways to undermine these secure connections; however hopes that the project could also assist responsible bloggers avoid arrest.³²⁸

The second initiative from Iceland is both an instructive example to local regulators and a hopeful alternative to content providers in Sri Lanka. The Icelandic Parliament has commenced the Icelandic Modern Media Initiative (IMMI) which seeks to make Iceland in to a freedom of expression haven.³²⁹ Under the proposal Iceland will be implementing model laws on a range of topics including on source protection, whistleblower protection, freedom of information and libel tourism.³³⁰ The initiative has been hailed by journalists and bloggers as it will allow for content that is controversial or illegal in its country of origin to be uploaded legally in Iceland. The initiative if and when it is implemented, will allow individuals to bypass their country of origin and upload content in Iceland, without fear of legal reprisals.

³²⁵ Breitbart, 'Paris hosts cyber-shelter for battered bloggers', Breitbart, 24 June 2010 <http://www.breitbart.com/article.php?id=CNG.c163a72ad245569e54eb251af457fe23.a01&show_article=1> accessed 30 June 2010.

³²⁶ Ibid.

³²⁷ Ibid.

³²⁸ Ibid.

³²⁹ Jonathan Stray, 'Iceland aims to become an offshore haven for journalists and leakers', Nieman Journalism Lab, 11 February 2010 <http://www.niemanlab.org/2010/02/iceland-aims-to-become-an-offshore-haven-for-journalists-and-leakers/?utm_source=Daily+Buzz&utm_campaign=b24195ba19-daily_buzz_2_11_2010&utm_medium=email> accessed 1 June 2010.

³³⁰ Ibid.

List of works cited

Books

- Asanga Welikala. A state of permanent crisis constitutional government, fundamental rights and states of emergency in Sri Lanka (2008)
- M. P. Jain. Indian Constitution Law (2006, 5th edition)
- Rohan Edirisinha 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)
- Sabina Fernando, 'Freedom of Expression and Media Freedom', in eds. Kanagananda Dharmananda and Lisa M. Kios, Sri Lanka: State of Human Rights Report 1997 (1997)
- Sunil Abeyaratne, Introduction to Information and Communication Technology Law (2008)

Case Law

Australia

Dow Jones v Gutnick (2002) HCA 56

India

People's Union for Civil Liberties v Union of India and Others AIR 1997 SC 568.

Ranjit v Udeshi v State of Maharashtra AIR 1965 SC 881.

Dr. Tokugha Yephthomi v. Apollo Hospital Enterprises Ltd AIR 1999 SC 495.

United States

ACLU v Reno 535 U.S. 1 (2002)

ACLU v Reno 521 U.S. 844 (1997)

Comcast Corporation v Federal Communications Commission and United States of America No 08-1291, Decided 6 April 2010

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

Sri Lanka

Abeysekara v Ariya Rubesinghe and Others (2000) 1 SLR 314

Amaratunga v Sirimal (1993) 1 SLR 264
A.M.K. Azeez v W.T. Senevirathne (SI Police) 69 NLR 209
Chinnapa et al v Kanakar et al 13 NLR 157
Jayawardane v Aberan (1964) Ramanathan Reports
Joseph Perera v AG (1992) 1 SLR 199
Karunathilaka v Dayanand Dissanayake (No. 1) (1999) 1 SLR 157
Pradeep Kumar Darmaratne v Inspector of Police W. Dharmaratne, OIC, Police Station, Aranayake and five others No 163/98
Malagoda v AG (1982) 2 SLR 777
Nadesapillai Vithyatharan Fundamental Rights Application under s 126 of the Constitution
Re Hulugalle 39 NLR 294
Victor Ivan v Sarath N. Silva Attorney General and Others (1998) 1 SLR 340
Wickremabahu v Herath (1990) 2 SLR 348
Wickremasinghe v Edmund Jayasinghe, Secretary to the Ministry of Media (1995) 1 SLR 300
Sinha Ratnatunga v State (2001) 2 SLR 172

South Africa

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)

