

Acknowledgements

Lucy Purdon, IHRB's ICT Project Manager, designed and managed this research project, supported by Salil Tripathi, IHRB Senior Advisor on Global Issues, and Motoko Aizawa, IHRB Managing Director USA. Hani Yousuf conducted additional research and company interviews in Islamabad.

IHRB partnered with *Bytes for All* in Islamabad and the *Centre for Internet and Human Rights* (CIHR) in Berlin in developing and producing this study. We are grateful for the support of Shahzad Ahmad, Furhan Hussain and Faheem Zafar from *Bytes for All* as well as Linda Walter and Joanna Bronowicka from *CIHR* in conducting this research project.

This paper is co-authored by Lucy Purdon of IHRB, Arsalan Ashraf from *Bytes for All* and Dr. Ben Wagner from *CIHR*.

IHRB would like to thank all representatives of *Telenor Pakistan* and *Telenor Group* involved in the drafting of this study for their co-operation and participation. The study reflects the views of IHRB and not those of *Telenor Pakistan* or *Telenor Group*.

IHRB is grateful to the *Centre for Global Communications Studies* (CGCS) at the *Annenberg School for Communication* (University of Pennsylvania, USA) for funding a portion of this research. IHRB would also like to thank the *Ministry of Foreign Affairs of the Netherlands* and the *Ministry of Foreign Affairs of Sweden* for initial funding for the *Digital Dangers* project.

All rights reserved. The IHRB permits free reproduction of extracts from any of its publications provided due acknowledgement is given and a copy of the publication carrying the extract is sent to its headquarters at the address below. Requests for permission to reproduce or translate the publication should be addressed to the IHRB.

Institute for Human Rights and Business
34b York Way
London N1 9AB
UK

Phone: (+44) 203-411-4333
Email: info@IHRB.org

About this Paper

The role of telecommunications operators in network shutdowns first captured global attention following events in Egypt during the 2011 Arab Spring, when former President Hosni Mubarak ordered a near country-wide shutdown of mobile and Internet services, reportedly with the aim of preventing anti-government protesters from utilising these tools to organise and spread their message⁴.

Network shutdowns impacting an entire country are now almost non-existent, but the practice of shutting down communications in certain cities or areas of a country, or suspending certain services continues globally. This has happened over the past decade or so for a variety of reasons, sometimes due to national security concerns but also to prevent the organisation of protests or the spread of civil unrest.

Other high profile cases of network shutdowns over the past decade include in India⁵, China⁶, the United Kingdom⁷ and the United States⁸. In 2013 and 2014 alone, Freedom House reported network shutdowns that were likely government-ordered in Ethiopia, Iraq, Kazakhstan, Pakistan, Syria, Sudan, Uzbekistan, Yemen and Zimbabwe⁹.

In January 2015, the Government of the Democratic Republic of Congo ordered a reportedly near country-wide mobile Internet and SMS shutdown following protests

4 Matt Richel, New York Times, Egypt Cuts Off Most Internet and Cellphone Service (28 Jan 2011) <http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html>
Jim Cowie, Dyn Research, Egypt Leaves the Internet (27 January 2011) <http://research.dyn.com/2011/01/egypt-leaves-the-internet>

5 On March 17th and 18th 2014, the government of India shutdown parts of the Internet in Kashmir, reportedly to prevent Kashmiri leaders from addressing a UN Human Rights Council side event in Geneva via video link. See: Kashmir Media Service, India shuts down internet to prevent Mirwaiz's address (18 March 2014) <http://www.kmsnews.org/news/2014/03/18/india-shuts-down-internet-to-prevent-mirwaiz-address.html>

In September 2014, mobile data and SMS were suspended in Vadodara, Gujarat following civil unrest. See: Mahesh Langa and M Rajendran, Hindustan Times, Vadodara tense, mobile data services suspended, (28 September 2014) <http://www.hindustantimes.com/india-news/communal-unrest-in-vadodara-internet-banned/article1-1269051.aspx>

In March 2015, Internet and SMS services were blocked in Kohima, Nagland, following the distribution of a video reportedly showing the lynching of a man accused of rape. See: Zee News, Mobile Internet facility suspended in violence-hit Vadodara (28 September 2014) http://zeenews.india.com/news/gujarat/mobile-internet-facility-suspended-in-violence-hit-vadodara_1476963.html

6 Following riots in the Xinjiang region, Internet access was shutdown for 10 months, affecting a reported 7 million people. See: Chris Hogg, BBC News Online, China Restores Xinjiang Internet (14 May 2010) <http://news.bbc.co.uk/1/hi/world/asia-pacific/8682145.stm>

7 BBC News Online, 7 July Phone Shutdown Criticised (1 March 2006) <http://news.bbc.co.uk/1/hi/england/london/4763350.stm>

8 Melissa Bell, The Washington Post, BART San Francisco Cuts Cell Services to Avert Protests (12 August 2011) http://www.washingtonpost.com/blogs/worldviews/post/bart-san-francisco-cut-cell-services-to-avert-protest/2011/08/12/gIQAfLCgBJ_blog.html

9 Freedom House, Freedom on the Net 2014 https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

over the President's unconstitutional decision to remain in power for a third term¹⁰.

In May 2015 in Burundi, following similar protests over the President's plan to seek another term in office, the government blocked access to social networking sites Facebook and Twitter, and messaging applications Viber and Whatsapp¹¹.

A timeline of network shutdowns created by the Centre For Democracy and Technology (CDT) indicates that shutdowns increased globally year on year from 2005 to 2014¹².

Due to the extremely sensitive nature of the subject, most telecommunications operators rarely address publicly the issue of network shutdowns and associated policies. Therefore, relatively little is known about the reasons for shutdowns, the mechanism through which governments affect such shutdowns, or the economic and social impacts of shutdowns on telecommunications companies, users, and society at large. Without such information, there is little opportunity to understand the avenues for prevention, mitigation and redress for business, users, or civil society.

To combat its own serious public security challenges, the Government of Pakistan has often instructed telecommunication operators to suspend mobile and/or Internet networks where intelligence indicates a threat to national security. The Government of Pakistan's stated intention in blocking access to communication at such a time is primarily in order to protect the right to life¹³ as violent extremists use mobile phones to inform each other of their movements and in some cases, mobile phones have been used to detonate bombs.¹⁴

Companies in most jurisdictions have a legal obligation to comply with and support the State's efforts where there is an imminent threat of violence. However, many experts argue that network shutdowns violate a range of human rights, and are neither necessary nor proportionate responses to potential violent activities. While the debate is often framed around the resulting restrictions to freedom of expression, network shutdowns also impact other rights, including life, access to health services, education, and work.

Due to the relatively frequent nature of network shutdowns and associated security

10 Lucy Purdon, IHRB, Network Shutdowns in the DRC: ICT Companies Need Clear Rules (19 February 2015) <http://www.IHRB.org/commentary/network-shutdowns-the-drc-ict-companies.html>

11 Vincent Matinde, ITWebAfrica, Burundi Shuts Down Internet Access (30 April 2015) <http://www.itwebafrica.com/ict-and-governance/363-burundi/234560-burundi-shuts-down-internet-access>

12 <http://network-shutdowns.cdt.info/timeline.php>

13 The right to life has been defined in a judgment of the Supreme Court of Pakistan- PLD 1994 SC 693, "Article 9 of the Constitution provides that no person shall be deprived of life or liberty save in accordance with law. The word "life" is very significant as it covers all facts of human existence. The word "life" has not been defined in the Constitution but it does not mean nor can be restricted only to the vegetative or animal life or mere existence from conception to death. Life includes all such amenities and facilities which a person born in a free country is entitled to enjoy with dignity, legally and constitutionally." See <http://pakistanconstitutionlaw.com/pld-1994-sc-693/>

14 Associated Press, Bomb at Pakistan Shiite Procession Kills 7 (24 November 2012) <http://www.cbsnews.com/news/bomb-at-pakistan-shiite-procession-kills-7/>

considerations, Pakistan was selected as the focus for this study. At the start of the project, IHRB posed the following research questions to apply to the context of Pakistan:

- Why does the Government make shutdown requests?¹⁵
- How are shutdown requests made to operators?
- What is the legal basis for a shutdown?
- How do shutdowns impact people's day-to-day lives?

Posing these questions at the start of this process demonstrated how little information exists in the public domain regarding shutdowns and the need for further research and discussion. This paper examines one particular network shutdown in the Pakistani capital Islamabad and in the city of Rawalpindi during March 2015. The aim is to:

- Analyse the Pakistan context as an introduction to further research on the economic and social impacts of network shutdowns.
- Explore how requests for disconnection are made by authorised agencies to telecommunication operators.
- Conduct a preliminary study on the day-to-day impacts and the perception of Pakistani citizens of network shutdowns, with a view to developing more in-depth research in the future. This study did not look into the full economic impact of a shutdown.
- Analyse instances of mobile and Internet shutdowns outside of Pakistan, which were followed by corporate and government campaigns to achieve positive change, such as an amendment in the law.
- Provide best practices and guidelines for telecommunication operators with regard to handling network shutdown requests.
- Explore short-term and long-term opportunities for government strategies that both safeguard human rights online and offline by working with companies and governments so that human rights (of expression, assembly, privacy, security, and others) are not undermined while governments pursue legitimate objectives such as protecting society from terrorism or violence.

15 For the purposes of this paper, shutdowns are defined as suspension of entire mobile or Internet services, rather than access to a particular website (e.g. a social networking site) or part of a mobile network (e.g. SMS) unless otherwise specified.

Methodology

An IHRB researcher spent three days at *Telenor Pakistan's* headquarters in Islamabad, Pakistan, to conduct research into the context of network disconnections and document how *Telenor Pakistan* receives and acts on requests from the Government to initiate network shutdowns. *Telenor Pakistan* co-operated with IHRB's request to visit company headquarters and made its staff available for interviews. Each department interviewed detailed its part in the process of implementing a network shutdown request. This study also compiles desk research on other network shutdowns, and draws on IHRB's previous research in this area. IHRB shared a draft of this report with *Telenor Pakistan* before publication in order to identify any proprietary information or information of commercial significance that should remain confidential, as well as to ensure accuracy.

IHRB partnered with the Islamabad based digital rights organisation *Bytes for All*¹⁶ and the *Centre for Internet and Human Rights (CIHR)*¹⁷ in Berlin to conduct on the ground research into the impacts of network shutdowns in Pakistan. *Bytes for All* and *CIHR* developed a survey, which aimed to ascertain how people perceive shutdowns and how shutdowns impacted day-to-day life, work and study. The survey was tested with members of the public during the network shutdown over Ashura¹⁸ in November 2014, which was also available online¹⁹. It was then revised and used during the network shutdown in Islamabad on 23 March 2015. The survey data collected during the latter shutdown features in this paper.

IHRB, *Bytes for All* and *CIHR* did not have official advance notice the shutdown would take place. However, researchers were able to identify patterns in shutdowns taking place around national and religious holidays as well as other key political events, which made it easier to anticipate when shutdowns would take place. *Bytes for All* also received information that a request had been issued by Pakistan's telecommunication regulator, the Pakistan Telecommunication Authority (PTA), on 11 March 2015. Once it became clear on the morning of 23 March that a shutdown was indeed in progress, *Bytes for All* researchers completed 190 surveys with members of the public in Islamabad and Rawalpindi on that day and in the following week after the shutdown.

Rapidly responding and collecting data under these circumstances is very challenging. Although readers should take note of the limited scope of this survey (featured in Section 6 and referenced throughout the study), the survey presents an important step in an exploratory study of the actual disconnection of communications networks and the consequences of such actions. The results of these surveys served as a catalyst for further research into identified impacts, as well as recommendations to mitigate the impacts on fundamental rights and scope for further in-depth research.²⁰

16 <http://content.bytesforall.pk>

17 <https://cihr.eu>

18 Ashura is a religious day for Muslims on the tenth day of Muharram, which is the first month of the Islamic calendar. Shia Muslims consider it a day of mourning and Shia Muslims in South Asia perform ritual processions and marches on this day.

