CENTRAL EUROPEAN UNIVERSITY

SOUTH ASIAN COMMUNICATION SURVEILLANCE AND RIGHT TO PRIVACY IN DIGITAL AGE

by Md Rezaur Rahman

LL.M. SHORT THESIS
COURSE: Freedom of Expression: Comparative Law perspective
PROFESSOR: Sejal Parmar, PhD
Central European University
1051 Budapest, Nador utca 9.
Hungary

Abstract

South Asian constitutional democracy and human rights movements have suffered severe setbacks since inception of their statehood, particularly the decade after the militant attacks in the United States (US) on September 11, 2001. In the wake of several terrorist attacks, the South Asian governments and private sector sponsored surveillance measures have been newly introduced by many authoritarian and repressive governments like Bangladesh, India and Pakistan and arguably have taken the opportunity to legitimize their repressive actions and re-justify existing laws in the defense of national security exception. Therefore, state and private sector sponsored 'communication surveillance' is particularly stimulating case study for South Asian human rights and online community because of pervasive nature of communication surveillance. The primary objective of this research is to explore and analyze the political, social, legal or juridical and administrative environment of communication surveillance in Bangladesh, India and Pakistan. By doing so, this research investigates emerging South Asian communication landscape and state sponsored crimes against digital rights and internet freedoms, analyze major international human rights frameworks and problematic national legal and administrative regimes of communication surveillance. It also broadly explores the key trends, nature and modalities of communication surveillance technologies and challenges for human rights defenders and online activists. The focus of this research largely comparative and contemporary in nature.

Table of Contents

Thesis Declaration

I, Md Rezaur Rahman, declare that this thesis, submitted partially in fulfillment of the requirements for the degree of Master of Laws (LLM) in Comparative Constitutional Law at Central European University, is wholly my own work unless otherwise referred or acknowledged. The document has not been submitted for qualifications at any other academic institutions.

Md Rezaur Rahman
April 2016

Acknowledgement

Over the years, I have been greatly benefited from my teachers and friends at University of Dhaka, Sungkonghoe University, University of Sydney, Lund University and Central European University for the fine tuning of my knowledge, though process and understanding of different issues beyond borderlines. My special thanks goes to my beloved friends Ishraq Abdel Rahman and Purabee Permita Bose for their patient love, affection and valuable support apart from their own tough and tight schedule.

Finally, and most importantly, my heartfelt thanks go to my loving parents for being the real backbone and helping me to achieve my academic excellence.

Abbreviations

BJP	Bharatiya Janta Party
BAL	Bangladesh Awami League
BTRC	Bangladesh Telecommunication Regulation Commision
BDIX	Bangladesh Internet Exchange
BTRA	Bangladesh Telecommunication Regulation Act
BTA	Bangladesh Telecommunication Act
BD-CSIRT	Bangladesh Computer Security Incidence Response Team
BWA	Broadband Wireless Access
COE	Common Operations Environment
CMS	Central Monitoring System
DSL	Digital Subscriber Line
DOT	Department of Telecommunications
DeiTY	Department of Electronics and Information Technology
FTA	Fair Trial Act
GCHQ	Government Communications Headquarters
HRD	Human Rights Defenders
HRC	Human Rights Council
ICT	Information and Communication Technology
ICCPR	International Covenant on Civil and Political Rights
IMSI	International Mobile Subscriber Identity
ISP	Internet Service Providers
ITU	International Telecommunication Union

ISA	Inter-Services Intelligence Agency
IPT	Internet Protocol Telephony
INGO	International Non-Governmental Organizations
IRINN	Indian Registry for Internet Names and Numbers
LIM	Lawful Interceptions and Monitoring
MTT	Ministry of Technology and Telecommunication
MICT	Ministry of Communication and Technology
NHRC	National Human Rights Commission
NETRA	Network Traffic Analysis System
NMC	National Monitoring Centre
OHCHR	Office of the United Nations High Commission for Human Rights
PPP	Public and Private Partnerships
PASHA	Pakistan Software Houses Association
PIX	Pakistan Internet Exchange
PI	Privacy International
PTA	Pakistan Telecommunication Authority
PMO	Prime Minister Office
RAB	Rapid Action Battalion
TRAI	Telecom Regulatory of India
UDHR	Universal Declaration of Human Rights
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Council
WAMS	Wide-area and Multiple-sensor

Introduction and Conceptual Framework of the Research

Brief Description of the Issues to Address

South Asian constitutional democracy and human rights movements have suffered severe setbacks since inception of their statehood, particularly, the decade after the militant attacks in the United States (US) on September 11, 2001.[1] In the wake of 9/11, the government and private sector sponsored surveillance measures have been newly introduced by many authoritarian and repressive governments,[2] and arguably have taken the opportunity to legitimize their repressive actions and re-justify existing laws in the name of fighting 'terror'.[3] Legislations violating human rights and encroaching into the privacy of citizens were freely passed in many countries[4] and conferred wide powers to governments and agencies to detain online activists for sustained periods,[5] while denying their right to have free and fair trials, and imposing greater surveillance powers 'to investigate of any offense'.[6]

[1] Fergal Davis, Nicola McGarrity, and George Williams, eds., *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, 2013).

[2] "Since 1997 the UK-based Privacy International in cooperation with the US-based Electronic Privacy Information Center have conducted annual surveys in order to assess how much privacy protection nations' populations have from both corporative and government surveillance". In 2007, Privacy International also conducted a summary on 47 countries around the world about the state of privacy in post 9/11 scenarios. See details Privacy International, "The 2007 International Privacy Ranking," Survey report (United Kingdom: Privacy International, July 2007), https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings. See also at "Reports | Privacy International," accessed March 26, 2016, https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings.

[3] Reporter Without Border, "The Enemies of Internet," NGO Websites, *The Enemies of Internet*, (July 2013), http://surveillance.rsf.org/en/.

[4] Last seven years, the United States department of Bureau of Democracy. Human Rights and Labor affiliated agency Freedom House has produced six editions of Internet Freedom reports which are named Freedom on the Net. In 2015, it has surveyed sixty-five countries on surveillance and censorship including in Bangladesh, India and Pakistan. See details Sanja Kelly, et al., "Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015," Human Rights Report (New York: Freedom House, October 2015), https://freedomhouse.org/report/freedom-net/freedom-net-2015.

[5] For example, in India, a young-male resident of Malda district arrested for a derogatory comment on Facebook against Chief Minister and trial court remanded him to 14 days' judicial custody. For details, see "Youth Arrested for Making Anti-Mamata Remark on Facebook - Times of India," *The Times of India*, accessed March 27, 2016, http://timesofindia.indiatimes.com/city/kolkata/Youth-arrested-for-making-anti-Mamata-remark-on-Facebook/articleshow/44828692.cms.

[6] For Example, see details analysis of Section 2 of Fair Trial Act, 2013 at Chapter II.

A decade after September 11, 2001, three years from 2013 to 2015 have been very problematic and distressful years for South Asian online community for several reasons. These years marked as 'problematic' because of a trapping situation between murders and repression of bloggers community in Bangladesh,[7] violations of 'net neutrality principles'[8] by the Indian Internet Service Providers (ISPs) and mobile service operators to their users and customers',[9] and 'the revelation of massive surveillance programs and spyware software installment against netizens in Pakistan'.[10] It is also evident that the vibrant online community in South Asia faced threats of long term jail sentences and judicial persecutions by state actors and states appeared more inclined than ever before to deploy surveillance technology and censorship gadgets over the information and communication technologies to curb the digital activism in the defense of national security exception.[11] Therefore, state and private sector sponsored 'communication surveillance'[12] is particularly stimulating case study for South Asian online community because of pervasive nature of communication surveillance. The epidemic nature of surveillance technologies and limited opportunity of anonymity on the internet have the nascent to change constitutional values of life, liberty and privacy and gradually changing, and reshaping the relationships between governments and netizens in South Asia.

[7] Charles Parkinson, "Trapped between Murder and Repression: Life as an Atheist Blogger in Bangladesh," *VICE News*, December 9, 2015, Online edition, sec. Asia Pacific Section, https://news.vice.com/article/trapped-between-murder-and-repression-life-as-an-atheist-blogger-in-bangladesh.

[8] For details about the Net Neutrality principle Tim Wu, "Network Neutrality, Broadband Discrimination," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, June 5, 2003), http://papers.ssrn.com/abstract=388863.

[9] EDRi, "India: Free Basics Violates Principles of a Neutral Internet," NGO Report (Belgium: EDRI, January 13, 2016), https://edri.org/india-free-basics-violates-principles-of-a-neutral-internet/.

[10] Jahanzaib Haque | Atika Rehman, "Hacking Team Hacked: The Pakistan Connection, and India's Expansion Plan," *Online Publication*, July 28, 2015, online edition, sec. op-ed, http://www.dawn.com/news/1196767.

[11] See details in chapter II

[12] Communication surveillance "includes not only the actual reading of private communications by another human being, but also the full range of monitoring, interception, collection, analysis, use, preservation and retention of, interference with or access to information that includes reflects or arises from a person's communications in the past, present or future", See details at United Nations Human Rights Council, "International Principles on the Application of Human Rights Law to Communications Surveillance" Electronic Frontier Foundation and Article 19, May 28, 2014), https://en.necessaryandproportionate.org/LegalAnalysis/communications-surveillance.

Scope and Objective of the Research

Across South Asia, the revelation of targeted and mass communication surveillance shattered political, social, legal scientists or even to the human rights defenders, journalists and bloggers. The central theme of this research is to broaden a debate towards communication surveillance and right to online privacy in South Asia by using a Human Rights Based Approach (HRBA).[13] Although this research recognizes that the scope of research is quite broad; therefore, the primary objective of this research is to explore and analyze the political, social, legal or juridical and administrative environment of communication surveillance in Bangladesh, India and Pakistan. By doing so, this research investigates emerging South Asian communication landscapes and state sponsored crimes against digital rights and internet freedoms, analyze major international human rights frameworks and problematic national legal and administrative regimes. It also explores broadly the key trends, nature, and modalities of communication surveillance technologies, recent development of international human rights frameworks, and challenges for human rights defenders and online activists. The focus of this research largely comparative and contemporary in nature. It is important to note that it does not set out to be exhaustive or to cover every alleged incidents of digital rights violations against 'Human Rights Defenders (HRD)[14] journalists[15], bloggers[16] by state apparatus. In short, this research delves into

[13] David Lyon, *Surveillance After Snowden* (John Wiley & Sons, 2015).

[14] See details at Article 1 of United Nations General Assembly adopted a Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms. In addition, European Union Guidelines on Human Rights Defenders-2008 also adopted a working definition. For details, United Nations Human Rights Council, "The Declaration on the Right of Individuals, Groups of Power in Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms" (United Nation), accessed March 27, 2016, See details at http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Defender.aspx

[15] "The core international and regional human rights treaties do not distinguish journalist as category… and their rights protection mechanisms still evolving under International law ", See details Sejal Parmer, "Towards an Effective Framework of Protection for the Work of Journalists and an End to Impunity," 2014, available at http://dare.uva.nl/record/1/448153.

[16] Like the term journalist, Blogger term is an essentially contested term and still evolving as a category under human rights and humanitarian law. For details Jane B. Singer, "The Political J-Blogger 'Normalizing' a New Media Form to Fit Old Norms and Practices," *Journalism* 6, no. 2 (May 1, 2005): 173–98, doi:10.1177/1464884905051009.

broader digital rights scenario analysis in relation to communication surveillance and right to privacy in the digital age of Bangladesh, India and Pakistan.

Research Methods and Methodology

A comparative and qualitative study encourages various methods and methodologies to gather or produce data. Largely, this comparative and qualitative research exercises 'historical and analytical approach'[17] to understand a contemporary 'problem'. In the qualitative research, using secondary materials is an established practice as Irwin and Winterton argues 'there is drive towards extending data reuse and analysis'.[18] Hence, this research deeply and extensively relies on secondary sources, literatures and organizational knowledge's to understand the changing communication landscape of South Asia and the reality of the South Asian digital rights and internet freedoms. The secondary sources include "books, research reports, academic articles, periodicals, magazines, newspapers, testimonies including the judicial verdicts, human rights defenders' observations and so on".[19] However, this paper also focuses on primary sources and materials, such as statute and case laws, to understand and analyze national and international legal regime of right to privacy and freedom of expression and their correlation in a digital context.

Limitation of the Study

There are number of shortcoming of this research, first, there is very little systematic, comparative and comprehensive research has been conducted before in the field of communication surveillance in South Asian context, in short almost non-exist. Indeed, it is an unexplored spectrum, perhaps, because of lack of conceptual clarity, possible physical and psychological risk of research actions, and also the

[17] Wodak, Ruth, and Michael Meyer. *Methods of Critical Discourse Analysis*. SAGE, 2001.

[18] Sarah Irwin, "Data Analysis and Interpretation: Emergent Issues in Linking Qualitative and Quantitative Evidence," in *Handbook of Emergent Methods*, ed. S. N. Hesse-Biber and P. Leavy (New York, NY, US: Guilford Press, 2008), 415–540.

[19] Md Rezaur Rahman, "Human Rights Defenders at Risk: The Case of 10th Parliamentary Election -2014 in Bangladesh" (Academic Thesis, University of Sydney, 2014).

discourse itself is in 'contemporary in nature'. However, it is unfair not to acknowledge certain ground breaking research by international organizations like Privacy International, Article 19 and national organizations such as *Odhikar* and Law Life Culture in Bangladesh, Center for Internet and Society in India, and Bytes for All in Pakistan, however, there is a need to conduct a comprehensive research in a comparative perspective to explore the trends and knotty nature of communication surveillance, repressive national legal regimes and state responses to right to internet privacy and netizens roles and challenges in relation to online platform and its power politics. As of today in 2016, the human rights defender and online communities in Bangladesh, India and Pakistan, specifically, those who are critical towards ruling governments have been subjected to various kinds of ill treatments and have been under constant surveillance and threats.[20] Second, it was difficult to perform a field research or conduct in-depth interviews of the relevant stakeholders, partly due to time constrains, resources and personal security concerns. Thirdly, this research limits itself into three South Asian countries, Bangladesh, India and Pakistan and also deals with only cyber and telephonic surveillance technologies in these respective countries. Basically, it excludes Wide-area and Multiple-sensor (WAMS)[21] surveillance systems, such as border surveillance, the use of Close Circuit Television (CCTV), facial recognition sensors or behavioral analyses sensors and so on. It is also evident that there are number of crosscutting and essentially contested concepts, terms and terminologies frequently being used, for example, internet freedom, crimes against internet, digital rights, human rights defenders or even the region 'South Asia' and so on. All these concepts, terms and terminologies have its' own discourse, paradigms and contestation with different values and norms but most cases it takes naïve and simple approach to simplify to the readers. However, there are number of cases evolving concepts, terms and terminologies

[20] Ibid.
[21] Davis, Fergal, Nicola McGarrity, and George Williams. *Surveillance, Counter-Terrorism and Comparative Constitutionalism*. Routledge, 2014.

discussed with references as well. Fourthly, it is safe to confess that there are several human rights violations happing offline as well as online and those are also need to be addressed such as extra-judicial killing, enforced disappearances, police torture, and so on. Therefore, it important to acknowledge that right to Internet privacy or freedom of expression online are not the only issues that are relevant to South Asian online community, although it is important to analysis and assess communication surveillance regimes from a rights based perspective. Fifthly, this research heavily depends upon human rights based principles, which actually at the end naming and shaming to the State centric surveillance systems and technologies. Indeed, this research failed to demonstrate number of ground breaking theoretical discourses and also private sponsored communication surveillance in South Asia.