United Nations Human Rights Committee

Victor Ivan Majuwana Kankanamge v Sri Lanka CCPR/C/81/D/909/2000

Legislation

Sri Lanka

Constitution of the Democratic Socialist Republic of Sri Lanka (1978)
Computer Crimes Act No 24 of 2007 (Sri Lanka)
Obscene Publications Ordinance No 4 of 1927 (as amended) (Sri Lanka)
Official Secrets Act No 32 of 1955 (Sri Lanka)
Parliament (Powers and Privileges) Act No.21 of 1953 (As Amended) (Sri Lanka)
Profane Publications Act No 41 of 1958 (Sri Lanka)
Public Performance Ordinance No 7 of 1912 (as amended) (Sri Lanka)
Public Security Ordinance No 25 of 1947 (Sri Lanka)
Sri Lanka Press Council Law No 5 of 1973 (As amended) (Sri Lanka)
Sri Lanka Telecommunications Act No. 25 of 1991 (As Amended) (Sri Lanka)

Regulations

Extraordinary Gazette Notice no 1651/24 (Sri Lanka) 2 May 2010
Private Television Broadcasting Stations Regulation of 2007 (Sri Lanka)

Europe

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>>

Internet sources

- Achara Ashayagachat, 'Web block adds controversies to laws', Bangkok Post, 6 May 2010 <<http://www.bangkokpost.com/breakingnews/177092/website-blockade-add-controversies-to-lese-majeste-cyber-laws>> accessed 4 July 2010.
- Adam E. Ellick, 'Pakistani court orders access to facebook restored', New York Times, 31 May 2010 <<http://www.nytimes.com/2010/06/01/world/asia/01pstan.html>> accessed 1 June 2010.
- Alton Parish, 'EU Report Shows Internet Censorship Increasing; Sophisticated And Hidden Censorship Tools Mobilised by Enemies of Human Rights', Beforeitsnews, 14 June 2010 <http://beforeitsnews.com/news/78/338/EU_Report_Shows_Internet_Censorship_Increasing;_Sophisticated_and_Hidden_Censorship_Tools_Mobilized_by_Enemies_of_Human_Rights.html> accessed 4 July 2010.
- Amnesty International, 'Skype users monitored in China', Amnesty International, 7 October 2008 <<http://www.amnesty.org.au/china/comments/18073/>> accessed 18 May 2010.
- Andrew Heining, 'Why Apple axed the Google Voice iPhone app', The Christian Science Monitor, 28 July 2009 < <http://www.csmonitor.com/Innovation/Horizons/2009/0728/why-apple-axed-the-google-voice-iphone-app>> accessed 31 May 2010.
- Andrew Puddappatt, New Challenges to freedom of expression, <<http://www.article19.org/speaking-out/new-challenges>> accessed 30 April 2010.
- Article 19, Press Release Jordan: Courts Extend Law to Curb Internet Freedoms, 13 January 2010 < <http://www.article19.org/pdfs/press/jordan-courts-extend-law-to-curb-internet-freedoms.pdf> > accessed 18 May 2010.
- 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>> accessed 4 April 2010.
- BBC, 'Pakistan to monitor Google and Yahoo for 'blasphemy'', BBC, 25 June 2010 <http://news.bbc.co.uk/2/hi/south_asia/10418643.stm > accessed 3 July 2010.
- BBC, 'Porn ban on net and mobiles mulled by South Africa', BBC, 28 May 2010 < <http://news.bbc.co.uk/2/hi/technology/10180937.stm>> accessed 1 June 2010.
- BBC, 'Sri Lanka denies 'hit list' charge', BBC, 17 March 2010 < http://news.bbc.co.uk/2/hi/south_asia/8571627.stm> accessed 18 May 2010.
- BBC, 'Sri Lanka news websites 'blocked'', BBC, 27 January 2010. <http://www.bbc.co.uk/sinhala/news/story/2010/01/100127_lankaenews_rsf.shtml> accessed 18 May 2010.
- BBC, 'Giant database plan 'Orwellian'', BBC, 15 October 2008 <http://news.bbc.co.uk/2/hi/uk_politics/7671046.stm> accessed 11 May 2010.

BBC, 'Tamilnet Blocked in Sri Lanka', BBC < http://www.bbc.co.uk/sinhala/news/story/2007/06/070620_tamilnet.shtml> accessed 4 April 2010.