19 <https://content.bytesforall.pk/disconnectionofcommunicationservices>

20 IHRB presented some initial findings in May 2015 at *Telenor's* 2015 Sustainability Seminar in London, and took part in a panel discussion on the issue. See video here: <http://www.Telenor.com/investors/presentations/2015/Telenor-group-sustainability-seminar/>

Executive Summary

Most countries' national laws allow governments to take control of communications networks during a national emergency, but the situations in which governments can exercise this power are often not clearly indicated²¹. Governments cite a number of different reasons for ordering a network shutdown: For perceived safety of citizens citing harms that might follow if (for example) a bomb is detonated by a mobile phone; to deal with civil unrest; to prevent information leaving the country; or to prevent further mobilisation of protests against a government.

Telecommunication operators often bear the responsibility of executing government orders to shutdown communications, whether mobile networks in particular cities or regions, Internet access, or access to particular websites or messaging applications. The request process may be unclear, execution is technically complex, and there is in most cases virtually no transparency. In addition, it is still a difficult topic for companies to discuss publicly, due to the national security element.

The primary duty of any government is to protect the safety and security of its citizens. But states have broader obligations to protect the whole spectrum of human rights. Such suspension or disconnection of services is likely to adversely impact on freedom of expression, freedom of assembly and a range of other economic and social rights. As more and more people become connected to and rely on mobile and Internet services, and telecommunications become an indispensable cornerstone of the economy, government-ordered network shutdowns become increasingly disruptive, even endangering the right to life which the government is likely trying to protect.

Pakistan's political trajectory has been unstable for much of the past two decades; however, in the past seven years, a democratic government has completed its tenure and there has been peaceful transfer of power from one political party to another. At the same time, the country has continued to suffer frequent terrorist attacks. The Government's security concerns are valid and it has an obligation to take all reasonable steps to protect civilian lives. However, experts are concerned that network shutdowns are becoming the norm, rather than an exception, and are being utilised as the main strategy to curb terrorism, when instead, improving other methods of investigation is required²².

Telecommunication operators doing business in Pakistan are operating in difficult circumstances, and need to balance their goal of providing seamless services to their customers with the needs of security agencies seeking effective steps to prevent acts of terror within their territory.

Network shutdowns began in Pakistan around 2005 during violence in the Balochistan

21 For example, see Article 34 and 35 of the International Telecommunication Union (ITU) Constitution http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF

22 For example, counter intelligence, forensic investigation, witness protection, additional training for local police forces.

region. Today, shutdowns usually occur over religious and national holidays, or during mass protests and political rallies. *Annex A* lists all known instances of shutdowns from 2012- 2015. Network shutdowns in Pakistan usually means the complete shutdown of cellular services, including voice, short message service (SMS), and mobile Internet. Fixed line Internet and telephone access can also be limited at times.

It is acknowledged that mobile network shutdowns have become less frequent in recent years and far more targeted in scope. This could be in part due to the introduction of a more streamlined request process that took effect from 2012, which is outlined in the body of this paper.

However, the trend of blocking communication services for security reasons may be set to increase in scope to include Wi-Fi networks. This expansion was witnessed during the network shutdown on 23 March 2015, which did not just impact mobile phone services, but also Internet access through Wi-Max networks. In addition, companies offering Internet-based services such as *Skype* and messaging applications such as *Whatsapp* and *Blackberry* may also be under threat, demonstrated by recent Government plans to temporarily ban *Whatsapp*, and completely ban *Blackberry's* secure messaging service by December 2015.

Network shutdowns are a fundamental risk, not just to freedom of expression, national or personal security or business operations, but also to the most fundamental of sustainable development challenges faced by all states. The new UN Sustainable Development Goals (SDGs)²³ are of direct relevance to Information and Communication Technology companies (ICTs). The SDGs aim to:

“increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.”²⁴

Therefore, stakeholders should consider the wider adverse impacts of network shutdowns on human rights, such as:

- **Safety and Security:** People are unable to assure friends and relatives that they are safe during shutdowns, causing further panic in situations of heightened tension. This concern came up frequently in the survey responses for this report. Demonstrators, health workers, human rights observers, and others are unable to call for help to be rescued from areas where protests are happening. ICTs can be used by both citizens and terrorists, but shutting down communication networks is a blunt instrument that deprives law enforcement of the opportunity to use communications for the purpose of fighting terrorism, and to disseminate important information to move people to safety, or to calm a concerned population. Advancements in technology

23 Transforming Our World: The 2030 Agenda For Sustainable Development (1 August 2015)
<https://sustainabledevelopment.un.org/content/documents/7891TRANSFORMING%20OUR%20WORLD.pdf>

24 Ibid. See 9.c

are making use of “crowdsourcing” technology that can help develop early warning systems and cement co-operation between citizens and law enforcement to create a collective shield against terrorism.

- **Restricted Access to Emergency Services:** A key dilemma concerns the state duty to protect the right to life. A government may be trying to protect the right to life - for example, by calling for network services to be shut down in an attempt to prevent a bomb being detonated - but the action also risks interrupting and stopping access to emergency services from a mobile phone. Injured people are unable to call emergency services, such as an ambulance, hospitals, fire and rescue via a mobile phone, and emergency services are unable to communicate and locate people. Doctors/ health workers are unable to access research or communicate in real time with each other. Health worker survey respondents expressed concern that they are unable to communicate directly with patients. People who need to contact police under different circumstances are unable to do so via mobile phone, such as to report crimes, in the event of an accident, or a hostage situation. This raises questions of proportionality, and how to protect the right to life by ensuring people can access emergency services. 69% of survey respondents for this report stated they did not feel safer during network shutdowns.
- **Work:** Small businesses are unable to operate and livelihoods are affected during network shutdowns. For example, businesses are unable to access data held in the cloud²⁵.
- **Education:** Students in institutions with hi-tech facilities cannot access educational material during periods of network disruption. Student respondents to the survey repeatedly voiced this as a concern.
- **Human Rights Defenders:** Human rights groups are unable to monitor situations effectively as a result of network shutdowns.
- **eServices:** Mobile banking transactions, relied on by millions of people, cannot take place if network access is not available. Transmission of health information on mobile phones also cannot take place. Other mobile services that are likely to become popular in the future, such as voting, birth registration and eGovernance, would be disrupted.
- **Economic Impacts:** There is yet to be a full study conducted on the economic impact of network shutdowns over time, but there is some indication of the loss of taxes to the government paid by operators and citizens on services that are not available during network shutdowns, not to mention lost revenues of telecommunication companies.

The results of the survey conducted for this report in March 2015 during a shutdown in Islamabad demonstrated there is often confusion among users as to what has happened during a network shutdown and a lack of communication from the government fuels speculation and suspicion. Responses range from expressions of frustration, anger, boredom, and isolation. Notably, respondents felt themselves thrown back in time to “*being back in the '90s*” or that disconnection from mobile phone networks is “*Probably what the Stone Age felt like.*”

25 In the simplest terms, cloud computing means accessing files and applications over the Internet, rather than on personal hard drives or servers, via third party services.

There are questions at an international level as to whether network shutdowns are a proportionate response to specific security related threats. The impact on freedom of expression is so severe that Special Rapporteurs on freedom of expression from the *United Nations* (UN), the *Organisation of American States* (OAS), the *African Commission on Human and People's Rights* and the Representative on freedom of the media from the *Organisation of Security and Co-operation in Europe* (OSCE), have all concluded in a Joint Declaration that cutting off access to the Internet "for whole populations or segments of the public can never be justified, including on public order or national security grounds."²⁶

In a second Joint Declaration, they concluded that filtering or shutting down entire parts of communications systems (mobile and Internet) during times of conflict can "never be justified under human rights law."²⁷ Despite these strong statements at an international level, they do not specifically address the issue of shutdowns of mobile networks outside of situations of conflict.

Outside of Pakistan, efforts by civil society to engage governments in order to reduce the frequency of network shutdowns have been attempted with varying degrees of success, for example, in Egypt and Ireland, and by an operator in Kazakhstan. However, companies and civil society have yet to join forces. Also, companies that offer Internet-based services, such as social networking (also known as "over the top" services), have not yet publicly entered the debate, even though these services would also be impacted by network shutdowns.

Recommendations for the Government of Pakistan:

- **Ensure continued access to emergency services.** Explore ways in which the emergency services can continue to operate even during periods of network disruption including by working with telecommunication operators to find ways to enable emergency calls.
- **Review the policy of network disconnection.** Consider if network disconnection is the most effective response to specific threats and explore more targeted responses. Questions to examine include: Do extremist groups have other means of communication, such as satellite communications, which make disconnecting networks redundant? Are the costs of disrupting networks, and attendant adverse impacts on daily lives, lower than the perceived benefit of dealing with a threat? The Government should work with telecommunications operators and civil society to find alternative methods to network shutdowns wherever possible.

26 Joint Declaration on Freedom of Expression and the Internet (2011) Article 6b.
<http://www.osce.org/fom/78309?download=true>

27 Joint Declaration on Freedom of Expression and Responses to Conflict Situation (2015) Article 4c
<http://www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation>

- **Review laws applicable to network disconnection.** Investigate if current laws require further clarification or if their scope can be narrowed (See Section 7 of this paper for examples from other countries where attempts were made to change the law). Governments should develop legislation to deal directly with suspension of mobile services in a clear and transparent manner, taking into account international human rights obligations. Such legislation should be subject to parliamentary review and judicial oversight.
- **Establish dialogue with companies.** Increased engagement between the Government and companies is vital to minimising the impact of shutdowns and should be part of long-term efforts to find alternatives to shutdowns.
- **Engage with citizens.** The results of the survey undertaken for this report on perceptions of network disruptions highlight confusion and mixed feelings about why and how shutdowns take place and confirm that a lack of communication from the government fuels speculation and suspicion. The Government should consider soliciting public views on the impact of network shutdowns, with the aim of improving communication and transparency.
- **Be transparent.** Wherever possible, the Government should make information publicly available about when a shutdown will take place, for how long and where. The Government should also make it a matter of public record after a shutdown has taken place by confirming the areas impacted, dates and times, plus the reason and legal justification, to improve transparency and reduce confusion.
- **Ensure Better Oversight.** The Government should consider a judicial or executive oversight mechanism, independent of the regulator, to review shutdown requests (before they are submitted and/or after the shutdown has taken place) to check that shutdowns have been authorised and implemented in accordance with the law and taking human rights concerns into account. The oversight regime should report regularly on the appropriateness of the way in which network shutdowns have been carried out and do so in ways that helps the public understand whether procedures have been followed and human rights considered.
- **Provide compensation to operators.** Financial losses incurred during network shutdowns should be adequately compensated in accordance with Section 54(3) of the 1996 Pakistan Telecommunications (Re-organisation) Act, Reason: "National Security"²⁸.