Structure of the Research

This research has three comprehensive chapters, first part of the first chapter, explores South Asian States' vision in digital civic space and the reality of internet usages, physical and technical infrastructures, universal access and service qualities. In the second part of the first chapter, identifies the key forms of digital rights violations, including targeted and mass surveillance programs in cyber space and telephonic communication, primarily, against online activists and human rights defenders in last three years from 2013 to the end of 2015 in three countries, namely, Bangladesh, India, and Pakistan. In the second chapter, it broadly investigates the knotty rise of national and international cooperation of communication surveillance, modalities of communication surveillance and their actors in South Asia, whereas, the second part of the same chapter largely discusses about the emerging international human rights frameworks in the age of massive communication surveillances. The final and third chapter efforts to discuss the problematic legal and regulatory landscapes of communication surveillance as well as

constitutional and ordinary legal protections of the right to privacy and freedom of expression, relevant case laws and its evolution as judicial responses in South Asia due to the increases pervasiveness of surveillance in the region. At the end of the same chapter attempts to identify the key challenges, problems and gaps of communication surveillance from HRDs and online activists in South Asian digital context and in response, it suggests to adopt a human rights based approach to communication surveillance in South Asia.

Chapter 1
South Asian Digital Rights: An Assessment of Changing Communication Landscape

Most of the South Asian countries have seen democratic changes of power through national parliamentary and presidential elections from 2013 to 2015, mainly, Bangladesh in the month of January 2014, India in May 2014, Pakistan in May 2013, and Sri Lanka in January 2015. Almost all major political actors during their election campaigns or even after sworn into power, as a new government or a coalition government were promised to develop internet infrastructures, end to 'digital divide'[22] and increase the internet and mobile phones penetration rates into their respective countries. Their mere declaration or political rhetoric does not change the reality and bring changes into the situation of digital rights, or not even end the digital divide. In spite of some positive changes in regards to burgeoning digital access, the internet users and communities have had experienced of more repressive regulatory frameworks,[23] escalated arrest and detentions for online speech,[24] and restrictions on digital access[25]. For instance, the head of the Government of Bangladesh, Prime Minister Sheikh Hasina amenably inspires open digital accesses and consider communication technology as tool of socio-economic development but under her leadership at least three-hundreds ostensible criminal cases had filed in related to Information and Communication Technology (ICT) crimes, among them at least twenty-one individuals convicted for online speeches against her and her family members.[26] In addition, the political and electoral victory in 2014 of a conservative political party, the *Bharatiya Janta Party* (BJP) posed threats to digital rights by intimidating internet users and increased website blocking

[22] Pippa Norris, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide* (Cambridge University Press, 2001).
[23] See Chapter III
[24] See Chapter I, section of 'Crimes against Freedom of Expression and Internet Freedom'
[25] See Chapter I, See Chapter I, section of 'Crimes against Freedom of Expression and Internet Freedom'
[26] New Age Report, "Youth Jailed for Parody on Sheikh Mujib, PM," *New Age*, September 25, 2014, Online Edition edition, sec. Front Page, http://newagebd.net/52448/youth-jailed-for-parody-on-sheikh-mujib-pm/.

and filtering. Interesting enough, another conservative political party, the *Muslim-League* formed a government in May 2013 and joined as a last soldier in the line of military and civilian authorities to restrict internet freedoms instead of concentrating previous allegations of abuse of powers and 'crimes against freedom of expression and internet. [27]

In 2011, the Freedom of Expression on the Internet report by United Nations Special Rapporteur for Freedom of Expression, Mr. Frank La Rue has emphasizes the importance of internet infrastructures and access to internet on the realization of the right to freedom of opinion and expression."[28] It reaffirms at paragraph 85, "each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of population".[29] Therefore, to understand the nature and landscape of communication surveillance and digital rights discourse of privacy in a digital context of South Asian trajectory, first, there is a need to understand the rhetoric of governments and changing technical and physical communication infrastructures of the Internet and cellular technologies and its platform politics and acknowledge the current contemptuous situation of digital rights and 'crimes against internet freedom' in South Asian. Therefore, the first part of this research chapter attempts to explore states vision in digital civic space and the reality of communication usages and access, physical and technical infrastructures, and service quality of communication technology. In the second part, this paper identifies the key forms of digital rights violations including targeted and massive surveillance programs in ICT sector over the three years from 2013 to the end of 2015

[27] See Joint Declaration on Crimes Against Freedom of Expression, June 2012.
[28] United Nations Special Rapporteur for Freedom of Expression, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (United Nation, May 16, 2011), United Nations Special Rapporteur for Freedom of Expression.
[29] Ibid.

in Bangladesh, India, and Pakistan with reference to organizations and specific communities affected such as Human Rights Defenders (HRDs), journalists, bloggers, and internet users in general.

Overview of Communication Infrastructures and Development in ICT

South Asian States and Digital Rhetoric

In spite of systematic and logical digital progression of ICT in the world, South Asian ICT sector could be termed as 'urban privilege commodity'[30] from internet users' perspective, on the contrary, South Asian governments consider ICT sector as a driving force of socio economic development and end poverty in the region. For example, Bangladesh state launched a digital Bangladesh 'Vision 2021'[31], the *Bangladesh Awami League's* (BAL) election manifesto in December 2013 to create a digital friendly Bangladesh. Around the same time, in August 2014, the Indian Government launched similar campaign 'Digital India'[32] which is also planning to a digital friendly country by 2018. In privation of sustainable and effective initiatives, 'Pakistan Vision 2025'[33] by the Ministry of Planning of Pakistan is misnomer, thereofore, private mobile service providing company *Telenor* and Pakistan Software Houses Association (PASHA) jointly launched 'Digital Pakistan 2020' in October 2015.[34] In spite of overhauls by the respective governments in South Asia, all the digital vision whitepapers and campaigns have faced ridicule and harsh

[30] Daniel Miller, "Could the Internet Defetishise the Commodity?," *Environment and Planning D: Society and Space* 21, no. 3 (June 1, 2003): 359–72, doi:10.1068/d275t.
[31] Prime Minister Office, "Digital Bangladesh | Access to Information (a2i) Program" (Access to Information Program, November 5, 2009), http://www.a2i.pmo.gov.bd/digital-bangladesh. However, the Year 2021 marks the 50th anniversary of Bangladesh's independence.
[32] Department of Electronics and Information Technology, Government of India, "Digital India" (Deity, Government of India, August 18, 2014), http://deity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf.
[33] Ministry of Planning, Development and Reform, Government of Pakistan, "Pakistan 2025: One Nation One Vision" (Planning Commission, Government of Pakistan, May 29, 2014), http://www.pc.gov.pk/wp-content/uploads/2015/05/Pakistan-Vision-2025.pdf.
[34] Ahsan Yameen, "P@SHA Aims to Energize IT Industry of Pakistan through Variety of Events," *Tech Mag – Pakistani Online IT & Technology Magazine & News Platform*, January 10, 2016, http://techmag.pk/psha-aims-to-energize-it-industry-of-pakistan-through-variety-of-events/.

criticism by the non-governmental organizations, academics, ICT experts, on-line activists, lawyers and even from the autonomous government agencies such as Telecom Regulatory Authority of India (TRAI),[35] the National Human Rights Commission (NHRC) of Bangladesh,[36], and a relevant parliamentary Standing Committee in Pakistan[37]. Despite of all criticism, ridicule, and overhauls by contested actors, the visionary whitepapers encourages the broad use of ICT, symbolizes the modern approaches, paradigms and philosophy of successful and expedient use of ICT in terms of improving and implementing the socio-economic rights in Bangladesh, India and Pakistan. For examples, the philosophy of "Digital Bangladesh" comprises of "ensuring people's democracy and human rights, transparency, accountability, establishing justice and ensuring delivery of government services to the citizens of Bangladesh through maximum use of technology, with the ultimate goal being the overall improvement of the daily lifestyle of general people".[38]

However, in depth reading suggests that all visionary whitepapers of digital vision in respective countries includes trade and economic affairs or engagement of the state and their agencies in realm of ICT but not necessarily speaks about the conditionality of civil and political affairs of the state. In addition, the concept of Public and Private Partnerships (PPP) heavily emphasized by the states in line with neo-liberal economic policy.[39] Nevertheless, the private commercial

[35] See details at "Trai Wants Auction of 3G Spectrum after Formation of New Govt. - Indian Express," accessed March 28, 2016, http://archive.indianexpress.com/news/trai-wants-auction-of-3g-spectrum-after-formation-of-new-govt/1225198/. And also "TRAI Spectrum Price Proposal May Fetch Rs 5.36 Lakh Crore for Govt.," *The Indian Express*, January 28, 2016, http://indianexpress.com/article/india/india-news-india/trai-spectrum-price-proposal-may-fetch-rs-5-36-lakh-crore-for-govt/.

[36] ChanneliFrance, *Dr. Mizanur Rahman in Paris, Channel I Europe News By Hasem*, accessed March 28, 2016, https://www.youtube.com/watch?v=bHKNi-q4-JE.

[37] See Details Asad Hashim, "Surveilling and Censoring the Internet in Pakistan - Al Jazeera English," *Aljazeera English Op-Ed*, May 13, 2015, Online Edition edition, sec. Internet, http://www.aljazeera.com/indepth/features/2015/05/pakistan-internet-censorship-150506124129138.html.

[38] "Vision 2021," *Wikipedia, the Free Encyclopedia*, December 27, 2015, https://en.wikipedia.org/w/index.php?title=Vision_2021&oldid=696993924.

[39] For examples, Ministry of Health of Bangladesh encourages public- private partnership in health sector via ICT.

stakeholders from Bangladesh, India and Pakistan are playing major role to train, engage and empower younger generation inside their respective countries in absence of government engagements to raise the communication usage proliferation.

South Asian Electronic Communication Usage and Access

The 2015 report of the Telecommunication Regulatory Authority of India (TRAI) claimed that India is the third largest internet subscribers' country after the China and United States and estimates that more than 302 million internet users subscribe internet via 1006.96 million of wireless and wirelines inside the country.[40] It also claimed almost 108.85 million internet users using internet via broadband internet servers and 980.81 million mobile users using mobile and among overall mobile users, 293 million people using mobile internet as of till June 2015.[41] However, it is important to remember that as of June 2014, internet users reached to 20 percent compared to overall sizeable population and later, raised to 24 percent in March 2015. At the same time mobile phone penetration (77 percent by March 2015) was much higher.[42]

According to World Bank (2013) out of 180 million populations, over 70 percent of people have mobile phone connection and only 11 percent of population uses internet in Pakistan.[43]. According to International Telecommunication Union (ITU) in early 2014, internet penetration is only 14 percent, whereas, the private mobile company graphed internet penetration stake at 16 percent and half of the connectivity transmits through mobile connection.[44] Like India, several parts of conflict

[40] Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators," Quarterly Report (New Delhi: Telecom Regulatory Authority of India, March 2015), http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator-Reports-Mar12082015.pdf.
[41] Ibid
[42] Ibid
[43] World Bank, "Pakistan | Data," Internation, *Pakistan: Internet Users (per 100 People)*, accessed March 29, 2016, http://data.worldbank.org/country/pakistan.
[44] International Telecommunication Union, "Internet World State 2014: Pakistan, Asia Marketing Research, Internet Usage, Population Statistics and Facebook information," accessed March 28, 2016, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

zones in Pakistan have not internet access, partly because of internal conflicts with central government/state. After the installation of the 3G and 4G spectrum of internet infrustructures, Pakistan Government expected to change internet proliferation rates in recent years and also significantly reduced bandwidth prices of internet.[45]

The comparative statistics suggests that internet penetration rates of Bangladesh are low compare to India and Pakistan and just under the 10% of population have internet access out of 160 million. It important to consider that access to internet and usage rates are gradually progressing although most of the users approximately 96 percent getting access to the internet via mobile phones, which recently offered 3G service.[46] Last few years, in spite of users complains, Government are trying hard to reduce the price of internet bandwidths and mobile internet data. According to ITU, internet penetration is 9.6 percent in the year of 2014 and got up from 3.3 percent compare to previous year, although Government argues it was just under 30 percent compare to overall population.[47] On the other hand, Bangladesh Government agency, Bangladesh Telecommunication Regulatory Commission (BTRC) estimates mobile users and penetration gained momentum from 74 to 76 percent in the year of 2014.[48]

South Asian ICT Infrastructures and Service Quality

South Asian physical internet infrastructures were historically poor and highly vulnerable compares to other emerging develop countries. After connecting to the undersea fiber optical cable of SEA- ME-WE 4[49] Bangladesh Internet Exchange (BDIX) established exclusive control access to the prime

[45] "In Demand: 3G User Base Expanding, Market Surges Forward," *The Express Tribune*, September 16, 2014, http://tribune.com.pk/story/762745/in-demand-3g-user-base-expanding-market-surges-forward/.
[46] "Internet Subscribers in Bangladesh June 2015 | BTRC" (Dhaka, Bangladesh: BTRC), accessed March 29, 2016, http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2015.
[47] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2014," accessed March 28, 2016, http://data.un.org/Data.aspx?d=ITU&f=ind1Code%3AI99H.
[48] Internet Subscribers in Bangladesh June 2015 | BTRC" (Dhaka, Bangladesh: BTRC), accessed March 29, 2016, http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2015
[49] ibid.

internet network inside the country, correspondingly, Pakistan Internet Exchange (PIX) has access control of SEA-ME-WE 3,[50] and I-ME- WE cable,[51] whereas, India connects directly to the global submarine cables. Since late 2000, after the connection to global submarine cables, all South Asian internet users produce huge amounts of communication data and traffic.