B Muralidhar Reddy, 'Pardon for Tissainayagam', The Hindu, 4 May 2010 < <http://www.hindu.com/2010/05/04/stories/2010050455871700.htm>> accessed 3 July 2010.

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>> accessed 4 April 2010.

Bangkok Post, 'Thailand: 400 website shut down', Asia Media Archives, 2 September 2008 <<http://www.asiamedia.ucla.edu/article.asp?parentid=96592>> accessed 18 May 2010.

Bandula Sirimanna, 'President halts cyber censorship', The Sunday Times, 21 February 2010 <http://sundaytimes.lk/100221/News/nws_05.html> accessed 4 April 2010.

Bandula Sirimanna, 'Chinese here for cyber censorship', The Sunday Times, 14 February 2010 <http://sundaytimes.lk/100214/News/nws_02.html> accessed 4 April 2010.

Ben Grubb, 'Govt wants ISPs to record browsing history', ZDNet, 11 June 2010 < <http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm?omnRef=NULL>> accessed 3 July 2010.

Brad Linder, 'Army tells soldiers to stop blogging', Download Squad, 2 May 2007, <<http://www.downloadsquad.com/2007/05/02/army-tells-soldiers-to-stop-blogging/>> accessed 18 May 2008.

Breitbart, 'Paris hosts cyber-shelter for battered bloggers', Breitbart, 24 June 2010 <http://www.breitbart.com/article.php?id=CNG.c163a72ad245569e54eb251af457fe23.a01&show_article=1> accessed 30 June 2010.

Colombo Declaration on Media Freedom and Social Responsibility, October 2008 < http://ict4peace.files.wordpress.com/2009/03/declaration_eng.pdf> accessed 15 July 2010.

Colombo Page, 'Sri Lankan government relaxes emergency regulations', Colombo Page, 4 May 2010 < http://www.colombopage.com/archive_10/May1272987911JV.php> accessed 1 June 2010.

Daily Mirror, 'Jailed over prank SMS', Daily Mirror, 1 July 2010 < <http://www.dailymirror.lk/index.php/news/4763-imprisoned-over-prank-sms.html>> accessed 4 July 2010.

Daily Mirror, 'Police seek mobile porn ban', Daily Mirror, 12 May 2010 <<http://srilankanewsfirst.com/politics/17315.html>> accessed 3 July 2010.

Daily News, 'TRC directed to filter obscene websites', Daily News, 2 August 2008 < <http://www.dailynews.lk/2008/08/02/news11.asp>> accessed 4 April 2010.

'Draft paper formulated', 3 April 2009, <<http://www.thefreelibrary.com/Draft+paper+formulated-a0199262018>> accessed 18 May 2010.

Daniel Soar, 'Short Cuts', London Review of Books, 14 August 2008 < <http://www.lrb.co.uk/v30/n16/daniel-soar/short-cuts>> accessed 1 June 2010.

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>> accessed 18 May 2010.

Dominic Casciani, 'Plan to Monitor all Internet use', BBC, 27 April 2009 <http://news.bbc.co.uk/2/hi/uk_news/politics/8020039.stm> accessed 17 May 2010.

EPDP, 'EPDP advisory to free media movement', Free Media Movement, 1 November 2008 < <http://freemediasrilanka.wordpress.com/2008/11/17/epdp-advisory-to-free-media-movement/> > accessed 1 June 2010.

The End, 'My conversation with Dialog GSM about the President's New Year Message', The End, 1 January 2010 <<http://finem.wordpress.com/2010/01/01/my-conversation-with-dialog-gsm-about-the-president's-new-year-message/>> accessed 18 May 2010.

Evgeny Morozov, 'Will Baharain's censorship efforts run into 'cute cat theory'?', Net.effect, 2 April 2009 < http://neteffect.foreignpolicy.com/posts/2009/03/30/will_bahraains_censorship_efforts_run_into_the_cute_cat_theory > accessed 4 April 2010.

Free Media Movement, '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/>> accessed 18 May 2010.