28 Section 54 states: "During a war or hostilities against Pakistan by any foreign power or internal aggression or for the defence or security of Pakistan, the federal government shall have preference and priority in the telecommunication system over any licensee. Upon proclamation of emergency by the President, the Federal Government may suspend or modify all or any order or licences made or issued under this Act or cause suspension of operation, functions or services of any licensee for such time as it may deem necessary provided the federal government will compensate any licensee whose facilities or services are affected by any action under this sub-section."

http://www.pta.gov.pk/media/telecom_act_170510.pdf

See also, *Telecommunications Industry Dialogue*, Information on Country Legal Frameworks pertaining to Freedom of Expression and Privacy in Telecommunications: Pakistan

<http://www.telecomindustrydialogue.org/resources/pakistan/>

Recommendations for Telecommunications Operators:

- **Open dialogue with Governments.** *Telenor Pakistan* and other operators in Pakistan have made great efforts to engage the Government of Pakistan in discussion, which has resulted in some limitations on network shutdowns in terms of scope and duration, and a more streamlined process of submitting requests. This demonstrates that while the issue is sensitive, positive change can be achieved by opening a dialogue with governments.
- **Widen support within the industry through collective action.** One company is unlikely to be able to effect widespread change at a local level. Telecommunication companies are finding a voice through membership in global industry initiatives such as the *Telecommunications Industry Dialogue*, a group of telecommunications operators and vendors who jointly address freedom of expression and privacy rights in the telecommunications sector in the context of the *UN Guiding Principles on Business and Human Rights*²⁹. Other telecommunication operators worldwide face challenges similar to those of *Telenor Pakistan*, and this platform could be used to exchange learning and discuss ways forward, including how to encourage dialogue between local operators on the ground.
- **Conduct stakeholder engagement.** According to the *UN Guiding Principles on Business and Human Rights*, businesses should build relationships and mutual understanding with stakeholders. In the ICT sector, in the case of network disconnection, both the company and local civil society have the same aim: to reduce the frequency of network shutdowns. Both can utilise their distinct skills and leverage to achieve this by joining forces. Greater alignment between business and civil society has the potential to produce real and long-lasting action that will ultimately improve the enjoyment of human rights.
- **Create a consumer grievance mechanism.** Customers should have effective means to report adverse impacts experienced during network shutdowns including on health, education and work. Companies should also explore how customers can be compensated for loss of service during network shutdowns.
- **Ensure transparency.** Public reporting on network shutdowns remains in its infancy. One area where further development is possible is to explore whether companies could publicly report instances when they have been ordered to wholly or partially shut down a network, or when they have been asked to block access to a particular service. The laws in some countries prevent companies from even revealing this information, and some companies believe the onus should be on governments to publish this information, not companies. *Telenor Group* and the mobile operator *Vodafone* have taken the step of including a review of laws they must abide by regarding suspension of services³⁰. In addition, the *Telecommunications Industry Dialogue* published an online resource detailing the laws of 44 countries concerning freedom of

29 <https://telecomindustrydialogue.org/>

30 *Telenor Group*, Government Access Report- Legal Overview (May 2015)

http://www.Telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf

See also Vodafone's 2015 Law Enforcement Disclosure Report here:

http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf

expression and privacy in telecommunications, including an analysis of Pakistan's laws.³¹ This analysis is useful and can help develop advocacy positions as a starting point for dialogue with governments.

This study highlights the need for further in depth research into government-ordered network shutdowns and their adverse impacts on society. In the meantime, a more concerted effort is needed to implement a streamlined process for requesting network shutdowns. From the analysis of the process of requesting network shutdowns in Pakistan, this report recommends that any process for requesting network shutdowns include the following key characteristics:

- Governments and ICT companies should refrain from authorising network shutdowns impacting the entire country.
- Network shutdowns should only be invoked in cases of real and imminent threats to national security or national emergencies, and requests should specify reason for such disruptions.
- National law should be in place to regulate network shutdowns including which bodies or agencies are authorised to make requests.
- Shutdown requests should be approved or authorised by the highest level of the government.
- Clear request processes should be established, with a limited number of actors in authorised law enforcement agencies allowed to make requests, and designated individuals within operators to receive such requests.
- All shutdown requests to network operators should be made in writing. The request should specify the duration and geographical reach of the shutdown as well as the reason, and demonstrating direct material necessity. Shutdowns should be limited in duration and geographical area and proportionate to the perceived level of risk.
- Whenever possible, the public should be informed of network shutdowns, including their duration, geography and services affected.
- All network disruptions should be logged/recorded, and the government should publish annually a list of all shutdowns.
- Access to and communication with emergency services should be guaranteed to the public at all times, including during network shutdowns.
- Legislation concerning network shutdowns should be subject to on-going review, including reviews by independent oversight bodies of specific events and disruptions.

31 *Telecommunications Industry Dialogue*, Information on Country Legal Frameworks pertaining to Freedom of Expression and Privacy in Telecommunications, June 2015. <http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/>

and the service covers over 90% of its geographical area.³⁷ When *Telenor Pakistan* entered the market in 2004, the total number of mobile subscriptions in Pakistan was just under 13 million, out of a population of 158 million people. By 2015, total mobile subscriptions reached over 116 million³⁸, in a current population of over 180 million people. Put another way, the total mobile penetration of Pakistan in 2002-2003 was 3.29%. As of July 2015 it is 61.45%³⁹, assuming one unique person uses each phone.

In the last decade, the telecommunication industry's tax contributions to the exchequer have grown from PKR 38.4 billion (US\$ 377 million) in 2003-04 to PKR 234.53 billion (US\$ 2.3 billion) in 2013-2014.⁴⁰

Internet use is on the rise in Pakistan, via Wi-Fi Internet connections or using 3G technology via mobile phones. There are around 50 Internet service providers (ISPs) in Pakistan.

1.1 About Telenor Group

Telenor Pakistan is 100% owned by *Telenor Group*⁴¹, a telecommunications company based in Norway. *Telenor Group* was established in 1855 and operates in 13 countries across Europe and Asia.⁴²

Worldwide, *Telenor Group* has over 187 million mobile subscribers and employs around 33,000 people. Worldwide revenues in 2014 were NOK 107 billion (around US \$13.5 billion).⁴³ *Telenor Group* holds a 33% non-controlling stake in Netherlands based operator *Vimpelcom*, which is present in a further 14 countries. *Vimpelcom* also has a stake in *Mobilink*, which has the largest market share of mobile services in Pakistan.⁴⁴

Telenor Group's human rights policy states the company's commitment to implementing the *UN Guiding Principles on Business and Human Rights*,⁴⁵ including respect for freedom of expression and privacy. *Telenor Group* is a member of the *Telecommunications Industry Dialogue*.

37 Farooq Baloch, The Tribune, FY2013: Telecom sector's revenues reach all-time high (4 January 2014) <http://tribune.com.pk/story/654539/fy2013-telecom-sectors-revenues-reach-all-time-high/>

38 July 2015 figures available at: <http://www.pta.gov.pk/index.php?Itemid=599>

39 Ibid.

40 Ibid.

41 <http://www.Telenor.com.pk/history>

42 The 13 countries are: *Telenor* Norway, *Telenor* Denmark, *Telenor* Sweden, *Telenor* Hungary, *Telenor* Montenegro, *Telenor* Serbia, *Telenor* Bulgaria, *Telenor Pakistan*, *Telenor* Myanmar, Grameenphone (Bangladesh), dtac (Thailand) DiGi (Malaysia) Uninor (India)

43 *Telenor Group* Annual Report 2013

<http://www.Telenor.com/wp-content/uploads/2014/04/Telenor-Group-Annual-Report-2013.pdf>

44 <http://www.Vimpelcom.com/Profile/Understanding-Vimpelcom/Brands/Mobilink/>

45 <http://www.Telenor.com/sustainability/human-rights/respect/>

Telenor Groups's human rights policy acknowledges some of the challenges facing telecommunications operators, including times governments may order the company to shutdown communication services:

"Another type of request we may get is to shut down the network. *Telenor* does not advocate the shutdown of its networks and believes that it is in the best interest of its customers to minimise disruption of its services. However, in extraordinary circumstances a government may require a network shutdown to protect its citizens from terrorism or other serious safety or security threats. *Telenor* will comply only as necessary and will resume operations as quickly as possible following such an incident."⁴⁶

Telenor Groups's 2013 annual report recognised that business in Pakistan is set to grow, but that the benefits brought by telecommunications are being hampered by network shutdowns:

"Total revenues in local currency increased by 3% driven by growth in subscriptions and usage, but negatively affected by several regulatory restrictions including government enforced network closures and a slow-down of economic growth in Pakistan."⁴⁷

In May 2015, *Telenor Group* published its first transparency report on government requests for user data, covering the 13 countries in which *Telenor Group* operates a subsidiary company. The report covers the number of times law enforcement agencies in each country requested lawful interception (real time access to content of communications such as phone calls) or access to communications data (such as telephone numbers, time, duration and location of specific calls) in 2014.⁴⁸ These data are accompanied by a legal review of each country, disclosing where possible the laws each *Telenor Group* subsidiary is compelled to disclose on issues such as user communications or restricted access to services.⁴⁹ The number of requests for network shutdowns is yet to feature in *Telenor Group's* transparency report nor is such information included in the transparency reporting of any other telecommunications operator.

46 <http://www.Telenor.com/sustainability/human-rights/mitigate/>

47 *Telenor Group* Annual Report, 2013, p11:

<http://www.Telenor.com/wp-content/uploads/2014/04/Telenor-Group-Annual-Report-2013.pdf>

48 *Telenor Group*, Authority Requests for Access to Electronic Communication- Country Data (May 2015) http://www.Telenor.com/wp-content/uploads/2015/05/Authority-requests-for-access-to-electronic-communication_04.pdf

49 *Telenor Group*, Government Access Report- Legal Overview (May 2015)

http://www.Telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf

1.2 Telenor Pakistan

Telenor Pakistan entered the mobile telecommunications market in Pakistan in 2004, with an initial investment of US \$1 billion to modernise and improve infrastructure. As of August 2015, it currently has 31.49 million subscribers, which relates to individual customers, out of a population of 158 million people. However there are 114.65 million mobile connections, which relates to the number of SIM cards connected to *Telenor Pakistan's* network.⁵⁰ *Telenor Pakistan* has a market share of 27.4%, making it Pakistan's second largest operator just behind *Mobilink* with 29.15% of the market share.⁵¹ *Telenor Pakistan* offers services in 3,500 cities and towns, covering more than 80% of the population. In 2014, *Telenor Pakistan* won one of the licenses to roll out 3G services and now offers mobile Internet to over 150 cities and towns throughout the country.

Telenor Pakistan directly employs over 2,700 people in Pakistan and indirectly employs 25,000 people in a network of over 200,000 retailers, comprising both local agents and retail outlets.

Telenor Pakistan has its own code of conduct which, like the Group Code of Conduct, is developed based on international and regional standards, including the UN Universal Declaration of Human Rights, the *UN Guiding Principles on Business and Human Rights* and the OECD Guidelines for Multinational Corporations.⁵² Each employee is required to sign this code and undergo training on understanding and implementing the principles and standards therein. Each employee undergoes annual, non-evaluated "refresher" courses, which includes working through real life examples to show how the code of conduct works in practice.

50 See Joss Gillet, GSMA, Measuring mobile penetration: Untangling 'subscribers', 'mobile phone owners' and 'users' 22 May 2014, "If one individual actively uses two SIM connections, that person will be counted by the industry as two mobile connections although he or she is only one mobile subscriber" <https://gsmaintelligence.com/research/2014/05/measuring-mobile-penetration/430/>

51 Figures provided by *Telenor Pakistan*, August 2015

52 <http://www.Telenor.com.pk/cr/pdf/newCOC.pdf>

2. History of Network Shutdowns in Pakistan

According to the *Global Terrorism Index* published by the *Institute for Economics and Peace*, 17,958 people died in terrorist incidents around the world in 2013.⁵³

Of these, Pakistan accounted for 13.1%, ranking third, after Iraq and Afghanistan. Terrorism is a major and genuine security threat in Pakistan.

In 2013, there were 1,933 terrorist “incidents”, which killed 2,345 people and injured 5,035.⁵⁴ In the same year, 23 different terrorist groups were known to be operating in Pakistan. The *Global Terrorism Index* reports that Islamist groups make up a significant portion of this total. The largest, responsible for 49% of claimed attacks is Tehrik-i-Taliban Pakistan (TTP), the Pakistani Taliban. However, in nearly half of all attacks in the country in 2014, no group claimed responsibility.⁵⁵

Terrorism in Pakistan takes many forms.⁵⁶ These include attacks on armed forces and their families by rebel groups; attacks by the Pakistani Taliban and other organisations against organs of state; attacks within Pakistan among political rivals; religious violence against minority communities; intra-Muslim violence, usually targeted against Shia Muslims; violence spilling over from the weakly-guarded border with Afghanistan; and, in the past, violence involving the Mohajir community (Muslims who migrated from India at the time of Partition in 1947), as victims or perpetrators.

Terrorism victims include prominent politicians such as former prime minister Benazir Bhutto, former Punjab governor Salman Taseer, and former minister of minority affairs, Shahbaz Bhatti, and scores of civilians, often during religious processions, religious holidays, or at shrines.