There are number of national and international service providers and their networks are providing internet and mobile services in Bangladesh, India, and Pakistan. For instances, as of March 2015, one hundred twenty-eight national and international Internet Service Providers (ISPs) are functioning under BTRC to provide internet and six international mobile connection operators providing fastest 3G internet which meet up ninety-six percent penetration of internet compare to overall internet users.[52] According to the Internet Service Providers Association of Pakistan, at least ten ISPs agencies are still using traditional service such as Digital Subscribers Lines (DSL) service and forty ISPs are using modern technology in spite of low internet penetration rate.[53] It is also reported that at lest sixty percent of broadband market controlled by the Pakistan Government agency, the Pakistan Telecommunication Authority (PTA)[54] whereas, in Bangladesh, BTRC does not have legality to conduct such business in market. In spite of poor coverage and low cost of mobile connectivity, at least four multinational companies, namely Ufone, Telenor, Zong and Mobilink are providing 3G and 4G spectrum to the mobile internet.[55] Whereas, in India eighty percent of mobile operators are coming from local companies with joint venture between or among international telecommunication companies (i.e.

[50] This connects to Southeast Asia, Middle East and Western Europe
[51] This links to India, Middle East and Western Europe
[52] Internet Subscribers in Bangladesh June 2015 | BTRC" (Dhaka, Bangladesh: BTRC), accessed March 29, 2016, http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2015.
[53] "ISPAK: Internet Service Providers Association of Pakistan," accessed March 29, 2016, http://www.ispak.pk/.
[54] "O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-Based Netsweeper's Role in Pakistan's Censorship Regime," *The Citizen Lab*, June 20, 2013, https://citizenlab.org/2013/06/o-pakistan/.
[55] "ISPAK: Internet Service Providers Association of Pakistan," accessed March 29, 2016, http://www.ispak.pk/.

Vodafone).[56] Moreover, there are one hundred and twenty-nine ISPs are proving internet service but ninety-eight percent of the market control by top ten intermediaries.[57]

Almost all three countries, ISPs residue via a traditional internet service providing infrastructure (i.e. fixed telephone network and DSL service) or modern infrastructures such as wireless Wimax technology and broadband subscription. However, the most striking fact is that all three countries government authorities namely, BTRC, PTA and Indian two ministerial departments (i.e. Department of Electronics and Information Communication and Department of Telecommunication) exert substantial control over ISPs and mobile operators through a cumbersome licensing regimes and bureaucratic process.[58] In addition, the intermediary agencies are using highly advanced and comprehensive surveillance technologies due to their own government request, partially in defense of national security exception and strict licensing regimes to track so called 'nation threats' and geopolitical roles of countering militant networks across the region. For example, Pakistan and Indian military establishments have received good number of funding from western government and their development partners to introduce a comprehensive communication surveillance mechanisms and infrastructure.[59]

However, the comparative study suggests that only few percentages of South Asian of the world population used internet in South Asia region and among all other countries, Bangladesh has lowest percent of internet users and usage. According to World Economic Forum's Global IT report in 2013, ranked India 87 out of 147, Bangladesh 114 out of 147, and Pakistan 132 out of 147 due to many reasons, including lack of internet and electronic infrastructures, electricity shortage, low literacy rate,

[56] "Cable Trouble Hits Twitter, Other Mobile Services," *The Indian Express*, February 19, 2015, http://indianexpress.com/article/technology/technology-others/cable-trouble-hits-twitter-other-mobile-services/.
[57] Ibid.
[58] See details in Chapter III.
[59] See Chapter I, section of 'Rise of National and International Surveillance Cooperation'.

economic hardship, poor service quality, lack of good will and cultural resistance by the users, limited contents and their access to uniform languages and so on.[60] Conversely, it is also evident that South Asian internet community and their usage had observed phenomenal progression in urban areas, particularly in and around major South Asian cities in last few years.

'Crimes against Freedom of Expression and Internet'

Since the inception of statehood, the post-colonial South Asia states are struggling to secure peace or protect human rights, end lifelong armed conflicts and also failed to stop indiscriminate acts of violence against citizens. Last few years, the cyber space also replicates similar reality like as offline. There have been several reported instances of lawful and unlawful or even unauthorized mobile interception and cyber surveillance, restriction on websites access including social networks such as YouTube and Facebook, state sponsored censorship, blocking and filtering, media manipulation and judicial harassments including summons from the judiciary to internet users or cyber dissidents for their online presence and speech. Although South Asian countries like Bangladesh, India or Pakistan governments does not have an official public policy on communication surveillance or tracking internet or mobile communication to monitor users' details including human rights defenders or dissident voices. Since right to privacy as a gateway for freedom of expression, all these state sponsored 'crimes against freedom of expression and internet' postures threat to the digital activism and digital rights. Hence, the following section examines the recent key developments (from 2013 to the end of 2015) of digital rights and internet freedom in the region with few utmost notable cases.

[60] "The Global Competitiveness Report 2013-2014," *World Economic Forum*, accessed March 26, 2016, https://www.weforum.org/reports/global-competitiveness-report-2013-2014.

Killing, Intimidation and Violence

Last few decades, there are number of human rights violations and state sponsored crimes swamps in South Asia, however, the most worrying aspect is how the offline reality extending gradually to the online domain. On a more serious note, in February 2013, Ahmed Rajib Haider, one of the *Shahbag* movement activists and bloggers in Bangladesh was killed by extremists on the ground of his blog posts that offended Islam and religious groups.[61] A year earlier, three journalists have been killed and a number of online activists and bloggers were attacked on similar grounds. As more and more fatal physical violence against online activists and bloggers, 2015 was just another bloody year. Dr. Avijit Roy, a self-proclaimed atheist blogger, and his wife Rafida Ahmed Bonya were attacked at University of Dhaka where Dr. Roy had hacked to death and his wife was severely injured. Another three bloggers, namely Anantha Bijoy Das, Washiqur Rahman, and Nilyo Neel also known for his critical writings about Islam were hacked to death.[62] The neighboring country, Pakistan has suffered from similar deadly attacks on cases related to 'online blasphemy'. In 2014, Rashid Rehman, a defense attorney of digital blasphemy case in Punjab was killed at his office by unidentified gunmen.[63] Also, a judge sentenced death penalty of two Christian couples for sending blasphemous text messages to local Muslims via online.[64] HRDs, bloggers and online activists were continuously reported to receive death threats related to their online and offline activism and presence. In the period between 2013 and 2015, women were increasingly harassed online where almost 45 percent of women reported online-harassment in Pakistan, while the rest refrained in

[61] Al Jazeera Englsih, "An Attack on Bloggers," accessed March 30, 2016, http://www.aljazeera.com/programmes/101east/2015/11/bangladesh-attack-bloggers-151117122237015.html.
[62] Ibid.
[63] AFP | Dawn.com, "Rights Advocate Rashid Rehman Khan Gunned down in Multan," May 7, 2014, http://www.dawn.com/news/1104788.
[64] "Pakistani Couple Get Death Sentences for Blasphemy," *BBC News*, accessed March 30, 2016, http://www.bbc.com/news/world-asia-26901433.

fear of losing access to ICT.[65] India on the other hand, is well-known for online harassment for women as well. In 2014, many online activists filed complaints against men making rape threats on social media.[66] In 2015, social activist Sunitha Krishnan was attacked at her car for initiating "Shame the Rapist" campaign on social media.[67] In addition, violence took place over a course of four days on the basis of Facebook posts against Islam in the city of Gujarat.[68]

Wrongful Detentions and 'Judicial Persecution':

The Information and Communication Technology Act-2006 of Bangladesh along with Penal Code have been actively used against human rights activists and journalist in Bangladesh. In 2013, Adilur Rahman Khan, Secretary of a human rights organization *Odhikar*, was arrested and charged on claims of publishing fabricated reports using distorted images in Photoshop.[69] Followed by the arrest of Adilur, Nasiruddin Elan, Director of *Odhikar* also arrested on the same ground. In 2014, a British journalist was charged with contempt of court by the International Crimes Tribunal for his blogs post published in 2011 and 2012 and later been punished with fine.[70] Blasphemy charges are the major cause of detention in Pakistan. In 2015, an Islamic evangelist pop-star was accused of blasphemous act in a video that went viral.[71] A year earlier, a Christian blogger was accused of

[65] "Statistics - Academic and Community Studies," *Stop Street Harassment*, accessed March 30, 2016, http://www.stopstreetharassment.org/resources/statistics/statistics-academic-studies/.
[66] "Woman Files Complaint against Man Who Called for 'Women like Her to Be Raped by Rapists,'" *The News Minute*, January 16, 2015, http://www.thenewsminute.com/socials/114.
[67] "Shame on Sunitha Krishnan: 5 Reasons Why Sharing the Whatsapp Rape Video Is Wrong - Firstpost," accessed March 30, 2016, http://www.firstpost.com/living/shame-on-sunitha-krishnan-5-reasons-why-sharing-the-whatsapp-rape-video-is-wrong-2086323.html.
[68] Gaikwad Rahi, "Over 100 Held for Vadodara Violence," *The Hindu*, September 30, 2014, http://www.thehindu.com/news/national/other-states/over-100-held-for-vadodara-violence/article6458715.ece.
[69] "Statement on Arrest of Adilur Rahman Khan, Secretary of Odhikar | Odhikar," accessed March 30, 2016, http://odhikar.org/statement-on-arrest-of-adilur-rahman-khan-odhikar-secratary/.
[70] Agence France-Presse, "Bangladesh Court Convicts British Journalist for Doubting War Death Toll," *The Guardian*, December 2, 2014, sec. World news, http://www.theguardian.com/world/2014/dec/02/bangladesh-convicts-british-journalist-david-bergman.
[71] Femi Ajasa, "Mob Attack Former Pakistan Pop Star Accused of Blasphemy," *Vanguard News*, March 27, 2016, http://www.vanguardngr.com/2016/03/mob-attack-former-pakistan-pop-star-accused-blasphemy/.

blasphemy online and arrested in Lahore.[72] While in India, statements against politicians were the major cause behind many arrests and complaints against online users. In 2014-2015, most of the arrests happened against young Facebook users who were charged under Section 66A of Information Technology Act-2000 for their questionable content and publication on social media against politician and the state.[73] Lots of defamation cases were also reported against website owners for users' comments.

Blocking, Filtering and Manipulation

The international and national service or content providers were also targeted of blocking and filtering regimes by South Asia governments. The government of Bangladesh has blocked Viber, WhatsApp and Tango on the ground of security that these apps were used in terrorist acts.[74] Facebook and YouTube suffered same blockage in 2012 and 2013 in Bangladesh.[75] While historically the government of Pakistan worked on blocking individual Internet Protocol (IP) addresses and ISPs at least from 2005, by the year 2015, the government increasingly sought to implement more fileting mechanisms on IPs.[76] Whilst the Pakistan Telecommunication (Regulation) Authority Act does not allow to block contents, the government worked in 2015 to do some amendments to give the PTA the power to block and regulate content based on terrorists' threats ground. Since 2012-2013, the YouTube was also blocked during 2013 for publishing of Anti-Islamic video. According to the Indian cybercafé law, cybercafé can filter and block websites

[72] AFP, "Christian Healer Arrested for Blasphemy in Lahore," October 19, 2015, http://www.dawn.com/news/1214151.
[73] "Facebook Trouble: 10 Cases of Arrests under Sec 66A of IT Act," *Http://www.hindustantimes.com/*, March 24, 2015, http://www.hindustantimes.com/india/facebook-trouble-10-cases-of-arrests-under-sec-66a-of-it-act/story-4xKp9EJjR6YoyrC2rUUMDN.html.
[74] Muhammad Zahidul Islam, "Viber, Tango Blocked in Bangladesh | Dhaka Tribune," accessed March 30, 2016, http://www.dhakatribune.com/bangladesh/2015/jan/18/govt-shuts-down-viber.
[75] Ibid.
[76] Sanja Kelly, et al., "Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015," Human Rights Report (New York: Freedom House, October 2015), https://freedomhouse.org/report/freedom-net/freedom-net-2015.

related to pornography and obscenity. In 2013, many ISPs were instructed to block more than 70 URLs criticizing the government.[77] Newspapers and online Journals like the Times of India and Wall Street Journal were blocked for reporting a defarmation cases[78].