Free Media Movement, 'After 365 Days its now a crawl for survival – LankaDissent', Free Media Movement, 21 July 2008 < <http://freemediasrilanka.wordpress.com/2008/07/21/after-365-days-it%E2%80%99s-now-a-crawl-for-survival-lankadissent/>> accessed 3 July 2010.

Gaurav Mishra, 'Indian Blogosphere condemns NDTV's bullying of blogger Chyetanya Kunte over criticism of Barkha Dutt', Gauravonomics < <http://www.gauravonomics.com/blog/indian-blogosphere-condemns-ndtvs-bullying-of-blogger-chyetanya-kunte-over-criticism-of-anchor-barkha-dutts-sensationalistic-coverage-of-the-1126-mumbai-terror-attack/>> accessed 31 May 2010.

Google, Government Requests, 31 May 2010 <<http://www.google.com/governmentrequests/>> accessed 31 May 2010.

Google, 'What do we mean by net neutrality', Google Public Policy Blog, 16 January 2007 <<http://googlepublicpolicy.blogspot.com/2007/06/what-do-we-mean-by-net-neutrality.html>> accessed 18 May 2010.

Google, Government requests directed to Google and YouTube <<http://www.google.com/governmentrequests/>> accessed 30 April 2010.

Google, Google Privacy Policy < <http://www.google.com/privacypolicy.html>> accessed 18 May 2010.

Google, 'Mandatory ISP level filtering submission to the Department of Broadband, Communications and Digital Economy', Arts technica < http://www.dbcde.gov.au/submissions/20100316_11.34.55/256-Google%20ISP%20filtering%20submission%20Feb%202010.pdf> accessed 18 May 2010.

Government of Sri Lanka, 'Govt comes down hard on SMS conspirators', The Official Government News Portal of Sri Lanka', 29 January 2010 <http://www.news.lk/index.php?option=com_content&task=view&id=13433&Itemid=44> accessed 9 July 2010.

Groundviews, 'Unsolicited sms messages are spam. Please desist Mr President', Groundviews, 1 January 2010 < <http://www.groundviews.org/2010/01/01/unsolicited-sms-messages-are-spam-please-desist-mr-president/>> accessed 1 June 2010.

Groundviews, 'Sri Lanka blocks TamilNet', Groundviews, 19 June 2007 < <http://www.groundviews.org/2007/06/19/sri-lanka-blocks-tamilnet/>> accessed 1 June 2010.

James Kirby, 'The Net- Overseas pornography will filter through', Business Review Weekly, 12 November 1999 <<http://www.brw.com.au/stories/19991112/4092.htm>> accessed 4 April 2010.