Following the tragic attack⁵⁷ on the Army Public School in Peshawar on 16 December 2014, the Government of Pakistan amended the constitution to allow for “speedy” trial of offences relating to terrorism.⁵⁸

53 Vision of Humanity, Global Terrorism Index

<http://www.visionofhumanity.org/#/page/our-gti-findings>

54 Vision of Humanity, Global Terrorism Index Report 2014, p18:

<http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014.pdf>

55 Ibid.

56 The Global Terrorism Index defines terrorism as “the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation.” (Ibid p6)

57 John Boone and Ewan MacAskill, The Guardian, More than 100 children killed in Taliban attack on Pakistan school (16 December 2014)

<http://www.theguardian.com/world/2014/dec/16/taliban-attack-army-public-school-pakistan-peshawar>

58 The Constitution of Pakistan, Constitution (Twenty-First Amendment) Act, 2015

<http://www.pakistani.org/pakistan/constitution/amendments/21amendment.html>

The Pakistan People's Party (PPP) won the 2008 elections following the resignation of General Pervez Musharraf, but political stability and national security were a growing concern.⁵⁹ During this time, more civilians, security personnel, known terrorists and insurgents were being killed every year.⁶⁰

Between 2008 and 2012, 12,020 civilians were killed in terrorism-related violence.⁶¹ Terrorist groups also began using technology to advance their aims. ICT-enabled tactics included using messages exchanged through mobile phones and setting off explosives from remote locations through mobile technology.

In 2012, the then Interior Minister of Pakistan began ordering mobile network shutdowns in more parts of the country as a tool aimed at curbing terrorist activities. Before 2012, *Telenor Pakistan* said that network shutdowns (or "blackouts" as they were referred to then) were experienced mostly in Balochistan, coinciding with the military operations that started in early 2005. Shutdowns now occur around a wider range of events, such as religious or national holidays, protests and marches. Shutdowns usually block mobile services, such as voice, SMS and mobile Internet.⁶²

According to *Telenor Pakistan*, these shutdowns peaked in 2012 and 2013 with a decline following the May 2013 elections. The elections ushered in the opposition Pakistan Muslim League, led by Prime Minister Nawaz Sharif, who promised a more "business friendly" agenda and sought closer co-operation with business to help boost the economy.⁶³ The change in government was accompanied by a partial reduction in shutdowns.

The Islamabad based digital rights group *Bytes for All* began keeping a record of all network shutdowns that occurred in the country from 2012⁶⁴, part of which is included as an Annex in this paper. These records suggest network shutdowns began to slow in 2014, but still continue to this day.

According to these data, it is rare for whole regions or provinces to experience a shutdown, although the regions of Balochistan and Gilgit-Baltistan do appear to face occasional disruptions in their entirety. However, many towns and cities can be impacted at one time by network shutdowns, which essentially means potentially

59 Arfan Shahzad, Dawood Ali Mithani, Abdullah Kaid Al Swidi , Faudziah Hanim Bt Fadzil, Political Stability and the Foreign Direct Investment: Inflows in Pakistan. Table 10 Political Stability Indicators, British Journal of Arts and Social Sciences ISSN: 20469578, Vol.9 No.II (2012)
http://www.bjournal.co.uk/paper/BJASS_9_2/BJASS_09_02_08.pdf

60 Fatalities in Terrorist Violence in Pakistan 2003-2015
<http://www.satp.org/satporgtp/countries/pakistan/database/casualties.htm>

61 Ibid.

62 ARTICLE 19, Pakistan: Government must stop 'kill switch' tactics (23 August 2012)
<http://www.article19.org/resources.php/resource/3422/en/pakistan:-government-must-stop-%27kill-switch%27-tactics>

63 Business Recorder, PML-N government is business friendly (17 August 2013)
<http://www.brecorder.com/top-news/108-pakistan-top-news/131719-pml-n-government-is-business-friendly.html>

64 <http://www.killswitch.pk>

millions of people are affected in wide geographical areas.

For example, during the Day of Ashura in 2014, *Bytes for All* reported that a network shutdown impacted a total of 56 cities and towns in Punjab, Sindh, Khyber Pakhtunkhawa, Balochistan, Gilgit-Baltistan and Azad Kashmir, which are almost all of the regions in Pakistan.

Although the threat of terrorism remains very real in Pakistan, there is concern among civil society groups that network shutdowns are becoming the norm. They contend that such disruptions are an inadequate tool to control the wider problem of terrorism, and grind much of day-to-day life to a halt.

In addition, the Government of Pakistan rarely communicates the reason for shutdowns, either before or after the fact, nor does it confirm when and where they have happened, which creates confusion and suspicion among citizens.

3. The Network Shutdown Process in Pakistan: Telenor Pakistan's Role and Responsibilities⁶⁵

The process of shutting down mobile networks in Pakistan was only streamlined across all operators in 2009, when the Ministry of Information Technology issued a directive to the national regulator, the *Pakistan Telecommunication Authority* (PTA),⁶⁶ following appeals from operators for a formal, established process. Before 2009, any part of the government or its law enforcement agencies could request operators to shutdown the network, and no common process or focal point was in place for the submission of these requests. This *ad hoc* method posed clear problems for the company, including its relationship with the State and its own responsibilities with respect to human rights. Although the directive was issued in 2009, *Telenor Pakistan* told IHRB during an interview as part of the preparation of this report that the process was not actually established until 2012.

The Government's policy directive defined a standard operating procedure for shutting down mobile networks. A shutdown request is now always routed through the *PTA*, so the operator knows it has been verified. A number of law enforcement agencies are authorised to request network shutdowns to the *PTA*, but the identity of these agencies remain confidential and not public knowledge. A designated person in an authorised law enforcement agency typically submits a request to the *PTA* for a network shutdown. Because requests are sent via the *PTA*, the telecommunications operator may not be aware of which specific law enforcement agency has made a specific request. *Telenor Pakistan*, like other operators in Pakistan, is obligated to shut down their network when ordered by the *PTA* and this provision is included in the company's operating license. The *PTA* Director General of Enforcement is the only person authorised to communicate shutdown requests to telecom operators.

According to *Telenor Pakistan*, there does not seem to be a standard notice period given in order to implement a Government shutdown request. During interviews as part of the preparation of this report, one employee told IHRB that a notice of 12-14 hours is given, while another employee said three hours notice was a more accurate figure. Several employees verified that some requests require the shutdown with immediate effect in case of an imminent threat or a high security situation. These requests can come in at any time of the night or day.

Telenor Pakistan said reasons for shutdown requests are usually quite general, such as "security" related matters. Once a request has been sent in writing (usually an email) by the *PTA*'s Director General of Enforcement to the designated person in *Telenor Pakistan* authorised to receive such requests, the technical team begins the process of shutting down the requested part of the network. The request usually specifies the geographical area, time and duration of the shutdown.

65 This process was described to IHRB by *Telenor Pakistan*'s Regulatory and Technical teams.

66 <http://www.pta.gov.pk/index.php?Itemid=1>

Shutdown requests are usually restricted to a small geographical area, described by *Telenor Pakistan* as “surgical” shutdowns, rather than “blanket” shutdowns, where cities or the entire country is affected. *Telenor Pakistan* representatives indicated that “surgical” shutdowns, blocking only sensitive areas rather than entire cities, require much more time and effort on the part employees as services in that area may be provided by more than one cell tower. It may also be necessary to shut down a wider area than specified, to ensure there is no “spillover” of service -- i.e. communications being accessible just outside of the designated shutdown site. *Telenor Pakistan* maintains a record of each shutdown. Before such disruptions became routine, *Telenor Pakistan* used to send reports, including financial losses to the company, to the *PTA*. However, when the Government made no resulting compensatory payments, this practice was stopped.

Key Observations:

The process for requesting network shutdowns in Pakistan currently follows several key steps:

- **A request is submitted by an authorised law enforcement agency to the Regulator, the Pakistan Telecommunications Authority (PTA).**
- **The PTA verifies the request and submits it to a designated person in the telecommunications operator in writing.**
- **The request specifies the geographical area, time and duration of shutdown.**

While *Telenor Pakistan* has never refused to implement a shutdown request, the company said it has engaged the Government, usually by requesting a narrowing of the scope of specific requests. As a result, *Telenor Pakistan* says shutdowns today are more ‘surgical’, focusing on high-risk geographical areas, rather than blanket shutdowns over entire cities. However, as many provinces and cities may be impacted by one shutdown, the operator has an ongoing dialogue with the regulator to explore how shutdowns can be limited in scope and duration. The operator keeps a record of each network shutdown.

- **The operator may have to implement the shutdown in a wider area to prevent “spillover”.**

Despite reforms over the past few years, there continues to be no standard notice period given to the operator and the length of time networks are disrupted varies greatly. From the limited records available, it appears shutdowns can last from isolated occasions of several hours to a few shutdowns repeated over several days. In addition, areas outside of the designated shutdown area, known as “spillover”, can be affected as well. This means areas where no security threat exists may end up with limited access to mobile communications.

Telenor Pakistan attempted to challenge the legal justification for shutdowns of any kind, but the law remains vague and wide in scope, as the next section of this report discusses in more detail.

4. The International and National Legal Framework

4.1 Pakistan's Responsibilities under International Human Rights Law

Pakistan ratified the *International Covenant on Civil and Political Rights* (ICCPR) in 2010 and the *International Covenant of Economic, Social and Cultural Rights* (ICESCR) in 2008.

Freedom of expression is enshrined in international law and is reflected in almost every country's constitution, including Pakistan. Under international law, the universal right to freedom of expression is well defined and clarified in a number of legally binding instruments and further declarations and principles:

Universal Declaration of Human Rights (UDHR) 1948:

Article 19: "Everyone has the right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

International Covenant on Civil and Political Rights (ICCPR) 1966:

Article 19: "1. Everyone has the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

Under international law, each country may have its own reservations on freedom of expression according to the country's social and religious norms, which are reflected in that country's domestic law. Article 19 (3) of the ICCPR states,

"The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be as are provided by law and are necessary:

- (a) for respect of the rights or reputations of others;
- (b) for the protection of national security or of public order (ordre public), or of public health or morals."

A country's history may dictate the restrictions it legally places on freedom of expression,

in order to protect the rights of others.⁶⁷ Further clarification on the application of Article 19 paragraph 3 (which allows for restrictions on freedom of expression) is recorded in UN General Comment 34.⁶⁸ Paragraph 34 of the General Comment also introduces the principle of proportionality:

“Restrictions must not be overbroad. The Committee observed in general comment No. 27 that “restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law”.

Therefore, any restriction on fundamental rights must be proportionate to the threat posed, provided for by law, and strictly necessary to achieve a proper public purpose, such as public safety. It is up to the State to demonstrate that a network shutdown is proportionate to the threat proposed.

UN treaty bodies have not to date issued concluding observations on Pakistan’s implementation of the right to freedom of expression under the ICCPR in relation to network shutdowns.

4.2 The International Telecommunications Union (ITU)

The *ITU* is the UN’s specialised agency for promoting development and use of ICTs. Membership includes the UN’s 193 Member States, and also ICT regulators, academic institutions and over 700 private companies.⁶⁹

The Constitution of the ITU protects the free flow of information and the right to communicate⁷⁰ and allows for network shutdowns in certain situations, albeit with unclear definitions:

67 Freedom of expression is not an absolute right and in order to protect the rights of others, states are permitted to derogate from this. See ICCPR Article 19:3 “The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be as are provided by law and are necessary: for respect of the rights or reputations of others; for the protection of national security or of public order (ordre public), or of public health or morals.”

68 UN General Comment 34, Article 19: Freedom of expression CCPR/C/GC/34, 12 September 2011. <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

69 <http://www.itu.int/en/about/Pages/default.aspx>

70 See for example, Article 33 of the Constitution, The Right of the Public to Use the International Telecommunications Service http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF (p37) and, Recommendation 2, Unrestricted Transmission of News and the Right To Communicate (Kyoto 1994) http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF (p655)

Article 34/181: "Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."

The ambiguity in terms such as 'public order' and 'decency' make it difficult to ascertain the specific situations in which shutdowns are justified.