Self-Regulation, Content Removal and Restriction on Connectivity

During the rise of the *Shahbag* movement in 2013, the government has requested blog hosts to remove blog posts related to content that was labeled as anti-Islamic. In the same year, a government committee along with religious clerics have identified 84 bloggers and Facebook users who posted "anti-Islamic" content and directed blog hosts to remove content belonged to four of the *Shahbag* movement.[79] Similarly, Pakistan has issued many orders to the global social media giants, such as Twitter and Facebook to remove content that were considered blasphemous or critical to the state. Also in 2014, it was reported that websites like the Guardian and Storify were inaccessible in some part of Pakistan.[80] It is also reported that in 2013 to 2015, as in previous years the government of Bangladesh and Pakistan suspended internet and cellular service on some religious holidays and certain 'sensitive' places.[81]

Compromised Anonymity, Digital Surveillance and Privacy

In the rise of mass surveillance around the world, South Asian cyber space is not immune from the debate of communication surveillance. The communication surveillance mechanisms to control cyber dissidents in many cases overlook the formal legal frameworks. Therefore, unauthorized surveillance also in rise and the State's attempts to legitimize their greater communication surveillance power with ostensible arguments such national security, public morality and public

[77] Ibid.
[78] ibid.
[79] "Myth of the 84 Bloggers 'Hit' List in Bangladesh: Busting the Media Narrative | Turkey Agenda," accessed March 30, 2016, http://www.turkeyagenda.com/myth-of-the-84-bloggers-hit-list-in-bangladesh-busting-the-media-narrative-2842.html.
[80] "The Guardian Website Inaccessible in Parts of Pakistan," *The Express Tribune*, February 3, 2014, http://tribune.com.pk/story/666959/the-guardian-website-reportedly-inaccessible-in-pakistan/.
[81] See details at Freedom of Net report from 2010 to 2015.

order. The State now has greater capacity to conduct targeted and broad scope of mass surveillance than ever before. As mentioned previously, the Pakistani government and intelligence agencies has expanded its communication surveillance and content monitoring beyond bloggers and activists but to encompass regular Pakistani users. For instance, the Fair Trial Act 2013 grants security agencies jurisdiction to monitor communication that may pose threat to national security inside and outside the country.[82] The compulsory SIM card biometric and obligatory registration prevent any kind of anonymity in telecommunication of regular Pakistani citizens on the ground of terrorism acts.[83] Documents obtained by Pakistani hackers showed that Fin Fisher, a surveillance system was used to collect data from Skype, audio and screenshots.[84] India on the other hand, is using the problematic Information Technology (IT) Act to promote more interception of online communication.[85] ISPs are forced by law to provide guaranteed to the government that it has installed programs and measurement to allow for communication interception in cases deemed to be necessary by the government. Cybercafés requires to provide photograph of customers, their national identification and maintain record of browsing histories for each customer.[86] In addition, IT Act of India penalizes "any ISP that doesn't comply with request to intercept, monitor and decrypt communication upon requests".[87] Added to that the Central Monitoring System (CMS) that is being used to intercept online activities and store them in a centralized database that is accessible by the Government officials anytime. India went beyond

[82] See details at Chapter II.
[83] Aziz Nayani Master's c, idate, and international affairs at Columbia University, "Pakistan's Cellphone-Registration Policy Will Do Little to Curb Terrorism," *Quartz*, accessed March 30, 2016, http://qz.com/360420/pakistans-cellphone-registration-policy-will-do-little-to-curb-terrorism/.
[84] "Digital Rights Foundation › Pakistan Is a FinFisher Customer, Leak Confirms," *Digital Rights Foundation*, accessed March 30, 2016, http://digitalrightsfoundation.pk/pakistan-is-a-finfisher-customer-leak-confirms/.
[85] See details at Chapter II.
[86] Anisha Ashokan, "Cyber Cafes Flout Rules, Do Not Ask Users for ID Proofs | Latest News & Updates at Daily News & Analysis," accessed March 30, 2016, http://www.dnaindia.com/mumbai/report-cyber-cafes-flout-rules-do-not-ask-users-for-id-proofs-1180572.
[87] See Section 67 of IT ACT 2000.

borders to request from international service providers like Facebook and Google to gain access to certain users' accounts and online content.[88]

The neighboring country Bangladesh has amended the Bangladesh Telecommunication Regulatory Act (BTRA) in 2006 to allow for telephonic interception of voice and data communication.[89] Since the citizens of Bangladesh are required to present their national identification card and provide personal information when applying for a mobile connection, the government has used what is called deep-packet inspection to monitor and intercept communication that is identified to be illegal or unlawful when transmitted over the internet. There is no legal body that is responsible to safeguard the people's right to privacy as guaranteed by the Constitution of the state parties and also investigative reports by international and national human rights organizations like Privacy International has stated that the government sought for a Swiss surveillance systems and technologies to obtain data from mobile phones specially in public demonstrations.[90] The year 2016 also witnessed fresh blockage of communication applications like *Viber* and requests from social media platforms like Facebook to gain access to content posted by online activists.[91]

'Digital Activism' at Risk: In the Name of…

There are number of South Asian digital activism under threats in the name of national security, public morality and order, decency, affecting friendly relations with other states, incitement to commit offences and contempt of court.[92] For instances, the *Shabag* movement of 2013, initially organized by

[88] Melody Patry, "India: Digital Freedom under Threat? Online Censorship," *Index on Censorship*, November 21, 2013, http://bit.ly/1LnnVAI.
[89] See section 97 of BTRC ACT 2006.
[90] David Bergman, "New Age," *New Age*, February 16, 2015, http://newagebd.net/95692/telecom-operators-retain-6-months-of-sms-other-info-for-law-enforcers/.
[91] Ibid.
[92] See details at Chapter II, All three countries restricts freedom of expression by constitutional provisions.

the Bangladeshi Online Activism Network (BOAN), was a prominent digital movements and due to their political stance and utilization of social media, many bloggers and online activists were subjected to harsh agitations by government officials as well as religious and secular extremists. In Pakistan, human rights activists and online activists called for campaigns to drive public attention against militancy through the online domain are also subjected similar persecution. Since in 2014, they initiated rallies and campaigns against clerks who refused to publicly condemn terrorist attacks on schools.[93] Net Neutrality campaigns and petitions in India is the fastest growing global digital movement in recent history and the campaign through civil society groups managed to push the government to review the internet.org agreement with Facebook in the light of concerns raised by the campaign.[94] However it has reported that some of the leading figures also faced illegitimate restriction and treats by the government and ruling party members.

In next chapter, this research pinpoints the key cooperation between national and international actors in regards to communication surveillance and the nature and modalities of key interferences used by the State in age of communication surveillance in Bangladesh, India and Pakistan. In the next chapter, it also highlights the key emerging International human rights frameworks of right to privacy and freedom of expression in the age of communication surveillance.

[93] See details at Freedom of Net Report 2015.
[94] Ibid.

Chapter 2
The Rise of Communication Surveillance in South Asia and International Human Rights Frameworks

The Knotty Rise of National and International Surveillance Cooperation in South Asia

In 2013, the United Nations General Assembly adopted a consensus Resolution (A/RES/68/167)[95] which "reaffirms existing human rights instruments and notes that technological developments enhance surveillance, interception and data collection capabilities which may violated or abuse human rights, in particular the right to privacy".[96] One the one hand, South Asian online communities participation and innovation in technologies have accelerated increased possibilities for communication and freedom of expression over the internet, on the other hand, states are gradually stepping or seeking for more interception and monitoring private individuals' communication to serve national pathological interest. In spite of all progressive and positive development in ICT in South Asia, troublesome digital rights records and call for the European Union trade control on ICTs,[97] there are good numbers of surveillance technology flow to South Asian governments and agencies. The citizens of Bangladesh and Pakistan found that countries premier network service providers respectively BDIX and PIX hosts a surveillance technology,

[95] After the Edward Snowden's revelation this document first time introduced by Germany and Brazil. See page page 138 of A/68/456/Add.2

[96] Intellectual Property Watch, "UN General Assembly Adopts Resolution on Privacy and Surveillance," *Intellectual Property Watch*, January 8, 2014, http://www.ip-watch.org/2014/01/08/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/.

[97] Since 2011, the European Commission Regulation No. 428/2009 under review which is regulating the European export of dual-use items. In Communication (2014)244 pointed out that the European Commission has set out to review export control policy in Europe to "ensuring security and competitiveness in a changing world". For details, Coalition against Unlawful Surveillance Exports, "The Critical Opportunity: Bringing Surveillance Technologies within the EU Dual- Use Regulation," NGO Report, CAUSE (Global: Coalition Against Unlawful Surveillance Exports, June 2015), https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf.

namely 'Fin Fisher'.[98] In addition, there are number of surveillance technology such as International Mobile Subscriber Identity (IMSI Catchers) or Stingrays,[99] which is capable to identify and track the mobile phones and intercept phone calls. After an investigation by PI and another Swiss magazine WOZ in March 2014, it revealed that brutal security force officials from Rapid Action Battalion (RAB) of Bangladesh were hosted for ten days as a potential buyer in Zurich by a manufacturer company of IMSI catchers, Neosoft.[100] Moreover, it also revealed by an investigative report of Privacy International (PI)[101] in 2012 that the National Security Agency (NSA)[102] of United States and the British counterpart, the Government Communications Headquarters (GCHQ)[103] have targeted Pakistan's cellular networks secretly monitor voice, traffic and data.[104] This report also identifies that "Targeted IP Monitoring System and Common Operations Environment (COE) would allow Pakistan to collect and analyze a significant portion of communications travelling within and through the country at a centralized command center".[105] For number of grounds, PI's report is significant, since it revels for the first time of the previous unknown mechanisms of surveillance capacity of Pakistan Government, particularly Inter-Services Intelligence Agency (ISA) and also discloses effective cooperation with foreign

[98] "Fin Fisher is a product suite from Gamma International UK, which helps government apply state-operated surveillance through its capabilities as an T intrusion and remote monitoring system". See details at Nighat Dad, "Big Brother Is Curtailing Net Freedom in South Asia," *Aljazeera English Op-Ed*, January 11, 2014, Online Edition edition, sec. Opinion, http://www.aljazeera.com/indepth/opinion/2014/01/big-brother-curtailing-net-freedom-south-asia-20141544556701717.html.

[99] "The Catchers imitate a mobile phone tower by sending and responding signals in order to extract the unique subscriber identification module (SIM)", See details at United Nations Human Rights Council, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," n.d., http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[100] See details Edin Omanovic, "Eight Things We Know so far from the Hacking Team Hack | Privacy International," Advocacy, *Being Stealth and Untraceable*, accessed March 28, 2016, https://www.privacyinternational.org/node/619.

[101] A UK based rights organization who is currently playing a crucial role in the discourse of communication surveillance, right to privacy and digital rights.

[102] A leading security and intelligence organization, commissioned by United States Government.

[103] A security and intelligence organization Commissioned by United Kingdom Government.

[104] Matthew Rice, "Tipping the Scales: Security and Surveillance in Pakistan | Privacy International," Special Report, Big Brother Project (London, United Kingdom: Privacy International, July 2015), https://www.privacyinternational.org/node/624.

[105] Ibid

government and their allies from at least 2005. It also found that "Pakistani Government obtained this technology from both domestic and foreign surveillance companies including Alcatel, Ericsson, Huawei, SS8 and Utimaco".[106]

Like neighboring country Bangladesh and Pakistan, for the first time Indian Government has introduced an aggressive surveillance mechanism called Network Traffic Analysis System (NETRA) which monitor communications to generate any content prescribing certain keywords.[107] On the one hand, NETRA targets to scan internet communication via different social media and blogs including chat transcripts and voice over traffic, on the other hand, the Central Monitoring System (CMS) and mobile phone tapping focuses telephonic communication targeted against individuals including rights activists and cyber dissidents.[108] In addition, in terms of International cooperation 'India states host many security technology expos' and many neighboring country officials and private individuals regularly attends those expos.[109] The Centre for Internet and Society of India's research reveals that seventy-six companies out of one hundred who participated at expos in different years, are actually selling surveillance products in different countries including India and their neighbors. The products includes "Internet Monitoring Software, social network analysis software, data mining and profiling software, surveillance cameras, analytics, biometric collection, access control systems etc.".[110] Among these companies almost all of them have their headquarters at United Kingdom, United States and France, Poland

[106] Ibid.
[107] For details see Chapter II.
[108] Nighat dad, "Big Brother Is Curtailing Net Freedom in South Asia," *Aljazeera English Op-Ed*, January 11, 2014, Online Edition edition, sec. Opinion, http://www.aljazeera.com/indepth/opinion/2014/01/big-brother-curtailing-net-freedom-south-asia-20141544556701717.html.
[109] See details at Privacy International in cooperation with Centre for Internet and Society, "State of Surveillance: India," Summary Report, State of Surveillance (United Kingdom and India: Privacy International, March 2, 2016), available at https://www.privacyinternational.org/node/738.
[110] Maria Xynou, "The Surveillance Industry in India," NGO Websites, *The Surveillance Industry in India*, (March 2014), http://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf.

and so on and have maintained long durable relationship with military, intelligence, and law enforcement agencies, internet service providers, telecom industry and even with high profile individuals. However, it is important to mention that none of these mass surveillance programs or arrangements have been reviewed by 'any competent authorities such as the judiciary or parliamentary committees in the respective jurisdictions till today'[111] and also most of the cases bypass well-defined legal protections of multiple legal instruments of national legal system.[112] On closer inspection of contemporary legislative acts in Bangladesh, India and Pakistan suggests that a number of unspecified Lawful Interceptions and Monitoring (LIM) systems have been allowed by law and legality grounds are very often broadly phrased and left out for further interpretations.[113]

Landscape for Communication Surveillance Actors in South Asia

Established Bodies and Centers

In Bangladesh, India and Pakistan, all three countries have similar kind of public administration to deal communication surveillance, however, among different actors, government actors are overrated above all. Communication surveillance actors' appointments, engagements and inclinations processes are complex and very often it is confused with the role of cyber security actors- as surveillance is legally acceptable for 'national security' and cyber security' in every jurisdiction. In addition to national security and intelligence agencies under the Ministry of Defense and the Ministry of Home Affairs, the government departments such as BTRC, PTA and two Indian departments of Ministry of ICT are also involving in cyber security and overseeing the

[111] For details see Chapter III.
[112] See case of General Secretary Amar Singh of Samajwadi Party, for details see Chapter II & III.
[113] For examples in Bangladesh, Section 57 of Information and Communication Act 2006, Section 68B of Information Technology Act 2000 in India, Section 2 of the Fair Trial Act in Pakistan.

information section and regulating surveillance. For example, along with nine security and intelligence agencies in Bangladesh,[114] BTRC formed office under the Ministry of Post and Telecommunication by a special legislation, Bangladesh Telecommunication Regulation Act (BTR) Act-2001. The prime responsibility of BTRC is to facilitate the Ministry as an auxiliary organization and also administering telecommunication and ICT issues in Bangladesh. However, different news reports and human rights organizations concern also suggests that BTRC's technical team members regularly monitor internet and mobile communication of the internet users to help other security agencies to track perpetrators since the BTR Act 2001 allow lawful interception of mobile communication and cyber space. In addition to the prime law, the Telegraph Act 1885, the Wireless Telegraph Act 1933, and Information and Communication Act 2006 also have similar kind of provisions. It is also interesting that according to the section 30 (1) (f) BTRA 2001 one of the responsibility of the BTRA is to "ensure protection of privacy telecommunication." Moreover, in January 2012, BTRC set up Bangladesh Computer Security Incident Response Team (BD-CSIRT) which duties are to identify the sites, persons, or institutions engaged in harmful activities against the state society and political and religious beliefs using mobile phones, websites and different social networking sites and also advice to take or recommend penal action to the law enforcement agencies". Lastly, the Informational and Communication Technology Act-2006 empowers for government to appoint a controller who is empowered to direct any governmental agency to intercept any information transmitted through any computer resource, if he is satisfied

[114] The name of the Security agencies is National Security Intelligence (NSI), Directorate General of Forces Intelligence (DGFI), Special Branch of Police, Criminal Investigation Department, Army Intelligence, Naval Intelligence, Rapid Action Battalion (RAB) etc. However, all of them have number of allegations of violation of human rights irrespective of any political regimes.

that it is necessary or expedient to do so for several grounds including 'national security and 'public order'.[115]

Another neighboring country, Pakistan has similar disturbing legal and political development in recent years. Like Bangladesh Internet Exchange (BDIX), "Pakistan Internet Exchange- a communication system that keep most of the Pakistan's communication within Pakistan."[116] Along with government intelligence agency i.e. Inter Service Intelligence and Joint Signal Intelligence are primarily responsible organization to intercept, monitor internet activity and extended communication surveillance to their citizen. However, the Pakistan Telecommunications Authority (PTA) also joins hand time to time with different intelligence agencies and human rights defenders, journalist and bloggers have their serious aloofness due to their critical role in recent years.[117] It is important to note that PTA works under the Ministry of Information Technology and Telecommunication and very recently extended their responsibility to manage the Internet.[118]

As mentioned earlier, Indian key Government departments, namely Department of Telecommunication (DOT) and Department of Electronic, Information and Technology (DeitY) are regulating cyber surveillance, overseeing and ensuring cyber security in the telecommunication and internet space respectively. In addition to that both departments are also involving in sectorial licensing, formulating policy and regulating the Indian Registry for Internet Names and Numbers (IRINN). However, compare to Bangladesh's BTRC and Pakistan's PTA, the Telecom Regulatory

[115] Section 46 of the Informational Communication and Technology Act 2006 (Amendment 2013) in Bangladesh.
[116] Matthew Rice, "Tipping the Scales: Security and Surveillance in Pakistan | Privacy International," Special Report, Big Brother Project (London, United Kingdom: Privacy International, July 2015), https://www.privacyinternational.org/node/624.
[117] For details Digital Rights Foundation and Article 19, "Pakistan: New Cybercrime Bill Threatens the Rights to Privacy… · Article 19," NGO Websites, *Article 19*, (April 20, 2015), https://www.article19.org/resources.php/resource/37932/en/pakistan:-new-cybercrime-bill-threatens-the-rights-to-privacy-and-free-expression.
[118] Article 19, "Pakistan: Telecommunications (Re-Organization) Act," Legal Analysis (United Kingdom: Article 19, January 2012), https://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf.