- Joel Hruska, 'Rumours fly as RIM, India talk BlackBerry snooping, privacy', Ars Technica, 27 May 2008 <<http://arstechnica.com/gadgets/news/2008/05/rumors-fly-as-rim-india-talk-blackberry-snooping-privacy.ars>> accessed 18 May 2010.
- John Markoff, 'Surveillance of Skype Messages Found in China', New York Times, 1 October 2008 <http://www.nytimes.com/2008/10/02/technology/internet/02skype.html?_r=1&em> accessed 18 May 2010.
- John W. Mayo, Mairus Schwartz, Bruce Owen, Robert Shapiro, Lawrence J White and Glenn Woroch, 'How to Regulate the Internet Tap', New York Times, 20 April 2010 < <http://www.nytimes.com/2010/04/21/opinion/21mayo.html>> accessed 31 May 2010.
- Jon Stokes, 'NSA eavesdropped on Americans, journalists in Baghdad', Arts technica, 9 October 2008, <<http://arstechnica.com/old/content/2008/10/nsa-eavesdropped-on-americans-journalists-in-baghdad.ars>> accessed 17 May 2010.
- Jonathan Stray, 'Iceland aims to become an offshore haven for journalists and leakers', Nieman Journalism Lab, 11 February 2010 < http://www.niemanlab.org/2010/02/iceland-aims-to-become-an-offshore-haven-for-journalists-and-leakers/?utm_source=Daily+Buzz&utm_campaign=b24195ba19-daily_buzz_2_11_2010&utm_medium=email> accessed 1 June 2010.
- Josh Silverman, 'Skype President Addresses Chinese Privacy Breach', The Big Blog, 2 October 2008 <http://blogs.skype.com/en/2008/10/skype_president_addresses_chin.html> accessed 18 May 2008.
- 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> accessed 1 June 2010.
- Information Policy, 'Australia: Measures to Improve Safety of the Internet for Families', Information Policy, 2 July 2010 < <http://www.i-policy.org/2010/07/australia-measures-to-improve-safety-of-the-internet-for-families.html>> accessed 4 July 2010.
- International Federation of Journalists, 'IFJ concerned over Google censorship deal', International Federation of Journalists, 5 September 2007 <<http://www.ifj.org/en/articles/ifj-concerned-over-google-censorship-deal-with-thailand>> accessed 18 May 2010.
- Indika Sri Aravinda, 'Complaints against Facebook', Daily Mirror, 13 July 2010 < <http://www.dailymirror.lk/index.php/news/5055-complaints-against-facebook-.html>> accessed 16 July 2010.
- Indika Sri Aravinda, 'Pop star Akon in Cabinet', Daily Mirror, 24 March 2010 < <http://www.dailymirror.lk/index.php/news/2600-pop-star-akon-in-cabinet.html>> accessed 18 May 2010.
- Islamic Human Rights Commission, 'Alert: Sri Lanka – Sri Lankan Muslim convert to be tried under Emergency Law Tomorrow', Islamic Human Rights Commission 14 May 2010. < <http://www.ihrc.org.uk/activities/alerts/9313-alert-sri-lanka-sri-lankan-muslim-convert-to-be-tried-under-emergency-law-tomorrow>> accessed 18 May 2010.
- Internet World Stats Usage and Population Statistics < <http://www.internetworldstats.com/asia/lk.htm>> accessed 11 May 2010.

Komsan Tortermvasana, 'Websites face new crackdown', Bangkok Post, 18 June 2010 < <http://www.bangkokpost.com/news/local/38943/websites-face-new-crackdown>> accessed 4 July 2010.

Krishan Francis, 'Buddha uproar halts Akon show', MSNBC.com, 28 March 2010 < <http://www.msnbc.msn.com/id/36020442/ns/entertainment-music/>> accessed 18 May 2010.

Kumar David, 'Implications of an Information Dark Age', Lankbima News, 21 February 2010 < <http://ict4peace.files.wordpress.com/2010/02/lankbima-21-2-2010.pdf>> accessed 18 May 2010.

Lanka Business Online, 'Crime Alarm', Lanka Business Online, 29 January 2009 <<http://www.lankabusinessonline.com/fullstory.php?nid=257786312>> accessed 25 May 2010.

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> accessed 4 April 2010.

Lasanda Kurukulasuriya, 'The Sirasa attack: Was Akon just an excuse?', Sunday Times, 28 March 2010 < http://sundaytimes.lk/100328/News/nws_79.html> accessed 18 May 2010.

Lankanewsweb, Government to block Internet in Sri Lanka, 10 February 2010 < http://www.lankanewsweb.com/news/EN_2010_02_10_013.html > accessed 20 February 2010.

Lucie Morillon and Jean-Francois Julliard, 'Web 2.0 versus Control 2.0', Reporters without Borders, 2 June 2010 <<http://www.europarl.europa.eu/document/activities/cont/201005/20100527ATT75115/20100527ATT75115EN.pdf>> accessed 28 June 2010.

Lee Min Keong, 'With site block, Malaysia seems to break promise', CNet News, 2 September 2009 <http://news.cnet.com/8301-13578_3-10030325-38.html> accessed 18 May 2010.

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>> accessed 1 June 2010.

Michael Arrington, 'Hit pause on the evil button: Google assists in arrest of Indian man', Washington Post, 19 May 2008 <<http://www.washingtonpost.com/wp-dyn/content/article/2008/05/18/AR2008051800657.html>> accessed 18 May 2010.

Marin Perez, 'RIM Questions India's BlackBerry Encryption Worries', Informationweek, 2 June 2008 <<http://www.informationweek.com/news/security/encryption/showArticle.jhtml?articleID=208401643>> accessed 18 May 2010.