4.3 Expert International Opinion on Network Shutdowns

Access to the Internet is well regarded as an enabler to freedom of expression.⁷¹ Experts from various bodies have declared that network shutdowns can rarely be justified due to the impact on freedom of expression. In 2011, Special Rapporteurs on Freedom of Expression from the UN, the Organisation for Security and Co-operation in Europe (OSCE), the Organisation of American States (OAS) and the African Commission on Human and People's Rights issued a Joint Declaration on Freedom of Expression and the Internet, which stated:

"Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet."⁷²

In May 2015, the same consortium of Special Rapporteurs issued a Joint Declaration on Freedom of Expression and Responses to Conflict Situations. This declaration states:

"...using communication 'kill switches' (i.e. shutting down entire parts of communications systems)... are measures that can never be justified under human rights law."⁷³

While these statements cover Internet shutdowns and network shutdowns in conflict situations, there is ambiguity as to the impact of mobile shutdowns in a government proclaimed "emergency".

4.4 Pakistan's National Laws

Article 19 of the Pakistan Constitution enshrines freedom of speech as a fundamental right, subject to several restrictions.

71 See Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16th May 2011. UN General Assembly A/HRC/17/27. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

72 Joint Declaration on Freedom of Expression and the Internet 2011, Article 6b. <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848>

73 Joint Declaration on Freedom of Expression and Responses to Conflict Situations, 2015, Article 4c <http://www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation>

“Article 19: Freedom of Speech etc.

Every citizen shall have the right to freedom of speech and expression, and there shall be freedom of the press, subject to any reasonable restrictions imposed by the law in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, commission of or incitement to violence.”⁷⁴

In addition, the Pakistan Constitution guarantees the right to information, which is impacted by a network shutdown:

“19A. Right to Information:

Every citizen shall have the right to have access to information in all matters of public importance subject to regulation and reasonable restrictions imposed by law.”

While Pakistan has no direct constitutional provision regarding suspending mobile service, the government has cited Article 148 of the Constitution as justification.

Article 148 (3) states:

“It shall be the duty of the Federation to protect every Province against external aggression and internal disturbances and to ensure that the Government of every Province is carried on in accordance with the provisions of the Constitution.”

The suspension of services has also been justified under Article 54(2) and 54(3) of the 1996 Pakistan Telecommunications (Re-organisation) Act⁷⁵, Reason: “National Security”. It states that:

“54 (2) During a war or hostilities against Pakistan by any foreign power or internal aggression or for the defence or security of Pakistan, the Federal Government shall have preference and priority in the telecommunication system over any licensee.

54(3) Upon proclamation of emergency by the President, the Federal Government may suspend or modify all or any order or licences made or issued under this Act or cause suspension of operation, functions or services of any licensee for such time as it may deem necessary provided the Federal Government will compensate any licensee whose facilities or services are affected by any action under this sub-section.”

According to the international NGO, ARTICLE 19, which campaigns globally for the right to freedom of expression and freedom of information, Article 54(3) is inconsistent

74 <http://www.pakistani.org/pakistan/constitution/part2.ch1.html#30>

75 http://www.pta.gov.pk/media/telecom_act_170510.pdf See also, *Telecommunications Industry Dialogue*, Information on Country Legal Frameworks pertaining to Freedom of Expression and Privacy in Telecommunications: Pakistan <http://www.telecomindustrydialogue.org/resources/pakistan>

with the permitted restrictions on freedom of expression under the ICCPR.⁷⁶

During interviews for this report, *Telenor Pakistan* officials told IHRB that the company has disputed and contested the use of Section 54(3) for invoking network shutdowns, since these powers can only be invoked if a state of emergency has been declared in the country. *Telenor Pakistan* believes that in the absence of a state of emergency, the provision does not apply and therefore network shutdowns are orders without any legal basis.

In 2012 *Telenor Pakistan* filed a writ petition in the Sindh High Court⁷⁷, and this case is still pending at the time of writing. In addition, citizens have filed writ petitions to challenge network shutdowns for the reasons that these shutdowns caused disruption in their personal and professional lives and were a threat to their security and well-being.

Around the same time as *Telenor Pakistan* filed a writ petition, another was filed by a gynaecologist, Dr Nishat Fatima, on the basis that shutdowns prevented her from communicating with her patients.⁷⁸ According to reports, during one particular shutdown a patient who was pregnant was unable to get in touch with Dr. Fatima when she wasn't feeling well and when Dr. Fatima was able to make contact discovered the pregnant woman had lost her baby.⁷⁹

Telenor Pakistan officials indicated that as a result of the initial hearings of the writ petition filed by the company, as well as on account of similar writ petitions filed in the Sindh High Court by ordinary citizens, the court passed an initial order on 25 October 2012 that any directive to shutdown the network should be made through a "speaking order with cogent reasons given for it" and that it should only apply to specific areas and be valid for a specific duration.

This is a significant development because a speaking order sets out reasons and rationale for a decision and cogent reasons for an order means that specific and actionable grounds are given for the order, thus making it easier to challenge before the courts. In addition, the reference to "specific areas" and a "specific duration" restricts the government's power to make open-ended orders for whole cities and for inordinately long periods and instead imposes upon them the requirement to pass an order which is targeted and a specific, reasonable duration.

76 ARTICLE 19 recommends Article 54(3) should be revised to ensure that any disconnections or shutting down of services is only approved by a court in limited, specific circumstances allowed under international law ARTICLE 19 (201) Pakistan: Telecommunications (Re-Organisation) Act Legal Analysis, p16 <http://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf>

77 Tahir Siddiqui, Dawn, Cellphone service suspension, SHC issues notice to PTA chairman (20th November 2012) <http://www.dawn.com/news/765389/cellphone-service-suspension-shc-issues-notice-to-pta-chairman-others>

78 The Express Tribune, Irked gynaecologist takes govt to court (22nd November 2012) <http://tribune.com.pk/story/469411/cellphone-ban-irked-gynaecologist-takes-govt-to-court/>

79 Fahad Desmukh, PRI, Pakistanis questions government's use of bans on cell phones, other tech (3rd January 2013) <http://www.pri.org/stories/2013-01-03/pakistanis-question-governments-use-bans-cell-phones-other-tech>

Before this order was passed, any directive for suspending the network did not need to provide a rationale or reasoning and could extend to whole cities and be open-ended.

However, owing primarily to the general delays in the adjudication of legal cases by the courts in Pakistan, *Telenor Pakistan's* writ petition is yet to be conclusively determined with a substantive final order on the overall merits of the case, including the issue of compensation for the financial losses suffered as a result of network shutdowns.

The Constitution of Pakistan clearly protects the right to free expression and information. It is not clear under the Telecom Law if the Government has the authority to shut down the network, and if so, under which specific circumstances. It is therefore difficult to determine how tests of necessity and proportionality would be carried out. It appears the policy of network shutdowns in Pakistan and the law governing them would benefit from a Government review that reflects the country's international human rights obligations.

Section 7 describes some instances from other countries where relevant laws were clarified and the scope of network shutdowns narrowed, in an effort to limit the frequency and potential for negative impacts on citizens.

5. The Network Shutdown on Pakistan Day - 23 March 2015

Pakistan Day is a national holiday held on 23 March each year to commemorate the signing of the 1940 Lahore Resolution, which called for an independent Muslim state that became Pakistan.

Pakistan Day has historically been commemorated with a large joint military parade in the centre of Islamabad, featuring displays by the Pakistan Army, Navy, and Air Force. The last such parade took place in 2008, but was put on hold amid security concerns. In 2015, the National Day Parade was again held in Islamabad, at a specially built site near Shakar Parian Park.⁸⁰

According to *Bytes for All*, in the run up to 23 March, there were rumours that mobile communications would be suspended from 11 March and disruption would last for 13 days. Restrictions would reportedly apply to a 5km radius around the site earmarked for the National Day Parade in Shakar Parian Park in the centre of Islamabad, as well as areas of Rawalpindi. This area covered a number of densely populated residential and commercial areas, as well as a major hospital, the Shifa International Hospital.

On 11 March, a number of residents in the area took to social media to complain about a loss of mobile service and to ask whether a shutdown was taking place.⁸¹ Neither the Government nor the regulator, the *Pakistan Telecommunication Authority* (PTA), issued any public communication to clarify the situation.

The National Day Parade passed peacefully, and it was only after the event that it was possible for IHRB to clarify with *Telenor Pakistan* what had happened with regards to the shutdown. According to reports, on 11 March, all mobile operators in Pakistan received a request to shutdown mobile communications within a 5km radius of the parade site from 12 to 23 March 2015. The reason given for the unprecedented duration of the shutdown was that dress rehearsals would be taking place over the days leading up to the Parade.

Representatives from the main mobile operators met with representatives from the Government of Pakistan and the *PTA* to express their concerns about the scope and scale of the requested shutdown. They pointed out that a key issue involved the fact that a major hospital lay inside the shutdown site, and that disruption of network service was impacting patients and relatives, visiting hours, ambulances and hospital staff communication.

The shutdown site also included an airport, the area of Shamsabad, Faizabad and the area of Rawalpindi, outside of Islamabad. There was no reported security threat in Rawalpindi or the surrounding areas. This area was shutdown in order to deal

80 Dawn, Pakistan holds first Republic Day parade in seven years (23 March 2015)

<http://www.dawn.com/news/1171371>

81 <https://storify.com/bytesforall/reports-of-mobile-network-outage-in-islamabad-marc>

with “spillover”(i.e. communications being able to be accessed just outside of the designated shutdown site).

Following conversations with the mobile operators, the Government of Pakistan and the *PTA* agreed to limit the shutdown between 5 am and 2 pm on 21 March, when a full military dress rehearsal took place, and during the same period on 23 March, the day of the parade itself, rather than the extended period originally requested.⁸²

All GSM/3G/4G services, Wi-MAX (a form of Wi-Fi capable of connectivity across greater distances) and CDMA (similar to GSM) services would be shutdown during these times, impacting nearly all voice and data services. While the scope of the shutdown was limited, the extent of services impacted was greater than other shutdowns, which had been restricted to mobile services, rather than including Internet access (as in this case Wi-MAX was also affected).

82 The parade took place between 8am and 12pm on 23 March 2015.

6. The Impact of Network Shutdowns and Effectiveness of Government Policy

In September 2015, the UN adopted a set of 17 Sustainable Development Goals (SDGs) aimed at combating poverty and advancing health, education, livelihoods, and access to information, as well as tackling gender and income inequality among other objectives.⁸³

Information and Communication Technology (ICT) is a key enabler to all of these, including in low-income countries, and the SDGs aim to, “increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.”⁸⁴

Network shutdowns are therefore a fundamental risk, not just to freedom of expression, national or personal security or business operations, but also to the most fundamental of sustainable development challenges faced by all states.

In the summer of 2014 *Bytes for All*, the *Centre for Internet and Human Rights* (CIHR) and IHRB developed a research project and survey methodology intended to better understand the effects of network disconnections. *Bytes for All* conducted 190 face to face field surveys to collect firsthand information on impacts in the immediate aftermath of the Pakistan network shutdown on 23 March 2015. Survey respondents were selected at random and from *Bytes for All's* contacts, from a range of occupations including business professionals, journalists, doctors, teachers and lecturers, students and human rights defenders.

The results of these surveys served as a catalyst for further research into the identified impacts and for the development of recommendations to mitigate adverse impacts of network disruptions on fundamental rights.

Although the shutdown took place over a public holiday, and therefore perhaps had a more limited impact than on a normal work day, the extent of services affected was greater than previous shutdowns, which had been restricted to mobile services, rather than including Internet access (as in this case Wi-MAX was also affected).

Overleaf we highlight some of the impacts identified by respondents, which suggested the need for further research.

83 Transforming Our World: The 2030 Agenda For Sustainable Development (1 August 2015) <https://sustainabledevelopment.un.org/content/documents/7891TRANSFORMING%20OUR%20WORLD.pdf>

84 Ibid. See 9.c

6.1 Safety and Security

Survey respondents were asked if they relied on other forms of communication during network shutdowns. Respondents said they often reverted to using landlines during shutdowns, which are not usually affected. Other messaging apps such as *Whatsapp* and Voice Over Internet Protocol (VoIP) tools such as *Skype* are typically available when they can connect to Wi-Fi.