Authority of India (TRAI) functions more independently and has maintain "transparency in exercise of its operations, which include monitoring licensing terms, complains and service quality".[119] It addition, the Telecom Regulatory Authority of India Act amended in 2000 and created Telecommunications Dispute Settlement and Appellate Tribunal. The Section 14 of the Act provides some quasi- judicial power and very recently TRAI criticized government departments not to create competitive environment among service providers and also not to respect net neutrality principles. It could argue that Indian telecom regulatory authority is much more independent from government undue influence compare to Bangladesh and Pakistan.

Emerging Bodies and Centers:

The South Asian governments are also in progression of constructing distinct and separate bodies and centers that would play key roles in communication surveillance and cyber security. For example, in the rise of illegal VOIP business, cybercrimes and cyber security threats, on 18 August, 2015, the BTRC made a proposal to Prime Minister Office (PMO) to form a central organization (in spite of existence of National Monitoring Centre) which will form "a holistic initiative to curb cyber threats by law enforcers, detective branches and security agencies".[120] It is quite clear that it will be made for stronger surveillance over the country's cyberspace and mobile networks. In addition, the Indian Central Government are in process of establishing similar kind of national center for cyber space and proposed name is National Cyber Coordination Center. Similarly, it will function as a new cyber security body to secure from cyber threats and cyber intelligence. In a public meeting, Pakistan's Police inspector general announced to open a new wing within police

[119] Section 11 (4), The Telecom Regulatory Authority of Indian Act, 1997. For details: Snehashish Ghosh, "The Telecom Regulatory Authority of India Act, 1997", The Centre for internet & society, March 15, 2013, http://cis-india.org/telecom/resources/trai-act-1997

[120] ibid.

by stating "police have no choice but to beef up efforts to monitor social media as many internet users in the country abuse the platform by issuing insensitive comments".[121]

However, the capacity of communication surveillance does not necessarily bound within governments agencies or bodies, it could be performed and develop in-house like in United Kingdom and United States by an individual who has access and technical expertise into this field. Apparently, there is an emerging commercial surveillance markets are evolving in South Asia. In absence data, lack of literature, and executive secrecy, this research failed to address the Wide-Area and Multiple-Sensor (WAMS) surveillance system, for example, video camera, radiation sensors, heat sensors, microphones and many more.

Modalities of South Asian Communication Surveillance Mechanisms in Practice

There are several kinds of surveillance technology could be per performed to monitor internet, mobile, fixed lines or intrusion kind of technology. Across South Asia, communication networks are under surveillance by lawful or unlawful surveillance practice by state apparatus irrespective of liberal or illiberal governments are in power which poses an array of challenges to human rights and their communities.

However, there are good number of tactics or models have played by the South Asian government, namely, centralized surveillance model of network traffic, packet inspection, and tactical surveillance and so on.[122] As mentioned earlier, investigative reports of PI and Citizen Lab's suggests that both Bangladesh and Pakistan are using of *Fin Fisher* server that was hosted at their premier network

[121] Dawn com | Imran Gabol, "Police Take down Offensive Anti-Minority Poster in Lahore after Outrage," December 11, 2015, http://www.dawn.com/news/1225696.

[122] See Details Matthew Rice, "Tipping the Scales: Security and Surveillance in Pakistan | Privacy International," Special Report, Big Brother Project (London, United Kingdom: Privacy International, July 2015), https://www.privacyinternational.org/node/624.

service. Later in 2012, major telecom companies agreed to grant the government access and real-time interception for BlackBerry users in India. In April 2013, India began implementing a Central Monitoring System (CMS) that allows the government to access all digital communications and telecommunications across the country.[123]

Through, different investigative reports it is also evident that all three countries actually have been using all possible methods to surveil over internet and intercept mobile communication. For instances in Bangladesh and Pakistan, centralized model of network traffic system is performed via controlling licensing regime.

The neighboring country India has used similar modalities of surveillance technology along with number of other methods. According to the operating licenses guidelines, "service providers are required to maintain all commercial records for a period of one year" and this includes call records, data traffic, location, callers' identity, cell number and so on.[124] In recent years more disturbing development has reported as well for artificial intelligence and robotics and such kind of software has developed by a private center. It has "ability to intercept and analyze internet traffic data".[125] There are number of interception technologies and national database technologies being used to monitor and intercept users' data in India. Similarly, in Pakistan number of tactical surveillance or intrusion technology (i.e. Malware) or packet inspection being used such as IMSI catcher, Fin Fisher on a targeted computer. As far as packet inspection concern, it has reported that Pakistan Government has bought number of 'Packet inspection' technology from western company which

[123] Nandakumar Indu, "Government Can Now Snoop on Your SMSs, Online Chats - Times of India," *The Times of India*, May 7, 2013, Online Edition edition, sec. Tech News, http://timesofindia.indiatimes.com/tech/tech-news/Government-can-now-snoop-on-your-SMSs-online-chats/articleshow/19932484.cms.

[124] See details at Chapter II

[125] See details "Government to Launch Internet Spy System 'Netra' Soon," *The Economic Times*, June 6, 2014, http://economictimes.indiatimes.com//articleshow/28440192.cms.

are able to search for particular key words in targeted computer or target's email, censoring online contents or searching for signature and also distance control computer.[126]

Communication Surveillance under International Human Rights Frameworks

Since the concept of communication surveillance is still evolving under international law, therefore, it argues that there is no specific international human rights or humanitarian law exists to regulate malpractices of communication surveillance but all surveillance mechanism must need to fulfil minimum requirements and standers under international human rights frameworks. However, there are number of international and regional human right instruments protects the right to privacy and right to freedom of opinion and expression against the backdrops of targeted and mass surveillance. For example, Article 17 of the International Convention on Civil and Political Rights (ICCPR) recognizes that "no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence". Correspondingly, Article 12 of the Universal Declaration on Human Rights (UDHR), Article 8 of the European Convention on Human Rights, Article 21 of the Arab Charter of Human Rights and many others Conventions also recognizes right to privacy. Since right to privacy as a gateway to right to freedom of expression and association, Article 19 of ICCPR also commits State to ensure the protection of the right to freedom of opinion and expression and Article 22 of ICCPR ensures right to freedom of assembly and association. Although the interrelation and interdependence among different rights such as right to life, freedom of expression, freedom of assembly and right to privacy, yet to consider comprehensively by the international human rights frameworks.[127] In addition, there are good numbers of regional

[126] Matthew Rice, "Tipping the Scales: Security and Surveillance in Pakistan | Privacy International," Special Report, Big Brother Project (London, United Kingdom: Privacy International, July 2015), https://www.privacyinternational.org/node/624.

[127] See details at "UN General Assembly Adopts Resolution on Privacy and Surveillance," *Intellectual Property Watch*, January 8, 2014, http://www.ip-watch.org/2014/01/08/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/.

Charters and Conventions recognized right to freedom of expression such as Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Article 9 of the African Charter on Human and peoples' rights, Article 10 of European Convention on Human Right, and Article 13 of the American Convention on Human Rights. As far as communication surveillance concerns, UN Human Rights Committee's interpretation via General Comment 16 (8) may relevant to understand the rights to privacy and right to freedom of expression. It has clarified that any lawful interference or inception to private communication via surveillance must need to be lawful and recognizes by a legislation that 'specifics in detail the precise circumstances in which such interferences may be permitted'.[128] Therefore, it is clear that communication surveillance allowed under International law in exceptional circumstances but it need to be occur 'only by the authority designated under the law, and on a case-by-case basis'.[129] Since the essence of human rights frameworks is not subject to limitations, therefore, these permissible limitations should be evaluated with three per tests which must be provided by the law, law should pursues legitimate aim and legitimate aim should be proportionate and necessary in a democratic society.[130] In addition, UN Special Rapporteur reaffirms that 'communications surveillance should be regarded as a highly intrusive act' and 'legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority'.

Moreover, it is evident that the Internet and other new communication technologies are rapidly changing how human rights communities or individuals seek, receive and impart information, and how the media works. As advancement of information and communication technology enhanced

[128] UN Human Rights General Committee, General Comment 16 (1988), Un Doc. HRI/GEN/1/REV.9(VOL 1).
[129] ibid.
[130] ICCPR General Comment 34.

global democratic participation and freedom of expression and free flow of information, the United Nation General Assembly recognized the importance of protecting civil and political rights online and urged member states and policy makers to review their practices, legislations and procedures to comply with these fundamental rights. It is well recognized reality that International human rights frameworks have equivalently slow like nation states to respond the human rights implications of the internet and new technologies on communication surveillance and interception to communication data.[131]

On December 18, 2013, the General Assembly adopted resolution 68/167[132] that conferred deep concerns regarding online surveillance and data interception and its impact on human rights. By reaffirming the UDHR Article 12[133] and the International Covenant on Civil and Political Rights Article 17,[134] this resolution recognized the importance of respecting the freedom to acquire, receive and disseminate information without wrongful and unauthorized intervention. It also emphasized that arbitrary and unlawful surveillance and intercepting and collecting of personal data violates the rights to privacy and freedom of expression and have a negative impact specially when carried on a mass scale or when it encompasses extraterritorial surveillance.

[131] See details of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". *Office of the United Nations High Commissioner for Human Rights*. United Nation, accessed March 26, 2016, Available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[132] United Nations General Assembly Adopts "Resolution On Privacy and Surveillance," *Intellectual Property Watch*, January 8, 2014, http://www.ip-watch.org/2014/01/08/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/.

[133] Article 12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks". Universal Declaration of Human Rights accessed March 26, 2016 http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

[134] Article 17 (1) states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and Article 17 (2) states that "everyone has the right to the protection of the law against such interference or attacks". International Covenant on Civil and Political Rights, accessed March 26, 2016, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

Furthermore, the General Assembly welcomed the report of Frank La Ru, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[135] submitted to the Human Rights Council on April 17th, 2013 that discussed concerns on the implication of state surveillance on human, predominantly on rights to privacy and freedom of expression and assembly.

Moreover, in March 2014, the United Nations Human Rights Council convened a Panel discussion on the right of privacy in the digital age. In the report submitted in pursuant to Human Rights Council (HRC) decision 25/117[136] by the Office of the United Nations High Commissioner for Human Rights (OHCHR), it reaffirmed the promotion and protection of the rights of privacy in the digital age. Indeed, after the revelation of Edward Snowden, leading academics, activists, lawyers and online community members were "jumping off point for the drafting of the international principles on the application of human rights to communication surveillance that explain how international human rights law applies in the context of communication surveillance".[137]

In addition, the OHCHR's report also underlines the need to expand the discussions and study of new surveillance modalities and its impact on democratic constitutionalism and human rights movements. Legislations in South Asia didn't keep up with the latest advancement of technology, if so, in most cases legal provisions are vague and sometime ill-defined and hence, repressive governments seek to justify the use of communication surveillance with old or newly enacted legislative frameworks without considering the violations of international human rights frameworks.

[135] See details of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". *Office of the United Nations High Commissioner for Human Rights*. United Nation, accessed March 26, 2016, Available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[136] Stacy Dry- Lara, "The Right to Privacy in the Digital Age," *FAWCO*, accessed March 26, 2016, https://www.fawco.org/fawco-the-un/what-we-do/current-initiatives/human-rights/human-rights-council/hrc-27-blog/3149-privacy-on-the-right-to-privacy-in-the-digital-age. For detail reporting Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39.

[137] For more details about surveillance consultation process, see Privacy International's report, towards Principles on Communication Surveillance, October 2012.

It has evident from the discussion of Chapter I and II that advancement of cyber technologies used by South Asian governments to control the lives of their own citizens whereas digital rights should be protected as it is protected in offline. Also, International Non-Governmental Organizations (INGOs) like Privacy International, Frontline Defenders and Access noted that when online privacy under threat, journalists, bloggers and human rights defenders specially those living under suppressive regimes like in South Asia, have been deprived from the right to communicate securely, anonymously and freely.

Chapter 3
Comparative Analysis of the South Asian Communication Law and Policy

It is evident from previous discussions that State actors of Bangladesh, India, and Pakistan, have engaged in debate of communication surveillance mechanisms to control cybercrimes and digital dissidents through problematic legal frameworks. After several terrorist attacks in Bangladesh, India and Pakistan, the decade after 9/11,[138] all the three countries enacted or at least review their respective national security and cyber laws and policies to intercept and launch mass surveillance in ICT. It is also evident that those laws and policies undermines human rights in a digital context. It is arguably that justification of restrictive legislations or administrative mechanisms of lawful surveillance, does not necessarily end unauthorized and illegal surveillance practices. Conversely, those legal provisions and policy recommendations related to greater control over internet, gradually, encroach upon the right to privacy of human rights defenders, bloggers, and journalists along with other fundamental rights in the region. It is important to remember that all corresponding countries within realm of this research incorporated the constitutional provisions relating to freedom of expression or press freedom or even right to privacy in their constitutions very loosely which are primarily targets to offline. However, United Nations Human Rights Council's (UNHRC) resolution 20/8 emphasis that 'the same rights should apply online as offline'.[139] Moreover, the mere declaration from hard international law or human rights

[138] For examples, nationwide bombing on 17 August 2005 by *Jamatul Muzahidin* in Bangladesh, Mumbai Attacks in 2008 in India and Peshawar School Attacks in 2014 in Pakistan. For details Md Rezaur Rahman, "Mapping Trends of and Counter Responses to 'Terrorism' in Asia after 9/11: Analyzing the Impact of Anti-Terrorism Laws and Policies." (MA Thesis, Sungkonghow University, 2012), Sungkonghoe University library.