Mark 'Rizzin' Hopkins, 'Freedom of Speech, Not Freedom of Consequences', Mashable, 2009 <<http://mashable.com/2008/06/05/truth-and-consequences/#more-27552>> accessed 18 May 2010.

Nate Anderson, 'Google tells Australia its 'net filters go way too far'', Arts technica, April 2010 < http://arstechnica.com/tech-policy/news/2010/03/google-tells-australia-its-net-filters-go-way-too-far.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss> accessed 1 June 2010.

Nate Anderson, 'Next up for France: police key loggers and web censorship', Arts technica, 19 March 2009 <<http://arstechnica.com/tech-policy/news/2009/05/next-up-for-france-police-keyloggers-and-web-censorship.ars>> accessed 19 May 2010.

Nate Anderson, 'Move over, Australia: France taking 'net censorship lead'', Arts technica, 17 February 2010 <<http://arstechnica.com/tech-policy/news/2010/02/move-over-australia-france-taking-net->

[censorship-lead.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss](#)> accessed 11 May 2010.

The Nation, 'Unidentified groups attack Mangala's news website', The Nation on Sunday, 18 May 2008 <<http://www.nation.lk/2008/05/18/news11.htm>> accessed 3 July 2010.

Neelie Kroes, 'Net Neutrality in Europe address at ARCEP conference', Europa Press Releases Rapid <<http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/153>> accessed 31 May 2010.

New Media Glossary <<http://www.sag.org/content/new-media-glossary>> accessed 18 May 2010.

New York Times, 'Editorial: Mr Obama's Internet Agenda', New York Times, 15 December 2008 <http://www.nytimes.com/2008/12/16/opinion/16tue3.html?_r=1> accessed 31 May 2010.

Orkut, Orkut Account Creation <<http://www.orkut.com/PreSignup>> accessed 18 May 2010.

Open Net Initiative, Jordan, 6 August 2009 <http://opennet.net/research/profiles/jordan#footnote13_st2wukl> accessed 18 May 2010.

Patrick O' Conner, 'Fijian military junta targets bloggers', World Socialist Web Site, 24 May 2007 <<http://www.wsws.org/articles/2007/may2007/blog-m24.shtml>> accessed 18 May 2010.

Peter Sayer, 'France bans citizen journalists from reporting violence', Macworld. 6 March 2007 <<http://www.macworld.com/article/56615/2007/03/franceban.html>> accessed 18 May 2010

Presi Mandari, 'Indonesia looks to block', AFP, 16 February 2010 <<http://www.google.com/hostednews/afp/article/ALeqM5hac4JRd2Zm2itcNWDH7JG3bynuCQ>> accessed 18 May 2010.

Privacy International, 'Republic of Sri Lanka', Privacy International, 18 December 2007 <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559488#\[21\]](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559488#[21])> accessed 1 June 2010.

Publius, 'The shocking behavior of the Telecommunications Regulatory Commission of Sri Lanka', Groundviews, 9 January 2010 <<http://www.groundviews.org/2010/01/09/the-shocking-behaviour-of-the-telecommunications-regulatory-commission-of-sri-lanka/#more-2442>> accessed 18 May 2010.

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/>> accessed 1 June 2010.

Rachel Donadio, 'Larger threat is seen in Google case', New York Times, 24 February 2010 <<http://www.nytimes.com/2010/02/25/technology/companies/25google.html>> accessed 1 June 2010.

Rathindra Kuruwita, 'Facebook users come under scrutiny', Lankanewspapers.com, 31 January 2010 <http://www.lankanewspapers.com/news/2010/1/53532_space.html> accessed 16 July 2010.

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> accessed 18 May 2010.

Reporters Without Borders, 'Countries under surveillance 2010- Sri Lanka', Reporter Without Borders, 18 March 2010 <<http://www.unhcr.org/refworld/docid/4c21f668c.html>> accessed 5 July 2010.

Reporters Without Borders, Internet Enemies – Countries under surveillance: Sri Lanka, 12 March 2009 < <http://www.unhcr.org/refworld/docid/4a38f97c.html>> accessed 4 April 2010.