However, Government officials have contended that terrorists are also attempting to circumvent mobile network shutdowns by using other methods of communication, such as *Skype*.⁸⁵ The Government has therefore previously floated plans to ban tools such as *Skype* and messaging apps such as *Whatsapp* and *Viber*, which are usually still available over Wi-Fi during mobile network shutdowns.⁸⁶ The Government of Sindh province decided to block these services for three months in 2013,⁸⁷ although this seemed at odds with central Government policy, which reportedly did not want to impose such a ban.⁸⁸

In July 2015, it was reported that Pakistan's telecommunications regulator had issued a directive to operators to permanently shutdown *Blackberry* services, which features an encrypted messaging service. This order was to be implemented before December 2015.⁸⁹ This indicates that the trend of blocking communication services for security reasons may be set to increase in scope, yet there appears to be inconsistency and no official policy or consultation on this proposal. Such expansion was witnessed during the network shutdown on 23 March 2015, which did not just impact mobile phone services, but also Internet access through Wi-Max networks.

While it is clear that ICTs can be used both for good purposes as well as for bad, shutting down communication networks is a blunt instrument that deprives law enforcement of communications tools for the purpose of fighting terrorism and protecting public safety. One survey respondent reflected that leaving communications networks functional would be a more effective strategy as "we can catch terrorists through networking instead of disconnection."

85 Imtiaz Ali, Dawn, Safoora Goth carnage suspects used to communicate via VoIP: Sindh IGP (30 June 2015) <http://www.dawn.com/news/1191422>

86 Global Voices, Pakistan's Sindh Province Proposes Block on Skype, Viber and WhatsApp (4 October 2013) <http://globalvoicesonline.org/2013/10/04/pakistans-sindh-province-proposes-block-on-mobile-communication-apps/>

87 Mehreen Zahra-Malik, Pakistan province orders halt to Skype over security concerns (7 October 2013) <http://www.reuters.com/article/2013/10/07/net-us-pakistan-internet-ban-idUSBRE9920LW20131007> Awaz.tv, Sindh decides to block Skype, Viber, Whatsapp (4 October 2013) http://www.awaztoday.com/News_Sindh-decides-to-block-Skype-Viber-Whatsapp_1_37691_Political-News.aspx

88 Geo.tv, Nisar says not in favour of banning Skype, Viber, Whatsapp, Tango (3 October 2013) <http://www.geo.tv/article-120972-Nisar-says-not-in-favour-of-banning-Skype-Viber-Whatsapp-Tango>

89 Samuel Gibbs, The Guardian, Pakistan bans *Blackberry* services in privacy crackdown (27 July 2015) <http://www.theguardian.com/technology/2015/jul/27/pakistan-bans-Blackberry-messaging-internet-services-privacy-crackdown>

In fact, “crowdsourcing” information and verifying reports can act as an “early warning” system concerning planned or potential attacks. One of the founders of the Kenyan organisation, Ushahidi, a crowd sourcing platform established in the wake of the 2008 post-election violence, said in an interview following the 2015 attacks on Kenya’s Garissa University,

“Most people agree that ordinary citizens should be involved in the prevention and response to terrorism. However, these noble thoughts are ineffective without having tools that enable ordinary citizens to share information quickly and privately, and tools that enable law enforcement agencies to process, verify and escalate that information promptly. Technology does not replace citizens or law enforcement agencies but the right platform can make that relationship a lot more effective.”⁹⁰

After the London riots in 2011, the Government of the United Kingdom contemplated cutting off access to social networks in times of social unrest, due to the assumption that the encrypted instant messaging service on *Blackberry* and *Twitter* was popular among the rioters who used those services to organise some of the rioting.

However, intervention from police forces and testimonies showed that the technology also had a positive effect, with social networking being used to locate looters, dispel rumours, and appeal for calm. As a result, those plans were shelved.

A study of the riots by the British newspaper *The Guardian*, and the *London School of Economics* (LSE) found that although some users were sending police social media messages that incited violence, *Twitter* was also used extensively to organise community clean-up operations in the following days.⁹¹ A recent study by European researchers concluded that censoring/blocking social media sites in times of social unrest could in fact provoke more violent protests.⁹² In Pakistan, outbreaks of violence occurred during network shutdowns, as in a procession during Ashura in 2013.⁹³

In times of a national emergency, fully functioning communication systems are essential. Lack of access to such facilities could have fatal consequences for affected parties. Reports from people affected by suspension of services are becoming more common, such as individuals being caught in the middle of protests and unable to call friends or relatives for help, or being unable to locate or trace their family and

90 Gabriella Mulligan, African Business Magazine, Tech companies step up to fight terror (22 July 2015) <http://africanbusinessmagazine.com/sectors/technology/technology-vs-terrorism/>

91 The London School of Economics and The Guardian, Reading The Riots, 2013 <http://eprints.lse.ac.uk/46297/1/Reading%20the%20riots%28published%29.pdf> pp.30-32

92 Antonio Casilli, Paola Tubaro. Social Media Censorship in Times of Political Unrest- A Social Simulation Experiment with the UK Riots. Bulletin de Methodologie Soci-ologique/Bulletin of Sociological Methodology, SAGE publications, 2012, 115 (1), pp.5-20. <https://hal.archives-ouvertes.fr/hal-00682317/document>

93 The Tribune, Curfew imposed in parts of Rawalpindi following riot at Ashura procession (15 November 2013) <http://tribune.com.pk/story/632366/rawalpindi-clashes-riot-leaves-7-dead-dozens-injured-at-ashura-procession/>

friends. This can cause or contribute to panic.⁹⁴ This concern came up frequently in survey responses. A number of respondents said that they “cannot connect to anyone in an emergency” and were “unable to connect with our family.”

Mobile phones can be enormously useful for victims and affected parties during times of crisis. Police in Indian-administrated Kashmir⁹⁵ have reported that mobile phones have saved the lives of hundreds of people trapped in buildings stormed by suicide attackers. People trapped in buildings during disasters or terrorist attacks have been able to communicate with authorities or their families when lines of communication have remained open. Hostages have often communicated with the police through mobile phones and managed to guide law enforcement to rescue them. On one such occasion, a senior police official told Reuters,

“This is the success story of mobile phones in anti-militancy operations.”⁹⁶

Relying on network shutdowns to prevent terrorist attacks deprives both citizens and law enforcement alike the opportunity to use communication tools in the fight against terrorism. While States are increasingly relying on monitoring and surveillance of communications, which can be controversial and often illegal, there are opportunities for ICTs to be developed as a collective shield against terrorism.

6.2 Restricted Access to Emergency Services

The people of Pakistan are served by several emergency services, but during a network shutdown these services become largely inaccessible as communicating with them is not possible from a mobile phone.⁹⁷ Survey respondents highlighted that during network shutdowns injured people are unable to call via a mobile phone emergency services, such as an ambulance, hospitals, fire and rescue, and emergency services are unable to communicate and locate people. People who need to contact police under different circumstances, such as to report crimes or in the event of an accident or a hostage situation face similar situations.

One respondent legitimately suggested that, “I feel more insecure to be honest, how would I call the police and ambulance?” This also extends to healthcare where survey respondents who work as medical practitioners asserted serious concerns about shutdowns for those they serve. As one put it, “our patients suffer a lot for it.”

94 <http://www.media-alliance.org/article.php?id=2169>

95 India refers to the region as Jammu and Kashmir.

96 Sheikh Mushtaq The China Post (via Reuters) Troops in Kashmir master new weapon: Cell phones (22 May 2006) <http://www.chinapost.com.tw/news/2006/05/22/82690/Troops-in.htm> via Reuters

97 Rescue 1122: Dialling 1122 from any phone connects the caller to the emergency services in Punjab province for fire, rescue and medical services. This includes the major cities of Islamabad and Lahore and serves over 90 million people. 115: Dialling 115 will connect the caller to an ambulance service in Islamabad, Lahore and Faisalabad (Punjab); Karachi (Sindh); Peshawar (North West); Quetta (Balochistan).

Open communication channels are also used in the event of a disaster to disseminate reliable information such as directions to support services, where to get medical help, and what to do next. For example, mobile services could be used to divert people away from already overloaded hospitals, which could otherwise increase the disaster.⁹⁸

6.3 Work

Respondents employed by businesses reported that they were affected by network shutdowns in that they could not receive or make calls, which slowed productivity. Some respondents who are office workers said they were unable to work due to the shutdown of email and Internet connections. If Internet services are also suspended, it is logical to assume that businesses are unable to access data held in the cloud.⁹⁹ Journalists also responded that network shutdowns affected their ability to research or file stories on deadline.

6.4 Education

Student respondents to the survey said that during network disruptions they could not access research materials or access online lessons, and were “unable to complete university assignments and projects”. One student also said that, “notes and slides cannot be downloaded to help with exam revision.”

Other Impacts Of Note:

6.5 Human Rights Defenders

The use of technology for human rights is well documented, and grassroots organisations regularly take advantage of communication tools to organise and campaign for various causes. In addition, ICTs have enabled greater monitoring of situations and documenting events as they unfold. For example, Human Rights Watch (HRW) has detailed the benefits of ICTs for gathering information on human rights violations and drawing attention to situations of actual or potential abuses by “live-tweeting”.¹⁰⁰ As outlined in Section 7, HRW researchers noted that the network shutdown during protests in Kazakhstan had cut off communication with human rights monitors on the ground and had made people “extremely vulnerable”.

98 Gabriella Mulligan, African Business Magazine, Tech companies step up to fight terror (22 July 2015) <http://africanbusinessmagazine.com/sectors/technology/technology-vs-terrorism/>

99 In the simplest terms, cloud computing means accessing files and applications over the Internet, rather than on personal hard drives or servers, via third party services.

100 Ian Levine, Human Rights Watch, Will technology transform the human rights movement? (26 March 2014) <https://www.hrw.org/news/2014/03/26/will-technology-transform-human-rights-movement>

6.6. eServices

Pakistan is keen to invest in its ICT sector, create economic opportunities and improve digital literacy. There are plans for an eGovernance master plan, which aims to use ICTs to deliver efficient and cost-effective public services to citizens as well as increase efficiency, transparency, and accountability in decision-making.¹⁰¹

In addition, millions of people rely on mobile banking. *Telenor Pakistan* was the first network operator in Pakistan to offer mobile banking, when it launched *Easypaisa* in 2009. *Easypaisa* covers 800 cities and serves over 6 million people each month who manage their money via their mobile phones. Almost 600,000 transactions take place nationwide each day, from 65,000 agents or shops nationwide. In 2014, there were 146 million *Easypaisa* transactions worth a total of US\$4 billion. In 2014, almost 2% of Pakistan's GDP moved through *Easypaisa*. This service is unavailable during a network shutdown.

Transmission of health information on mobile phones also cannot take place.¹⁰² A *Telenor Pakistan* and United Nations Children's Fund (UNICEF) initiative is currently under trial to enable people in Pakistan to register births with the aid of their mobile.¹⁰³ Such services would also be unavailable during network shutdowns.

6.7 Economic Impacts

The cost of network shutdowns is difficult to estimate and figures are hard to come by. In 2011, the OECD¹⁰⁴ estimated that the 5-day shutdown in Egypt incurred direct costs of at minimum US \$90 million from lost revenues due to blocked telecommunications and Internet services, which account for around US \$18 million per day. However, the actual figure is possibly much higher, as the study did not take into account secondary economic impacts, which resulted in loss of business from other sectors. If the shutdown had continued every day for a year, it would cost Egypt roughly 3-4% of GDP.