[139] United Nations Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet" (United Nation, July 16, 2012), https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

frameworks or soft international law like United Nations Resolution such as 20/8, does not automatically enforce or change the ground reality in national contexts. Therefore, in absence of strong legal footing or legal provisions of right to internet privacy and freedom of expression online into laws and policies, the HRDs, journalists and bloggers most cases take defense on the basis of the case laws. Therefore, this chapter efforts to discuss the legal and regulatory landscapes of communication surveillance as well as constitutional and ordinary legal protections of the right to privacy, and freedom of expression relevant case laws and its evolution as judicial responses due to the increases pervasiveness of surveillance in the region.

The South Asian legal landscape of offline surveillance is often colonial archaic but the legal regimes governing information and communication sector in Bangladesh, India and Pakistan comprises of two sets of laws and policies: first, laws and policies with regard to mobile communication; and second, those in relation to the regulation of cyberspace; thirdly, there are some special laws and policies (such as Anti-Terrorism Act-2009 Bangladesh, the Unlawful Activities Prevention Act-1967 of India or Anti-Terrorism Act 2015 of Pakistan) exists which addresses national security administrations but some of the legal provisions of these laws attempts to regulate cyberspace and telecommunication sector. The first part discusses the legal and policy landscape of communication surveillance and right to privacy in the context of the mass surveillance, alternatively, overall protection mechanism of the freedom of expression and privacy.

Analyzing the Laws and Policies of Communication Surveillance and Rights to privacy in South Asia

Inadequate Constitutional Provisions for New Technologies

The constitutional development and popular constitutional history of South Asia has lots of similarities to ensure the fundamental rights in the Constitution. In Bangladesh, freedom of thought, conscience, speech and press guarantees according to the Constitution of People's

Republic of Bangladesh, Article 39 (1) guarantees the freedom of thought, and conscience and Article 39 (2) guarantees the freedom of speech and expression but at the same time restrictions imposed by law. In addition, the Article 43 of the Bangladesh Constitution guarantees the privacy of home and correspondence and communication and does not categorically guarantees 'right to privacy'. It provides that "every citizen shall have the right to…privacy of his correspondence and other means of communications." Several other provisions of the Constitution such as Articles 11, 31 and 32 –can constructively be interpreted to extend the ambit of the right to privacy. Like Bangladesh, the Constitution of India also guarantees citizens' fundamental rights to freedom of expression and speech under Article 19(1) (a) and have not specifically guarantee a 'right to privacy'. Moreover, there are number of verdicts suggests to read right to privacy with other Constitutional rights, for example, R Rajgopal v. State of Tamil Nadu,[140] pronounced that right to privacy has to be read with right to life guaranteed by Article 21 of the Constitution. In 1962, the first court case appeared in the supreme court of India, recognized the right to privacy as a constitutional principle in the case of Kharak Singh v. Union of India.[141] The court stated "it is true that our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty".[142] There are number of judgments also pronounced by stating that the right to privacy can be restricted if there is a compelling state interest to be served.[143] Unlikely to Bangladesh and India Constitutions, Pakistan Constitution provides more weights to the right to privacy. Article 14 (1) of the Constitution of Islamic Republic of Pakistan, 1973 established that "the dignity of man and subject to law, the privacy of home shall

[140] AIR 1995 SC 264
[141] 1963 AIR 1295, 1964 SCR (1) 332
[142] For details analysis see at "Surveillance and the Indian Constitution - Part 1: Foundations," *The Centre for Internet and Society*, accessed March 30, 2016, http://cis-india.org/internet-governance/blog/surveillance-and-the-indian-consitution-part-1.
[143] Govind v State of M.P.

be inviolable". Similarly, Article 19 of the Constitution of Pakistan confirms the freedom of speech with reasonable restrictions such as public morals, public order and national security.

Through realization of UNHRC resolution no. 20/8, online expression or online privacy supposed to be protected under the national constitution. The wording 'other means of communications' from the perspective of individual netizens or human rights defenders, it is tempting to claim that their right to internet privacy be securely safeguarded by the state, nonetheless, from the perspective of state, it is, however, not so easy to recognize this right in an absolute and unconditional form unless the policymakers take liberalism as an end in itself. In both rights, namely, freedom of expression or right to privacy, there are different values – e.g., national security, public order, morality, public policy etc. poses reasonable restrictions- that a state should also safeguards and it is undeniable that sometimes these values conflict with the right to privacy and freedom of expression. Therefore, right to internet privacy or right to online expression better to understand as contextual constructs, as opposed to abstract concepts, that negotiate with conflicting values.

Major Communication Laws and Communication Surveillance in South Asia

ICT related principal sectoral laws are (a) the Information and Communication Technology Act, 2006 (amended in 2009 and 2013) and (b) the Bangladesh Telecommunication Regulation Act, 2001 (amended in 2006 and 2010). Though neither of them defines the term 'privacy' but they contain several norms in furtherance of the right to internet privacy such as Section 63 of ICT Act.[144] At the same time, these laws contain provisions that allow communication surveillance and the infringement of digital rights in cases of 'national security', 'public order' and so on.

[144] Section 63 states the punishment for disclosure of confidentiality and privacy of any correspondence.

The ICT-2006 Act criminalises several acts or omission that are likely to violate the privacy of computer system. These include damage to computer or computer system,[145] tampering with computer source code[146] and hacking with computer system.[147] Most problematic provisions in regards to communication surveillance are Section 46 and Section 57 of ICT Act- 2006. Section 46 of the ICT Act advocates for appointment of a control within Bangladesh Telecommunication Regulatory Commission by stating that "a controller who is empowered to direct any governmental agency to intercept any information transmitted through any computer resource, if he is satisfied that it is necessary or expedient to do so for several grounds including 'national security' and 'public order'."[148] In addition, Section 57 of the ICT Act, 2006 provides for a "maximum punishment of up to 10 years of imprisonment or a maximum fine of Taka (Tk) 10,000,000, or both" in case of any cybercrimes.

In addition, Section 97A, the BTRA-2001 Act states that in the interests of 'national security' and 'public order' -the government may empower any officer belonging to intelligence services, national security agencies, investigating agencies or law enforcement forces -to intercept, record or collect any data transmitted through telecommunication. In response to that in 2008 the Government of Bangladesh established the National Monitoring Centre (NMC) for exercising these powers. It is made up of representatives from agencies like Director General of Forces International, National Security Intelligence, Security Branch of Police, Rapid Action Battalion, Special Security Forces (SBP) etc. Such legal recognition of establishments of NMC came after the nationwide bomb blasts on 17 August, 2015. Hence, any law enforcers along with the help of

[145] See Section 54 of ICT Act 2006.
[146] See Section 55 of ICT Act 2006.
[147] See Section 56 of ICT ACT 2006.
[148] Section 46 of ICT Act 2006

NMC can conduct searches based on any suspicion resulting from the monitoring subscribers or as a result of any complaints.

According to the said Act, some amendments was made in the earlier Bangladesh Telecommunication Act 2001. Section 97A has been inserted in addition to section 97 of the act which states that for the security of the state and public tranquility the Government can empower any of its agencies to record, prevent and collect information regarding shall be bound to assist the government communication made by any person through telephone. This section also states that the Government can order any service provider for assistance and in that case the service provider shall bound to assist the Government. Section 97B of the Act states that any information collected under section 97A shall be admissible under the Evidence Act 1872 and section 97C states about punishment if anybody does not comply with the order under section 97A. Therefore, present situation is that the Government (Ministry of Home Affairs) is entitled to tap any telephone line of any person if so desires without any prior warrant or order of any court and collect information which can be used as evidence at court of law.

India, like the rest of countries in the region, has adopted Information Technology Act- 2000 and encouraged surveillance technologies as an acceptable conduct by law. The main regulatory bodies for the ICT sector in India are the Department of Electronics and Information Technology (DeitY) the Department of Telecommunications (DoT) and the Telecom Regulatory Authority of India (TRAI), an independent regulator. These are the three regulatory bodies are responsible for managing the telecommunication sector, mobile service providers and internet licensing. The Telegraph Act (1885), empowers government by Section 5 to intercept messages for reasons deemed related to national security and the IT Act (Information Technology Act, 2000 that

regulates the interception, monitoring and decrypting of digital communication, specifically Section 66, 67 and 69 of IT Act, legalize communication surveillance to protect national security and allow for investigation for any offense online. Telephone tapping, and cellular phones interception doesn't need a court order and can be extended over 180 days. Third part telecommunication providers are obliged by law to intercept, monitor and decrypt communication and are subject to fines, jail and license lose in cases of con-compliance with interception orders.

The problem of terrorism has always haunted Pakistan and pushed it to enact more and more laws as advances in technologies had taken place. One area would be the admissibility of evidence in courts in cases that were clearly linked to terrorists but were acquitted of charges as the evidence were found in-admissible in court. To handle the issue of collecting admissible evidence using modern techniques, a law called the Fair Trial Act, FTA was passed in 2013. The act drastically amended the law on surveillance and data interception to power state officials with new procedures for collecting admissible evidence. Moreover, the interception and surveillance gained more widespread in Pakistan since the creation of the Pakistan Internet Exchange that allows internet traffic to pass through a single core gateway easing the way to state actors to intercept and monitor online communication.

In short, digital surveillance practices and data interception have been justified mainly due to terrorist attacks by non-state actors in Pakistan, actions have been made by the state to legalize these activities. In 2013, the government has passed a legislation law named the Investigative for Fair Trial Act also referred to (FTA 2013) that gives jurisdiction powers to police and intelligence agencies to collect and intercept communication and information mainly "motivated by the necessity to investigate, contain

and even pre-empt offences related to terrorism"[149]. It also allows these agencies to issue warrants to monitor communications "to neutralize and prevent [a] threat or any attempt to carry out scheduled offences"[150]. Mir and Niazi argues that the law provides intelligence entities power within the legal framework to violate human rights to privacy and freedom of expression. It is argued that in the case of someone being suspected and a warrant have been issued, the citizen has no way to know that a warrant has been placed and hence their information has been intercepted, collected and scrutinized and their privacy have been intruded. If a citizens' physical equipment has been seized, the law doesn't provide any regulations on how these data will be stored, processed and for how long.

Many existing laws in Pakistan have been used to restrict freedom of expression. The Penal Code section 295 has been invoked to file blasphemy cases against each other in Pakistan. Although many cases have been filed for reprisals purposes, some of these cases where charged against online users. Both 2014 Defamation Act and Section 124 of the Penal Code have been used in court cases again online freedom of expression and the usage of certain "words" and "visible representation" in the online domain.

In 2015, the cybersecurity bill, or an anti-cybercrime law, has been drafted to define some of the cybercrimes and introduced certain safeguards to the accused in the context of malpractices by law enforcement agencies in cybercrime investigations. Critics of this bill have argued that this law lack clear definitions in accordance with international standards that might grant these agencies the green light for unrestricted mass surveillance acts. In addition, despite the discussion of this bill was characterized as a public hearing, only a handful of civil society stakeholders were invited

[149] Waqqas Mir and Niazi Hassan, "Surveillance Laws & Practices in Pakistan: History, Current Legislation & Lessons from the United Kingdom," *Online Publication*, n.d., 22–23.

[150] See details of the Section 2 of the Fair Trial Act 2013, *The Gazette of Pakistan*, February 22, 2013, accesses on 26 March 2016, available at http://bit.ly/18esYjq.

to the discussion and many members of the committee used to approve this draft had said that they didn't read the approved draft and no major changes have been made after the discussion.

Largely, there are number of backdates colonial criminal laws also permits communication surveillance such Pakistan Telegraph Act-1885, Code of Criminal Procedures- 1898 in Bangladesh and so on. On the other hand, in the name of cyber security all three countries are in process to pass laws such as Cyber Security Bill in Bangladesh or National Encryption Act in India. Most of the laws are attempting to criminalize the use of encryption or brought restriction on encryption and online anonymity. These are also vague and broad offenses and ordering mass surveillance. However, the lists of the problematic cyber laws are not exhaustive in this part but number of ways, they all violates international standards and principles of communication surveillance.

Avowed Communication Policies and Guidelines in South Asia

Like India and Pakistan, Bangladesh doesn't have any particular privacy legislation or data protection legislation for general application. While, the BTRA- 2001, section 30(1)(f) states that one of the responsibilities of the BTRC is to 'ensure protection of the privacy of telecommunication' and also Section 63 of ICT Act provides clear mandate to the operators to strictly maintain their clients' privacy.[151] However, there are number of reasons, it is quite impossible for internet service providers or mobile operators to maintain clients' privacy. For instance, in Bangladesh, the generic form of Operator License for Broadband Wireless Access (BWA) Services (BWA license) and the Amended Regulatory and Licensing Guidelines for Internet Protocol Telephony Service Provider License (IPT guidelines) provide that "the licensee shall maintain confidentiality in respect of all information provided by the subscriber".[152] The data

[151] See Section 30 of Bangladesh Telecommunication Regulation Act- 2001.