Reporters Sans Frontiers, 'Websites blocked just hours before poll results due to be announced', Reporters without Borders, 26 January 2010 <<http://en.rsf.org/sri-lanka-websites-blocked-just-hours-before-26-01-2010,36213>> accessed 18 May 2010.

Rezwan, 'India: blogger silenced', Global voices, 30 January 2009 < <http://globalvoicesonline.org/2009/01/30/india-blogger-silenced/>> accessed 1 June 2010.

Lepoint, 'Reviews LOPPSI two texts and the reform of criminal procedure carried', Lepoint.fr, 5 May 2010 < <http://translate.google.com/translate?hl=en&sl=fr&u=http://www.lepoint.fr/actualites-politique/2010-05-05/senat-la-reforme-de-la-procedure-penale-reportee/917/0/451385&ei=rCIETNGNBseXcZbY2dUB&sa=X&oi=translate&ct=result&resnum=1&ved=0CБУQ7gEwAA&prev=/search%3Fq%3DExamens%2Bdes%2Btextes%2BLOppsi%2B2%2Bet%2Bde%2Bla%2Br%25C3%25A9forme%2Bde%2Bla%2Bproc%25C3%25A9dure%2Bp%25C3%25A9nale%2Breports%26hl%3Den%26rls%3Dcom.microsoft:en-us> > accessed 11 May 2010 (Translated from French to English via Google Translator).

Ministry of Defence, 'WFP apology for BBC falsehood on Sri Lankan IDPs', Ministry of Defence, 12 December 2008 < http://www.defence.lk/new.asp?fname=20081210_08 > accessed 1 June 2010.

Rebekah Heacock, 'Afghanistan begins Internet filtering with Gmail, Facebook', Opennet, 28 June 2010 < <http://opennet.net/blog/2010/06/afghanistan-begins-internet-filtering-with-gmail-facebook>> accessed 4 July 2010.

Richard Ford, 'Big Brother' database for phones and e-mails', Times Online, 20 May 2008, <http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article3965033.ece> accessed 17 May 2010.

Robert Mackey, 'Briton convicted for 'Menacing tweet against Robin Hood Airport'', New York Times, 10 May 2010 < <http://thelede.blogs.nytimes.com/2010/05/10/briton-convicted-for-menacing-tweet-against-robin-hood-airport/>> accessed 1 June 2010.

Rohan Samarajiva, 'Quo Warranto TRC?', Lirneasia, 14 February 2010 < <http://lirneasia.net/2010/02/quo-warranto-trc/>> accessed 4 April 2010.

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/>> accessed 18 May 2010.

Sanjana Hattotuwa, 'Banning Sri Lankan porn online: a couple of month after', ICT for Peacebuilding, 31 January 2010 < <http://ict4peace.wordpress.com/2010/01/31/banning-sri-lankan-porn-online-a-couple-of-months-after/>> accessed 4 April 2010

Sanjana Hattotuwa, 'The arrest of the 'blogger' in Sri Lanka: Crowd-sourcing trumps traditional media follow up', ICT for Peacebuilding, 8 November 2009 < <http://ict4peace.wordpress.com/2009/11/08/the-arrest-of-the-%e2%80%98blogger%e2%80%99-in-sri-lanka-crowd-sourcing-trumps-traditional-media-follow-up/>> accessed 18 May 2010.