Another indication of the economic costs is reflected by the case involving former Egyptian President Hosni Mubarak, former prime minister Ahmed Nazif and former minister of Interior Habib Al-Adly, who are currently appealing a collective fine of EGP 540m (about US\$ 69 million), as compensation for operators and Internet companies'

101 More Magazine, Pakistan, IT Ministry makes master plan for E-governance (3 December 2014) <http://www.moremag.pk/2014/12/03/it-ministry-makes-master-plan-for-e-governance/>

102 BBC Media Action, Still Left in the Dark? Policy Briefing no.6 (March 2012) http://downloads.bbc.co.uk/mediaaction/policybriefing/bbc_media_action_still_left_in_the_dark_policy_briefing.pdf

103 See: http://www.unicef.org/pakistan/media_8732.htm and <http://www.Telenor.com/media/articles/2014/providing-proof-of-identity-in-pakistan/>

104 OECD, The economic impact of shutting down Internet and mobile phone services in Egypt (4 February 2011) <http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm>

financial losses incurred during the 2011 shutdown.¹⁰⁵

Shutdowns have caused losses of tax revenue to the Government of Pakistan. It was reported that shutdowns during the Eid (a major national holiday) in 2012 caused an estimated loss of 507 million Pakistani rupees (PKR) (US\$ 49 million) in taxes from the mobile operators to the exchequer.¹⁰⁶ Shutdowns in November 2012 during Ashura, a religious day in the Islamic calendar, are estimated to have caused PKR 500 million (US\$ 49.02 million) of losses to the Government in tax revenue from cellular subscribers.¹⁰⁷

The 1996 Pakistan Telecommunications (Re-organisation) Act states that network providers would be compensated for the losses they may have incurred as a result of action taken under Section 54, which has been used to justify shutdowns (see Section 6):

“Provided that the Federal Government may compensate any licensee whose facilities or services are affected by any action under this sub-section.”

Compensation to operators is an issue that has not been resolved in Pakistan. An online tech publication, Propakistani.com, reported that telecom companies lost PKR 2.6 billion (US\$ 25 million) in the shutdown on Eid in August 2012.¹⁰⁸ In February 2013, *Telenor Pakistan* requested compensation of PKR 163 million (US\$ 1.59 million) for losses incurred because of shutdowns in 2012 and in January 2013 along with other telecom operators, which the company has not received.¹⁰⁹

6.8 People’s opinions of network shutdowns

As part of the survey, respondents were asked their personal opinion of how they felt during network shutdowns. The responses received were diverse and range from expressions of frustration to anger and isolation. Notably, respondents felt themselves thrown back in time to “being back in the 90s” or even further that disconnection from mobile phone networks is “probably what the Stone Age felt like.”

105 Amira El-Fekki, Daily News Egypt, Court to rule on Mubarak’s appeal in telecommunications case on 24 October (4 July 2015) <http://www.dailynewsegypt.com/2015/07/04/court-to-rule-on-mubaraks-appeal-in-telecommunications-case-on-24-october/>

106 Aamir Attaa, Propakistani, Mobile Companies Lost PKR 2.6 Billion On Eid Day Due to Cellular Shut Down (23 August 2012) <http://propakistani.pk/2012/08/23/mobile-companies-lost-pkr-2-6-billion-on-eid-day-due-to-cellular-shut-down/>

107 Aamir Attaa, Propakistani, Pakistan Telecom Saw Two Darkest Days of Its History (26 November 2012) <http://propakistani.pk/2012/11/26/pakistan-telecom-darkest-days-history/>

108 Aamir Attaa Mobile Companies Lost PKR 2.6 Billion On Eid Day Due to Cellular Shut Down (23 August 2012) <http://propakistani.pk/2012/08/23/mobile-companies-lost-pkr-2-6-billion-on-eid-day-due-to-cellular-shut-down/>

109 Tribune, *Telenor* asks govt to pay Rs163m for forced cellular suspension losses: Report (11 February 2013) <http://tribune.com.pk/story/505711/Telenor-asks-govt-to-pay-rs163m-for-forced-cellular-suspension-losses-report/>

The main emotions associated with disconnection included isolation, embarrassment and just plain boredom. While some respondents preferred to simplify their experience as simply “absolutely rubbish” others responded more poetically seeing the disconnection of communications “like a sea without water.” Some respondents did report feeling “relaxed” and “happy” during periods of shutdowns.

These responses are also indicative of a more general trend among respondents who suggested they would themselves not take the same measures if they were in power. When asked whether they would be willing to disconnect communications services, the vast majority of respondents (72%) said no.

A large portion of survey respondents (69%) said they did not feel safer when communications are shutdown for security reasons. A frequent response was general scepticism of the impact of network shutdowns in improving security. Some respondents suggested disconnecting mobile phone networks “has no effect on security” or simply that “it doesn’t make any sense.” Equally, it is argued that, “terrorists have other ways [to communicate] e.g. satellite phones”. This is not to say respondents are opposed to security measures per se, but that they are sceptical of the disconnection’s efficacy in achieving security. One respondent argued that disconnecting mobile phone networks “is not a safety measure. Actually, true and relevant safety measures are desired.”

The reflections from respondents in the survey indicate that there is scope for the Government of Pakistan to engage with citizens on the issue and consider soliciting public views on the impacts of network shutdowns, with the aim of improving communication and transparency. Furthermore, as outlined earlier, there is scope to use ICTs in improving the exchange of information between citizens and law enforcement, to help build early warning systems, and improve prevention and response.

7. Other Examples of the Network Shutdown Debate

It is not unusual and sometimes necessary for a government to implement legislation that can control communication networks in an emergency. But the law is often ambiguous and the process or chain of command for a governmental request to be implemented is often unclear. Security and terrorism are politically sensitive subjects and it is possible that there may be little political will to consider policy alternatives.

The examples in this section provide brief summary case studies from countries in which there has been a dialogue between the government and other actors with the aim of finding alternatives to network disconnection or clarifying laws where needed.

Egypt is a prominent example due to the country-wide shutdown ordered by former President Hosni Mubarak in 2011, which brought the issue of network shutdowns to global attention. Northern Ireland, with its history of suffering terrorist attacks, offers some parallels with Pakistan. The example of Kazakhstan demonstrates that companies can have a positive impact when entering into dialogue with the government.

7.1 Egypt

The disruption of national mobile and Internet services in Egypt by former President Hosni Mubarak during the protests of 2011 brought the issue of network shutdowns to national and international attention. This shutdown was viewed as a desperate attempt by the Government to retain power. It was ultimately ineffective because it brought more people onto the streets calling for change and eventually led to the President's resignation.

The Egyptian Telecommunication Regulation Law (2003), in particular Article 67 (see box overleaf) was invoked as justification for the shutdown. That law was originally intended to address situations such as natural disasters when authorities needed to control and direct the flow of communication traffic and prioritise emergency service communication. Article 67 did not contain any provision for blocking communications.

Amendments to this Article were drafted in 2013 and published in Egypt's National ICT Strategy (2012-2017)¹¹⁰ but were not implemented, in part due to a second revolution in 2013 which led to the army ousting the elected President Morsi and installing an interim government. Nevertheless, a comparison of the original and amended text is useful.

110 Egypt Ministry of Communication and Information Technology (MCIT) National ICT Strategy (2012-2017) Towards a Digital Society and Knowledge Based Economy pp 32-33
<http://mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf>

Comparison of Article 67 text:

Original version:

"The competent state authorities shall have the power to subject to their administration the telecommunications services and networks of any operator or service provider, and those working in the operation and maintenance of these services and networks, in case of natural or environmental disaster or during periods of declared general mobilization in accordance with the provisions of Law No. 87 of 1960 concerning these and other cases related to national security."

Amended version of Article 67

"In the case of a declaration of general mobilization as provided for in Article 65, the Cabinet shall issue a resolution activating the plan referred to in Article 65. The resolution shall define when implementation of the plan is to begin and the duration of its application. In all cases, it shall be prohibited to disconnect telecommunications services or to stop their operation entirely or partially, except in the case that a written decision has been issued by the President of the Republic following a proposal to do so by the Cabinet.

In this case, the President of the Republic shall, within 15 days of issuing such a decision, submit a detailed report to the People's Assembly explaining the reasons for adoption of the measure. In the event that the People's Assembly is not in session, the submission shall be made in the first session held. In all cases, it shall not be permissible to disrupt or stop relief and emergency services."

The amended text prohibited network disconnection entirely, except on a written decision by the President (rather than unspecified "competent authorities"), following approval by the Cabinet. Following any disconnection, a written report must be presented to the wider People's Assembly to explain the decision. While this measure could add some transparency and accountability to the process, it is not stated clearly what should be contained in the written report, nor does it specify any limits on the length of the shutdown or the geographic spread of the area that would be affected. It also says disruption of emergency services is not permissible, but does not specify what measures should be taken to ensure that.

In an analysis of the original Telecommunications Law text, ARTICLE 19 and the Egyptian organization, the Association for Freedom of Thought and Expression (AFTE) recommended that:

- Cutting off access to the Internet of for an entire population should be abolished and prohibited;

- It should be clarified which public authorities are authorised to take control of communications networks in an emergency.
- Their powers in times of emergency should be, “redefined and limited to the least restrictive measure required to face genuine perils to national security.”
- “The [Telecommunications] Law should ensure that any disconnection of a specific service only happens after a prior judicial approval and for limited, specific circumstances allowed under international law”¹¹¹

7.2 Ireland

In May 2013, the Government of the Republic of Ireland warned that service providers may be asked to shutdown mobile networks during the G8 Summit to be held in Northern Ireland the following month.¹¹² Northern Ireland’s police warned that dissident republicans were “likely” to launch a terrorist attack.¹¹³ The summit was to be held at a golf resort in Fermanagh, a remote part of Northern Ireland and 11 miles north of the border with the Irish Republic. Some 8,000 extra police officers were reportedly called for duty, making this the biggest police operation in Northern Ireland’s history.¹¹⁴

Although the G8 summit was to be held in Northern Ireland, the Irish Republic’s justice minister brought in legislation¹¹⁵ to allow Gardaí (the Irish Republic’s police force) to order telecom companies in the Irish Republic to shut off signals to prevent terrorists from using mobile phones to detonate bombs. The legislation stated that:

- Only the Minister for Justice and Equality has the power to implement;
- Only a member of the police above a certain rank can request in writing;
- Only in exceptional cases can requests be made orally, as long as it is confirmed in writing shortly after;

111 Article 19 and AFTE, Egypt: Legal Analysis of Telecommunications Law (2015) <http://www.article19.org/resources.php/resource/37966/en/egypt:-legal-analysis-of-telecommunications-law>

112 Fionnan Sheahan and Tom Brady, The Irish Independent, Gardaí will get powers to block phone signals for G8 (16 May 2013) <http://www.independent.ie/business/irish/gardai-will-get-powers-to-block-phone-signals-for-g8-29270951.html>

113 Belfast Telegraph, Mobile phones could be cut for G8 summit amid terrorist bomb fears (15 May 2013) <http://www.belfasttelegraph.co.uk/news/local-national/republic-of-ireland/mobile-phones-could-be-cut-for-g8-summit-amid-terrorist-bomb-fears-29270258.html>

114 Haroon Siddique, The Guardian, G8 summit sparks biggest police operation in Northern Ireland’s history (20 May 2013) <http://www.theguardian.com/world/2013/may/20/g8-summit-police-northern-ireland-fermanagh>

115 The Journal (Ireland) Plan to shut down mobile phones in G8 terror event signed into law (13 June 2013) <http://www.thejournal.ie/g8-mobile-phone-shutdown-law-949539-Jun2013/>
Ireland Criminal Justice Act 2013 (Part 3)
<http://www.irishstatutebook.ie/pdf/2013/en.act.2013.0019.pdf>

- Any proposed disruption is subject to strict time limits and must be demonstrated to be of direct material necessity;
- Ministers can refuse requests.

However, the legislation provided the minister with the right to refuse to disclose information about the order. For this reason, the lack of transparency, it is difficult to determine if these powers were actually enforced during the G8 summit. This highlights the secretive nature of network shutdowns globally, and that even if a process is in place, politicians may be given the right to refuse to disclose information about the order, including if it actually happened.

Commenting on the proposed legislation, *The Irish Council for Civil Liberties* on the whole approved the legislation, but suggested areas for improvement¹¹⁶:

- The public must have access to emergency services, and network providers must be obliged to ensure access to continued services;
- In the interest of proportionality, geographical limitations should be explicitly mentioned;
- The legislation should be subject to review by Parliament.