[152] Bangladesh Telecommunication Regulatory Commission, "Regulatory and Licensing Guidelines for Issuing License," Guidelines (Dhaka, Bangladesh: BTRC, August 6, 2008), http://lirneasia.net/wp-content/uploads/2008/08/bwa_guidelines1.pdf.

protection standard is not applicable if the disclosure is deemed 'necessary' by the BTRC or other national security and law enforcement agencies and most importantly, this criterion does not speak of any 'purpose' or 'necessity' for which confidentiality of the data provided by the subscriber may be compromised. In addition, a BWA licensee is under an obligation to provide the National Monitoring Centre (NMC)[153] with necessary hardware and software needed for on-line and off-line monitoring of every exchange, to ensure on-line listening capability of call content and on-line viewing of content, and to store bulk intercepted products. The licensee should also be capable of sorting and sending data content to the NMC on the basis of the criteria including but not limited to the followings: (a) source IP address, (b) destination IP address, (c) e-mail address, (d) MAC address, (e) web address, (f) catchy words in email, ftp, chatting, and (g) type of application. The generic form of Operator License for International Internet Gateway (IIG) Services (IIG license) and the IPT Guidelines impose similar obligations on IIG licensee and IPT licensee respectively. This arrangement of interception is dangerously broad in scope, combing targeted as well as centralized strategic/massive interception, targeted interception in contemporary time amounts to almost a totalitarian control on individual. Such kind of centralized strategic interception can lead to an unintended infringement of the right to privacy and of course this dangerously broad power rests on the discretion of the NMC. Similarly, Indian ISPs and mobile operators are also required to follow number of guidelines such as License Agreement for Provisions of Internet Service, Unified Access Service (UAS) and Telecom Service Providers Guidelines. According to these guidelines, ISPs require to keep identification and registration of subscribers such as for telephonic data, call party lists, location, telephone numbers of call forwarding, and data records of failed call and so on. In the case of cyber space monitoring internet gateway and exchange of internet users

[153] See details at Chapter II

also compulsory. In addition, according to the section 84A of the Indian Information Technology Act government can set up a national office to set up standard for encryption and there is one National Encryption Policy is open for public comment which empower government for further installment of algorithms based surveillance.[154]

In addition, cyber cafes are playing crucial role in Bangladesh, India and Pakistan, it important to recognize that in all three countries ISPs related provisions and guidelines also include cyber cafes as semi-public nature of ISPs. Therefore, as per guidelines requirements, they all have to act within legal boundaries. Although, ISPs related guidelines or policies in Bangladesh and Pakistan are not categorically talks about cyber cafes. On the other hand, Section 4(2) Indian Information Technology Intermediary Guidelines Rules requires that "the Cyber Cafe shall keep a record of the user identification document by either storing a photocopy or a scanned copy of the document duly authenticated by the user and authorized representative of cyber cafe. Such record shall be securely maintained for a period of at least one year".[155]

Case Laws and Judicial Responses

It is undeniable fact under international law, judicial oversights plays a significant role to stop or control mass surveillance practices and covert operation of surveillance.[156] Compare to neighboring countries Bangladesh and Pakistan, Indian judiciary played more progressive role in protecting internet privacy against the backdrops of mass surveillance. Therefore, there are number of case laws being developed. In 1996, People's Union for Civil Liberties v. Union of India, "laid

[154] See details at thirteen Necessary and Proportionate Principles of Communication Surveillance.
[155] See details Section 3 (4) of the Information Technology Intermediary Guidelines Rules.
[156] For example, Digital Rights Ireland v. Ireland & org. T. J. McIntyre, "Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2015), http://papers.ssrn.com/abstract=2694512.

down guidelines which form the backbone for checks and balances in interception provisions"[157] and other cases such as Selvi and others v. State of Karnataka and others[158], Petronet LNG LTD v. Indian Petro Group[159] and Hyderabad and another v. Canara Bank and another[160] extended the right to freedom expression, freedom of movement, and personal liberty as the fundamental rights which gives rise to the right to privacy.

On the one hand, the apex court of the Pakistan has not yet got any notable opportunity to offer such progressive interpretation. On the other hand, the Supreme Court of Bangladesh have failled two notable opportunities to offer a human rights based interpretation in the pervasiveness of communication surveillance, however in both cases those were missed opportunity. On 06 June, 2010, a group of rights activists filed a writ petition (4719 of 2010),[161] and challenged the constitutionality of Section 46 and 57 of the Information and Communications Technology Act, 2006 (Act 39 of 2006) against the Ministry of Information, Communication and Technology and Bangladesh Telecommunication Regulatory Commission. The petitioners argued that the impugned provisions are unconstitutional in as much as they are vague and uncertain in their terms, and granted unfettered powers to intercept and monitor cyber space based on subjective satisfaction, which violates the fundamental rights guaranteed under Articles 39 and 43 of the Constitution. Later, on 26 July, 2010, a bench of High Court Division comprising Mr. Justice Md. Imman Ali and Mr. Justice Obaidul Hasan directed the Ministry of Information Communication Technology along with BTRC to show cause as to why Sections 46 and 57 the ICT Act 2006, should not be held to be *ultra vires* of the Constitution, and in violation of fundamental rights to

[157] Writ Petition (civil) 490 of 2002; Writ Petition (civil) 509 of 2002 and Writ Petition (civil) 515 of 2002
[158] Criminal appeal no. 1267 of 2004, Supreme Court of India,
[159] CS (OS) No.1102/2006
[160] Appeal (civil) 6350-6374 of 1997
[161] As Facebook access was restored at 11pm on 5 June, 2010, on the day before the writ was filed, the petitioners did not pursue the issue of the ban in the hearing. However, they continued their case against the provisions of ICT Act and prayed the Court to strike down these provisions as being unconstitutional.

freedom of expression and right to privacy. The Rule has been made returnable in four weeks but the concern parties didn't conform to the High court direction till today and even the High Court Division didn't pursue through the Contempt of Court Act-1926. Analogously, on May 18, 2006, immediately after the enactment of BTR Act, a leading rights organization *Odhikar*, filed a writ petition 4453 of 2006 under Article 102 of the Constitution against the Government of Bangladesh and claimed that the indiscriminate power to tap any telephone line without any warrant or order from court is beyond the limit of the 'reasonableness' of law therefore the section 97A of Bangladesh Telecommunication Regulation Act -2006 is *ultra vires* to Article 43 which guarantees communication privacy. Since amendment of BTRA-2006 enacted, 'in accordance with law in force at relevant time' therefore, a bench of the High Court Division quashed the petition and declared the BTRA is constitutional.[162]

Problems and Gaps: Thus Human Rights Based Approach Essential to Communication Surveillance in South Asia

It is quite clear from the previous discussion that communication surveillance paradigm violates the right to freedom of expression and right to privacy in South Asia. However, there is an increasing flow of narratives against communication surveillance in South Asia but resistance always stakes between of two different essentially contested concepts, namely cyber security and digital rights. In the defense of 'national security exception' and cyber security, all the three countries have attempted to present new cyber related laws and policies from 2013 to end of 2015. In addition to available comunicaiton laws and policies, governments are also using colonial hangover laws to surveil dissident voices or human rights defenders and online activists, limiting access or punishing internet speech. It also demonstrates that national constitution and other

[162] Opinion of Justice Kemaluddin Hossain in Mofizur Rahmna vs. Governmetn of Bangladesh, 34 DLR (AD) 321.

communication related laws and policies do not necessarily legalize or recognize protection of right to privacy and free expression protections in regards to cyber surveillance. Therefore, in this final part of this paper attempts to explore the problems and gaps in exercise of communication surveillance and at the end it suggests to adopt a human rights based approach to South Asian states, so that all three nascent polities effectively comply with international standards.

In South Asia, it is evident that governments have used ill-defined and broad definition of cybercrime to invest more in its cybersecurity arms and surveillance technologies. The extent of unauthorized access and collection of data is very extensive. In Bangladesh, according to a report published by Freedom house in 2015,[163] while the government allows anonymous access to the internet with no need for websites and bloggers to register and provide personal information. At the same time, it has approved some laws that allows the government to intercept voice and data communication of individuals and organizations without a judicial oversights.[164] Even in 2014, the government went ahead and asked Facebook to provide it with information about a number of their users.[165] Not to mention that it has blocked a number of mobile communication application like Viber without a justified reason. It is arguable that according to Article 43 of the country's constitution, Bangladesh recognizes its citizens' right to privacy and any kind of correspondence. In absence of privacy and data protection law in Bangladesh, leaves peoples' communication and information sharing vulnerable to government surveillance and data interception systems. On the other hand in Bangladesh and Pakistan, censorship and filtration of content related to religious issues or offending state leaders is also widely used and surveillance prominently targeting online activists, bloggers. For examples, four bloggers of

[163] Sanja Kelly, et al., "Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015," Human Rights Report (New York: Freedom House, October 2015), https://freedomhouse.org/report/freedom-net/freedom-net-2015.
[164] Aby Saieed Khan, "Bangladesh Telecommunication (Amended) Act, 2006," in *Internet Freedom in South Asia* (Third South Asian Meeting on the Internet and Freedom of Expression, Dhaka, Bangladesh, 2013).
[165] Tribune Online Report, "Bangladesh Sought Data on 17 Facebook Users | Dhaka Tribune," *The Dhaka Tribune*, November 5, 2014, Online Edition, http://www.dhakatribune.com/bangladesh/2014/nov/05/bangladesh-sought-data-17-facebook-users.

Bangladesh have been arrested and the owners of their hosts have been requested to close their sites without showing any court warrant.[166]

On the other hand, India has been actively involved in surveillance activities that is resulted in content censorship of social media on the basis of number of anti-terrorism acts. It was reported that Facebook along with other social media platforms has been contacted by the Indian government to remove content that was allegedly violates local laws. In addition, artificial intelligence programs were developed to scrutinize content of social media, blogs, mobile and data communication in search for words that attributed to be threats of violence or terrorism. [167] India, in contrary to other mainstream surveillance and data interception programs adopted by law and administratively that allows law enforcers to contact internet and communication service providers to intercept communication. It is also equally disturbing that all the three states had developed a Central Monitoring System (CMS)[168] that allows the government to store intercepted data locally and in regional databases. This system intercept, analyze and filter voice, SMS, video, GSM and 3G network communication in an automated process that provides the government with a centralized access of all intercepted communication and data bypassing service providers.

Again on the grounds of counter terrorism and fighting crimes, Bangladesh, India, Pakistani intelligence agencies and police force has been expanding their surveillance and monitoring activities over the years and even pressuring the governments and officials to expedite location tracking. According to an investigative report by Privacy International "Mass network surveillance has been in

[166] Rezwan Islam, "Bangladesh Authorities Go After Bloggers, Claim They Are 'Anti-Muslim' · Global Voices," Human Right Community, *Global Voices*, (April 1, 2013), https://globalvoices.org/2013/04/01/bangladesh-authorities-go-after-anti-muslim-bloggers/.

[167] IFSEC International, "Internet Surveillance Picks up Speed in India," Online Newspaper, *IFSEC Global*, (January 1, 2014), http://www.ifsecglobal.com/internet-surveillance-picks-speed-india/.

[168] Maria Xynou, "Big Democracy, Big Surveillance: India's Surveillance State," Community, *open Democracy*, (April 16, 2015), http://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state.

place in Pakistan since at least 2005," using technology obtained "from both domestic and foreign surveillance companies, including Alcatel, Ericsson, Huawei, SS8 and Utimaco".[169] Fin Fisher was also found to have traces in Bangladesh and Pakistan. While it was not evident that the government of Pakistan or Bangladesh was aware of Fin Fisher operation within its jurisdiction, Hackers in 2014 managed to obtain documents that link to Fin Fisher[170]. In 2015 in Bangladesh, hackers managed to maintain similar documents from an Italian surveillance system that are linked private sector actors. Moreover, the government sought to gain access to older versions of mobiles that has a wide use among citizens.[171]

Internet service providers and telecommunication companies are no different from many other countries in the world where all SIM cards needs to be verified and registered against a national service database before the SIM card is being activated. After the terrorist attacks that killed 150 students in Pakistan in 2014 and bloggers killing in Bangladesh in 2015, biometric verification and registration of SIM cards had become mandatory features.[172] All the problematic laws such as ICT Act in Bangladesh, IT Act in India, and FTA 2013 of Pakistan were also criticized by digital rights groups that issued a whitepapers analyzing the provisions of the respective laws that violates the constitution and International law. Surveillance over the Social media is not also uncommon and Social media platforms like Facebook and Twitter have been constantly asked to remove certain content by the South Asian governments. The YouTube have been blocked in Pakistan since 2012 along with other encryption and

[169] Matthew Rice, "Tipping the Scales: Security and Surveillance in Pakistan | Privacy International," Special Report, Big Borther Project (London, United Kingdom: Privacy International, July 2015), https://www.privacyinternational.org/node/624.
[170] Sohali Abid, "Massive Leak Opens New Investigation of Fin Fisher Surveillance Tools in Pakistan," Community, *Global Voices Advocacy*, (August 22, 2014), https://advox.globalvoices.org/2014/08/22/massive-leak-opens-new-investigation-of-finfisher-surveillance-tools-in-pakistan/.
[171] Bolo Bhi, "Hacking Team in Pakistan - Bolo Bhi," NGO Websites, (July 5, 2015), http://bolobhi.org/hacking-team-in-pakistan/.
[172] Bilal Sarwari, "SIM Activation New Procedure-*Pak Telecom,* (September 3, 2010, http://bit.ly/pqCKJ9

virtual private networks (VPNs) that were used to overcome this restriction were also blocked in 2014.[173]

The enactment of the repressive laws and policies suggests that the South Asian Human Rights Defenders, journalists, and bloggers inputs and participation in ICT sectors to ensure right to internet privacy, freedom of expression online or offline, personal data protection are not highly encouraged. On the other hand, it is also evident that government policies and initiatives do not provide much opportunity to engage and ensure a rights based approach to heighten internet freedom or digital rights. It has found throughout the research process that human right based organizations and stakeholders in South Asia have not encouraged to conduct an in-depth research against problematic practices of communication surveillance and their own challenges or impacts on their human rights movements, rather it shows that they are tending to remain silent, perhaps due to physical and physiological risk and complexity of the issues. In spite of such barriers, very few civil society groups have been challenging at court or campaigning for the abolition or amendment of repressive legal provisions in different laws and policies in South Asia, such as Section 46 and 57 of the Information and Communication Technology Act (amend 2009 and 2013) - 2006 in Bangladesh, Section 66, 67, and 69 of the Information Technology Act-2000 in India and the Cyber Security Act (Draft) - 2014 in Pakistan. Like elsewhere, there is a long trends exists in South Asia that legitimate civil rights movements or

[173] The Express Tribune "Creeping Censorship: Spotflux Claims Its Service Is Being 'Actively Blocked' in Pakistan - The Express Tribune," January 28, 2014, Online Edition edition, sec. Web desk, http://tribune.com.pk/story/664341/creeping-censorship-spotflux-claims-its-service-is-being-actively-blocked-in-pakistan/.

protests against injustices are being criminalized as 'anti national'[174] or stigmatized as 'infidel',[175] political dissidents labeled as 'terrorists'[176], and online activists are being detained[177] and netizens faced judicial harassment.[178] In addition, legitimate human right activism in the exercise of freedoms of expression and freedom of assembly, and association are severely restricted in the name of 'national security',[179] public order and public moral. Discrimination against religious based politics[180] and racial profiling became rampant[181], even high profile and vocal human rights defenders phone calls, e-mails, and postal correspondences are now being monitored and checked by state security agencies due to their critical role against communication surveillance.[182]

[174] For details Priyamvada Gopal, "This Is a Watershed Moment for India. It Must Choose Freedom over Intolerance," *The Guardian*, February 17, 2016, Online Edition edition, sec. Opinion, http://www.theguardian.com/commentisfree/2016/feb/17/india-kanhaiya-kumar-watershed-freedom-intolerance-bjp-hindu.