- Sanjana Hattotuwa, 'Blogger arrested in Sri Lanka for 'offensive' comments regarding President and Defense Secretary?', ICT for Peacebuilding, 1 November 2009 < <http://ict4peace.wordpress.com/2009/11/08/the-arrest-of-the-%e2%80%98blogger%e2%80%99-in-sri-lanka-crowd-sourcing-trumps-traditional-media-follow-up/>> accessed 18 May 2010.
- Sanjana Hattotuwa, 'Freedom of Expression in Singapore vs Sri Lanka', ICT for Peacebuilding, 7 June 2009 <<http://ict4peace.wordpress.com/2008/06/07/freedom-of-expression-in-singapore-vs-sri-lanka/>> accessed 18 May 2010.
- Sanjana Hattotuwa, 'UK's proposed Internet surveillance a model for repressive regimes?', ICT for Peacebuilding, 2 May 2009 <<http://ict4peace.wordpress.com/2009/05/02/uks-proposed-internet-surveillance-a-model-for-repressive-regimes/>> accessed 17 May 2010.
- Sanjana Hattotuwa, '2008: Celebrating the growth of media freedom and the freedom of expression in Sri Lanka', ICT for Peacebuilding, 4 March 2009 < <http://ict4peace.wordpress.com/2009/03/04/2008-celebrating-the-growth-of-media-freedom-and-the-freedom-of-expression-in-sri-lanka/> > accessed 1 June 2010.
- 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/>> accessed 1 June 2010.
- Sanjana Hattotuwa, 'Significant issues arising out of the Private Television Broadcasting Regulations of 2007 for bloggers and new media producers in Sri Lanka', ICT for Peacebuilding, 24 November 2008 < <http://ict4peace.wordpress.com/2008/11/24/significant-issues-arising-out-of-the-private-television-broadcasting-station-regulations-of-2007-for-bloggers-and-new-media-producers-in-sri-lanka/>> accessed 18 May 2010.
- Sanjana Hattotuwa, 'The rise of Big Brother in the UK', ICT for Peacebuilding, 8 May 2008 <<http://ict4peace.wordpress.com/2008/05/28/the-rise-of-big-brother-in-the-uk/>> accessed 17 May 2010.
- Sanjana Hattotuwa, 'A step backwards for Citizen Journalism – France bans citizen journalism from reporting violence', ICT for Peacebuilding, 7 March 2007 <<http://ict4peace.wordpress.com/2007/03/07/a-step-backwards-for-citizen-journalism-france-bans-citizen-journalists-from-reporting-violence/>> accessed 18 May 2010.
- Shalini Singh, 'Govt widens interceptions to cover SMS, data & email', The Times of India, 27 April 2010 <<http://timesofindia.indiatimes.com/india/Govt-widens-interceptions-to-cover-SMS-data-email/articleshow/5861899.cms>> accessed 1 June 2010.
- 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>> accessed 4 April 2010.
- Tech2, 'Obscene Orkut Post Lands Youth in Prison', Tech2.in, 20 May 2008 <<http://tech2.in.com/india/news/internet/obscene-orkut-post-lands-youth-in-prison/36611/0>> accessed 18 May 2010.
- Telecommunications Regulatory Commission of Sri Lanka, June 2009 Statistics < <http://www.trc.gov.lk/information/statistics.html>> accessed 11 May 2010.

The Bottom Line, 'Plans to kill TNA website?', The Bottom Line, 9 April 2008 <<http://www.thebottomline.lk/2008/04/09/B38.htm>> accessed 3 July 2010.

Yahoo, 'France, Netherlands seek to halt Internet censorship', Yahoo!, 8 July 2010 <http://news.yahoo.com/s/afp/20100708/tc_afp/francenetherlandsinternetpoliticsrights_20100708160333> accessed 8 July 2010.

Zeeshan Haider, 'Pakistan to monitor Google, others for blasphemy', Reuters, 25 June 2010 <<http://in.reuters.com/article/idINIndia-49655320100625?feedType=RSS&feedName=everything&virtualBrandChannel=11709>> accessed 3 July 2010.

Reports

Article 19, War of Words: Conflict and Freedom of Expression in South Asia Thematic Reports, (May 2005)

Article 19, Background Paper on Freedom of Expression and Internet Regulation for the International Seminar on Promoting Freedom of Expression with Three Specialized International Mandates. (2001)

Gus Hosein, Politics of the Information Society: The Bordering and Restraining of Global Data Flows, (2004)

Human Rights Commission, Contempt of Court the need for substantive cum procedural definition and codification of the law in Sri Lanka (2005)

International Telecommunications Union, Measuring the Information Society (2010)

Thomas Lum, Internet Development and Information Control in the People's Republic of China CRS Report for Congress. (Updated 6 February 2010)

Newspaper Articles

Dianne Silva, 'USA only sympathetic towards Fonseka: Gota', Daily Mirror 1 March 2010

Journal Articles

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

Correspondence

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

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.