These comments, combined with those submitted by ARTICLE 19 and AFTE in Egypt, help to build a common approach to how network shutdowns are requested, authorised and reviewed, which has helped inform our recommendations on the key characteristics of a framework around network shutdown (see next section).

7.3 Kazakhstan

In 2011, a peaceful strike by oil workers in the town of Zhanaozen became violent when police intervened, resulting in multiple deaths and injuries. The Government of Kazakhstan declared a state of emergency and ordered the operator Tele2 Kazakhstan, (majority owned by Swedish telecommunications operator Tele2,) to suspend services in the city for five days.¹¹⁷ Human rights organisations reported that they were unable to contact colleagues who were monitoring the situation, and according to one *Human Rights Watch* researcher:

“Without a means to communicate with the outside world, people in Zhanaozen are

116 Irish Council for Civil Liberties (ICCL) Mobile Phone Shutdown Powers “Proportionate” says Rights Watchdog (22 May 2013) <http://www.iccl.ie/news/2013/05/22/mobile-phone-shutdown-powers-%E2%80%9Cproportionate%E2%80%9D-says-rights-watchdog-.html>

117 Tele2, Corporate Responsibility Report (2011), p14
http://www.tele2.com/Documents/documents/Tele2_CR_2011_120416_low.pdf

extremely vulnerable.”¹¹⁸

Following this incident, *Tele2* engaged the Government in dialogue, spoke publicly about the challenges, and advocated for clearer legal frameworks. The Kazakh telecommunications law was recently amended to include limiting measures such as restricting shutdowns to three hours.¹¹⁹

These three examples demonstrate different kinds of engagement with the government from civil society or an operator on the issue of network shutdowns. Missing are examples where operators and civil society have joined forces in government engagement. Also missing are examples where companies offering Internet-based services such as social networking sites (known as “over the top services) have publicly entered the debate, as their services are disrupted or inaccessible during some network shutdowns.

According to the *UN Guiding Principles on Business and Human Rights*, businesses are advised to conduct stakeholder engagement, designed to build relationships and mutual understanding between a company and its stakeholders. Often, stakeholder engagement can be tense and difficult, for example if a mine or oil pipeline is being built over community land. But in the ICT sector, a different kind of stakeholder engagement and relationship is emerging. In the case of network disconnection, both the company, whether an operator or “over the top”, and local civil society have the same aim: to reduce the frequency of network shutdowns. This alignment of goals has the potential to produce real and long-lasting action that will ultimately improve the enjoyment of human rights.

118 Human Rights Watch Kazakhstan: Investigate Violence in Oil-Rich Western Region Communications Shut Down after Clashes Near Long-Peaceful Labor Protest (17 December 2011) <http://www.hrw.org/news/2011/12/17/kazakhstan-investigate-violence-oil-rich-western-region>

119 Tele2, New law amendments and reorganization of the Government of Kazakhstan (14 August 2014) <http://www.tele2.com/Our-Responsibility/archive/sustainability-in-focus/in-focus/new-law-amendments-and-reorganization-of-the-government-of-kazakhstan/>

Conclusion

The spread of the use of ICTs has been rapid because of innovations and decreasing costs in mobile technology, allowing more remote and rural parts of the world to connect, in some cases sidestepping landlines altogether. The importance of communications is recognised internationally as having a profoundly positive effect on the enjoyment of both civil and political rights and economic, social and cultural rights, in particular the right to freedom of expression, freedom of assembly, the right to education as well as the right to work.¹²⁰

Network shutdowns are usually justified on security grounds, and the counter-argument is often framed around the impact on freedom of expression. However, the impacts of network shutdowns can have far-reaching, adverse economic and social implications and could affect future economic growth; furthermore, they can actually endanger the very right it seeks to preserve, the right to life, by denying users the ability to connect to family, health and emergency services.

Although the Government of Pakistan faces grave internal threats and serious security situations, concerns that network shutdowns are becoming the go-to tool are growing. More effective strategies to prevent attacks are required. Blunt network shutdowns cannot offer a long-term solution for any country in combatting terrorism or other security threats. ICTs are used by citizens and terrorists alike, but without access to ICTs, law enforcement lose the opportunity to use communications for the purpose of fighting terrorism, and to disseminate important information to move people to safety, or to calm a concerned population. Advances in technology such as “crowdsourcing” can help develop early warning systems and cement co-operation between citizens and law enforcement to create a collective shield against terrorism.

Globally, network shutdowns impacting an entire country are extremely rare. Usually, smaller geographical areas are targeted, but this could be made up of several cities simultaneously and reach across many different services.

Telenor Pakistan has demonstrated its willingness to engage with the Government of Pakistan on the issue of network shutdowns and says it will continue to do so. It appears that the engagement is having some impact, as the process has become more streamlined and shutdowns appear to be more targeted. Shutdowns have also reduced in the past few years.

For example, network shutdowns took place during the Chinese Premier’s visit to Pakistan in 2013¹²¹ but during a visit in 2015, *Telenor Pakistan* confirmed no shutdown was implemented. This demonstrates that while the issue is sensitive, positive change can be achieved by opening a dialogue with governments. However, while the frequency of mobile shutdowns has been reduced in Pakistan, the scope of

120 See UN Resolution A/HRC/20/L.13 The Promotion, Protection and Enjoyment of Human Rights on the Internet, 29 June 2012

<http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>

121 Nick Macfie, China’s Li Offers to Help End Pakistan Energy Crisis Reuters, (22nd May 2013)

<http://www.reuters.com/article/2013/05/22/us-pakistan-china-idUSBRE94L06G20130522>

shutdowns is increasing to incorporate Internet based messaging services such as *Skype* and *Whatsapp*. Examples from other countries suggest this is a growing trend.

From the survey undertaken for this report during the shutdown of 23 March 2015, it is clear there is widespread confusion around the issue of network shutdowns in Pakistan, and a general question about the effectiveness of shutdowns in combating terrorism. Outside of Pakistan, efforts to engage governments to slow the trend of network shutdowns have resulted in mixed success. There is not yet a known example where companies and civil society have joined forces, and there appears to be a lack of engagement on the part of “over the top” companies, whose services are also impacted by network disruptions, to publicly enter the debate. On the whole, confusion reigns around the issue; many countries’ legislation governing network shutdowns remains vague and related processes lack transparency.

As network shutdowns are a relatively frequent occurrence in Pakistan, and there has been some engagement between the government and *Telenor Pakistan* to reduce the frequency, the analysis of network shutdowns in Pakistan can help inform broader recommendations for other countries. In the short term, a clearer framework and process around accountability and transparency of network shutdowns is needed in many countries. The process for requesting network shutdowns should include the following key characteristics:

- Network shutdowns should only be invoked in cases of real and imminent threats to national security or national emergencies, and requests should specify reason for such disruptions.
- National law should be in place to regulate network shutdowns including which bodies or agencies are authorised to make requests.
- Shutdown requests should be approved or authorised by the highest level of the government.
- Clear request processes should be established, with a limited number of actors in authorised law enforcement agencies allowed to make requests, and designated individuals within operators to receive such requests.
- All shutdown requests to network operators should be made in writing. The request should specify the duration and geographical reach of the shutdown as well as the reason, and demonstrating direct material necessity. Shutdowns should be limited in duration and geographical area and proportionate to the perceived level of risk.
- Whenever possible, the public should be informed of network shutdowns, including their duration, geography and services affected.
- All network disruptions should be logged/recorded, and the government should publish annually a list of all shutdowns.
- Access to and communication with emergency services should be guaranteed to

ANNEX A: Timeline of Network Shutdowns in Pakistan (2012-2015)

Data provided by *Bytes for All (2012-2015)*¹²²

2012	Event
19th August 2012	Eid-ul Fitr is a celebration that marks the end of fasting month Ramadan. The Government of Pakistan suspended cell phone services in at least four major cities in the wake of intelligence reports of possible terror attack on the day.
21st September 2012	Ishq e Rasool , Love for Prophet Muhammad (PBUH) Day, was observed throughout Pakistan condemning the film "The Innocence of Muslims". At least 20 people were killed and over 200 wounded in protests across Pakistan.
16th November 2012	First day of Muharram , the first month of the Islamic calendar. Mobile services suspended amid fear of possible terror attacks.
23rd November 2012	Ashura . The Day of Ashura is on the tenth day of Muharram in the Islamic calendar and on that day the martyrdom of Hussain Ibn Ali is observed. Government bans mobile services to avoid any act of violence and terrorism in the country. Government also bans riding motorcycles.
14th August 2012	Independence Day . Security concerns.
23rd March 2012	Pakistan Day is a national holiday in Pakistan to commemorate the Lahore Resolution of 1940. Mobile services were banned due to potential threats of terrorism in the country.

2013	Event
3rd January 2013	Imam Hussain Chelum Chelum day is observed to mark the 40th day after martyrdom of Imam Hussain, the grandson of Prophet Muhammad (PBUH). Mobile services blocked due to possible terror attacks.
13th January 2013	Tahir ul Qadri Long March Pakistani religious scholar and head of Pakistan Awami Tehreek (PAT) Muhammad Tahir-ul-Qadri organised a long march to protest government's corruption. The march moved from Lahore to Islamabad and stayed in Blue Area, Islamabad between 14 and 17 January 2013. Cellular services were blocked on the route of long march throughout its way to Islamabad.
23rd March 2013	Imran Khan Jalsa A major political party Pakistan Tehreek-e-Insaf in Lahore carried out a jalsa [public gathering]. Mobile services around the venue were blocked due to possible terror attack.
7th May 2013	Ahlesunnat Wal Jamaat (ASWJ) observed a strike against the 'Gilgit-Baltistan Empowerment and Self Rule Order 2009'. The decision to suspend cellular services taken as a precautionary measure to avoid any terror incident during the day.
23rd May 2013	Chinese Premier's visit to Islamabad. Government suspended cellular services in Rawalpindi and Islamabad when Chinese Premier Li Keqiang visited.
31st July 2013	Youm e Ali. The martyrdom anniversary of Hazrat Ali ibn Abi Talib (A.S) is observed on this day. Government of Pakistan banned mobile services in few cities in the wake of terror threats.

2013	Event
14th November 2013	Ashura. The Day of Ashura is on the tenth day of Muharram in the Islamic calendar and the martyrdom of Hussain Ibn Ali is observed. Government ban mobile services to avoid any act of violence and terrorism in the country.
24th November 2013	Ashura
24th December 2013	Chelum of Imam Hussain is observed to mark the 40th day after martyrdom of Imam Hussein (PBUH), the grandson of Prophet Muhammad (PBUH). Government banned mobile services in various parts of country due to possible terror threat.

2014	Event
14th January 2014	Eid Milad un Nabi is the observed on 12th day of Rabi' al-awwal to mark birth of Prophet Muhammad (PBUH). Government banned cellular services in different parts of the country due to security threats.
23rd June 2014	Dr. Tahir-ul-Qadri [Chairman of Pakistan Awami Tehreek (PAT)] was flying in from Dubai to Rawalpindi. Initially some areas if Rawalpindi were blocked and then, when his plane was diverted to Lahore, the area from Lahore airport to his residence were blocked.
20th July 2014	Youm-E-Ali The martyrdom anniversary of Hazrat Ali ibn Abi Talib (A.S) is observed on this day. Government banned mobile services in few cities in the wake of terror threats.
8th - 14th August 2014	Inqilaab March Inqilaab March was an ongoing public protest throughout August, organised by the political party Pakistan Awami Tehreek (PAT). The protesters demand the resignation of Prime Minister Nawaz Sharif.
23rd - 27th August 2014	As above. Shutdown due to security reasons.
3rd - 4th November 2014	Ashura. The Day of Ashura is on the tenth day of Muharram in the Islamic calendar and marks a very important day as martyrdom of Hussain Ibn Ali is observed. Government ban mobile services to avoid any act of violence and terrorism in the country.

2015	Event
23rd March 2015	Pakistan Day Parade
14th August 2015	Independence Day



Institute for
Human Rights and Business

Shaping Policy • Advancing Practice • Strengthening Accountability

Institute for Human Rights and Business
34b York Way
London N1 9AB
UK

Phone: (+44) 203-411-4333
Email: info@IHRB.org