[175] See details Samanth Subramanian, "The Hit List," *The New Yorker*, December 21, 2015, http://www.newyorker.com/magazine/2015/12/21/the-hit-list.

[176] In Bangladesh, it is quite interesting that a largest Islamic political party *Jamaat-e-islami* Bangladesh and largest opposition political party Bangladesh Nationalist Party (BNP) regularly or loosely labeled by the ruling political party or monopolized state machinery as a 'terrorist' organization due to their top leadership's direct involvement involvement in war crimes, crimes against humanity and genocide during the liberation war in spite of their open alignment with mass movements. See details at Naureen Chowdhury Fink, "Bombs and Ballots: Terrorism, Political Violence and Governance in Bangladesh," Country report (Oslo, Norway: International Peace Institute, February 2010), https://www.ciaonet.org/attachments/16071/uploads.

[177] See case of Adilur Rahman Khan, Sectary of Odhikar, a Dhaka Based rights organization at Chapter I and also according to chief public prosecutor of Cyber Crimes Tribunal at least 500 cases are pending against netizens in various charges. For details see chapter I.

[178] In Pakistan, a Christian blogger being accused of blasphemy over the internet and went into hiding for three years when he was first accused in November, 2014 in Chakwal, see details Nabeel Anwar Dhakku, "Man Held over Blasphemy Allegation," November 15, 2014, http://www.dawn.com/news/1144655.

[179] In South Asian context, the term 'national security' always being used loosely since the inception of the statehood and overlook the fifteen principles of Tshwane or Johannesburg principles. For details "The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points" (Open Society Justice initiative, June 2013), http://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points. And also "The Johannesburg Principles on National Security, Freedom of Expression and Access to Information," 1996, U.N. DOC. E/CN.4/199639, https://www1.umn.edu/humanrts/instree/johannesburg.html.

[180] For example, last few decades' religion based politics mostly political islam being criminalized in spite of fundamental their fundamental limitations in South Asia and rise of secular extremism is quite evident. See details Ali Riaz, *Religion and Politics in South Asia* (Routledge, 2010) and Maidul Islam, *Limits of Islamism* (Cambridge University Press, 2015)

[181] For example, case of Samajwadi Party General Secretary Amar Singh. See details at DNA India, "HC Reserves Order on Phone-Tapping Case | Latest News & Updates at Daily News & Analysis," *Dna*, January 25, 2006, Online Edition, http://www.dnaindia.com/india/report-hc-reserves-order-on-phone-tapping-case-1009566.

[182] See details at Chapter I & II

In this context of complex scenario, the internet and communication landscape should be open and free, activists and policy makers' narrative should be enhanced to cover main areas of cyber security and cyber surveillance to prevent countries into a police-state (other words Orwellian societies), the number of challenges are increasing for human rights defenders, journalists and bloggers, and radical reforms are in high demand to be adopted to the legislative and policies framework. At the same time State should realize that online threats and cybercrimes are not something new, even fraudulent activities and illegal access to data and computers are far more complex now due to advancement of technology and the more reliance on the internet in our daily activities and interactions. However, any legislations or cybersecurity procedures and measures should be implemented in accordance with the international human rights frameworks whereas the human rights community and actors should be actively involved in identifying online threats and shaping the policies, guidelines and frameworks, otherwise, State could jeopardize human rights to privacy and freedom of expression, association and access to information.

Therefore, human rights defenders should ask what 'cybersecurity' is, do we have a well-defined, unanimous agreement on the definition of cybersecurity across different context and disciplinary? The broad definition of cybersecurity terminology that incorporate legitimate and illegitimate concerns leads to misinterpretation in South Asia. Kovacs and Hawtin[183] adds to these challenges what they refer to as 1) Threats where technology are the basis to carry out security threats and breaches like DDoS attacks, unauthorized access to infrastructure, data and information; 2) Threats that are carried over the internet but necessarily are pausing a critical risk like spamming, planning for terrorist attacks and child pornography. What they noted was that threats that are related to countries infrastructure and computer

[183] Anja Kovacs and Dixie Hawtin, "Cyber Security, Surveillance and Online Human Rights - Publication | Global Partners Digital" (Stickholm Internet Forum, Sweden: Global Partners Digital and Internet Democracy Project, 2013), 4–5, http://www.gp-digital.org/publication/second-pub/.

systems needs more technical understanding in nature and thus, needs a deeper analysis of the implementation of cybersecurity strategies that takes human rights into consideration. Given that usually the impact of human rights laws is not straightforward or clear when realized in this domain, the focus or the work done in this regard is less apparent. However, threats related to content, are far more analyzed and addressed for many years now where the impact of these threats to freedom of expression and privacy is well-defined according to the international human rights law.

After Snowden revelations, the extent of cooperation in sharing information between intelligence agencies across the world raised serious concerns regarding the extra-territorial application of human rights treaties as these intelligence information is being collected, shared and stored across different territorial jurisdiction. In addition, these activities raised questions on when these governments are held reliable under national and international laws when it comes to activities conducted beyond their national borders. These and similar questions shaped what has become the thirteen (13) 'Necessary and Proportionate Principles'[184] that provides civil society groups, legislative entities and courts with a framework to evaluate whether communication surveillance laws and practices comply with human rights principles in post-Snowden era.

This research suggests to South Asian online and human rights community, particularly to states' to adopt thirteen necessary and proportionate principles in the age of mass communication surveillance However, the communication surveillance principles highlight "two core definitional issues that have raised specific challenges in the application of human rights protection to technologically advances communication surveillance"[185]. These thirteen principles (i.e. legality, legitimate aim, necessity,

[184] The full text of the International Principles on the Application of Human Rights to Communication Surveillance is available at:!https://en.necessaryandproportionate.org/text.

[185] See details at Privacy International in cooperation with Centre for Internet and Society, "Communications Surveillance | Privacy International," accessed March 30, 2016, https://www.privacyinternational.org/node/10.

adequacy, proportionality, oversights of competent judicial authority, due process, notification, and so on) also include well recognized and established notions of freedom of association, right to privacy, and freedom of expression as guaranteed in the Universal Declaration of Human and International Covenant on Civil and Political Rights (ICCPR).

Concluding Remarks

This research acknowledges that the gradual accumulation of communication surveillance regimes and compromised privacy rights in the digital age has raised serious concerns across South Asia and beyond. However, this is taking place not only in countries that are known to have negative human rights track records, and practice 'fragile democracy' like Bangladesh, India and Pakistan, but also in countries which are traditionally deemed to be liberal and democratic such as United States, United Kingdom and others. Therefore, human rights defenders and academic-activists have critical duty to unpack and display the reality which reduces a human life to a mere 'bare life'[186] or 'sub-human', and in line with these challenge human rights defenders, bloggers and online activists should rethink and remodels their online safety and risk, and of course, reconnoiters the ground upon which the whole edifice of unjust communication surveillance, content blocking, filtering, removal and manipulation, censorship and other state-sponsored 'crimes against freedom of expression and internet are committed in South Asia.

[186] One of the most important theory introduced by Giorgio Agamben which instigates us to reevaluate the political contradiction of modernity. See the explanation of the theory by Giorgio Agamben, at *State of Exception* (University of Chicago Press, 2005).

Bibliography

Abid, Sohali. “Massive Leak Opens New Investigation of Fin Fisher Surveillance Tools in Pakistan.” Community. *Global Voices Advocacy*, August 22, 2014. https://advox.globalvoices.org/2014/08/22/massive-leak-opens-new-investigation-of-finfisher-surveillance-tools-in-pakistan/.

“A Brief History of the State of Exception by Giorgio Agamben.” Accessed March 27, 2016. http://www.press.uchicago.edu/Misc/Chicago/009254.html.

AFP. “Christian Healer Arrested for Blasphemy in Lahore,” October 19, 2015. http://www.dawn.com/news/1214151.

Agamben, Giorgio. *State of Exception*. University of Chicago Press, 2005.

Ajasa, Femi. “Mob Attack Former Pakistan Pop Star Accused of Blasphemy.” *Vanguard News*, March 27, 2016. http://www.vanguardngr.com/2016/03/mob-attack-former-pakistan-pop-star-accused-blasphemy/.

Al Jazeera English. “An Attack on Bloggers.” Accessed March 30, 2016. http://www.aljazeera.com/programmes/101east/2015/11/bangladesh-attack-bloggers-151117122237015.html.

Article 19. “Pakistan: Telecommunications (Re-Organization) Act.” Legal Analysis. United Kingdom: Article 19, January 2012. https://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf.

Article 19, Digital Rights Foundation. “Pakistan: New Cybercrime Bill Threatens the Rights to Privacy… · Article 19.” NGO Websites. *Article 19*, April 20, 2015. https://www.article19.org/resources.php/resource/37932/en/pakistan:-new-cybercrime-bill-threatens-the-rights-to-privacy-and-free-expression.

Ashokan, Anisha. “Cyber Cafes Flout Rules, Do Not Ask Users for ID Proofs | Latest News & Updates at Daily News & Analysis.” Accessed March 30, 2016. http://www.dnaindia.com/mumbai/report-cyber-cafes-flout-rules-do-not-ask-users-for-id-proofs-1180572.

“Avijit Roy’s Publisher, 2 Bloggers Hacked in Dhaka | Dhaka Tribune.” Accessed March 26, 2016. http://www.dhakatribune.com/crime/2015/oct/31/three-bloggers-hacked-dhaka.

Bangladesh Telecommunication Regulatory Commission. “Regulatory and Licensing Guidelines for Issuing License.” Guidelines. Dhaka, Bangladesh: BTRC, August 6, 2008. http://lirneasia.net/wp-content/uploads/2008/08/bwa_guidelines1.pdf.

Bergman, David. “New Age.” *New Age*, February 16, 2015. http://newagebd.net/95692/telecom-operators-retain-6-months-of-sms-other-info-for-law-enforcers/.

Bolo BHi. “Hacking Team in Pakistan - Bolo Bhi Bolo Bhi.” NGO Websites. *Advocacy*, July 5, 2015. http://bolobhi.org/hacking-team-in-pakistan/.

“BTRC to Form Body to Curb Cyber Crime.” *BTRC to Form Body to Curb Cyber Crime | Daily-Sun.com*. Accessed March 28, 2016. http://www.daily-sun.com/post/68318.

“BTRC to Form Body to Curb Cyber Crime.” *BTRC to Form Body to Curb Cyber Crime | Daily-Sun.com*. Accessed March 28, 2016. http://www.daily-sun.com/post/68318.

“bwa_guidelines1.pdf.” Accessed March 28, 2016. http://lirneasia.net/wp-content/uploads/2008/08/bwa_guidelines1.pdf.

“Cable Trouble Hits Twitter, Other Mobile Services.” *The Indian Express*, February 19, 2015. http://indianexpress.com/article/technology/technology-others/cable-trouble-hits-twitter-other-mobile-services/.

"CAUSE Report v7.pdf." Accessed March 28, 2016. https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf.

c, Aziz Nayani Master's, idate, and international affairs at Columbia University. "Pakistan's Cellphone-Registration Policy Will Do Little to Curb Terrorism." *Quartz*. Accessed March 30, 2016. http://qz.com/360420/pakistans-cellphone-registration-policy-will-do-little-to-curb-terrorism/.

ChanneliFrance. *Dr. Mizanur Rahman in Paris, Channel I Europe News By Hasem*. Accessed March 28, 2016. https://www.youtube.com/watch?v=bHKNi-q4-JE.

Coalition Against Unlawful Surveillance Exports. "The Critical Opportunity: Bringing Surveillance Technologies within the EU Dual- Use Regulation." NGO Report. CAUSE. Global: Coalition Against Unlawful Surveillance Exports, June 2015. https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf.

"comm2006.pdf." Accessed March 30, 2016. http://www.icnl.org/research/library/files/Bangladesh/comm2006.pdf.

"Cyber_violence_gender Report.pdf." Accessed March 30, 2016. http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf.

Dad, Nighat. "Big Brother Is Curtailing Net Freedom in South Asia - Al Jazeera English." *Aljazeera English Op-Ed*. January 11, 2014, Online Edition, sec. Opinion. http://www.aljazeera.com/indepth/opinion/2014/01/big-brother-curtailing-net-freedom-south-asia-20141544556701717.html.

Davis, Fergal, Nicola Mc Garrity, and George Williams, eds. "Mapping the Terrain." In *Surveillance, Counter-Terrorism and Comparative Constitutionalism*, First Edition., 3–9. Routledge, 2013.

———. , eds. *Surveillance, Counter-Terrorism and Comparative Constitutionalism*. Routledge, 2013.

Dawn.com, AFP |. "Rights Advocate Rashid Rehman Khan Gunned down in Multan," May 7, 2014. http://www.dawn.com/news/1104788.

Department of Electronics and Information Technology, Government of India. "Digital India." Deity, Government of India, August 18, 2014. http://deity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf.

Dhakku, Nabeel Anwar. "Man Held over Blasphemy Allegation," November 15, 2014. http://www.dawn.com/news/1144655.

"Digital Rights Foundation › Pakistan Is a Fin Fisher Customer, Leak Confirms." *Digital Rights Foundation*. Accessed March 30, 2016. http://digitalrightsfoundation.pk/pakistan-is-a-finfisher-customer-leak-confirms/.

DNA India. "HC Reserves Order on Phone-Tapping Case | Latest News & Updates at Daily News & Analysis." *Dna*. January 25, 2006, Online Edition, sec. Online. http://www.dnaindia.com/india/report-hc-reserves-order-on-phone-tapping-case-1009566.

EDRi. "India: Free Basics Violates Principles of a Neutral Internet." NGO Report. Belgium: EDRI, January 13, 2016. https://edri.org/india-free-basics-violates-principles-of-a-neutral-internet/.

"Facebook Trouble: 10 Cases of Arrests under Sec 66A of IT Act." *Http://www.hindustantimes.com/*, March 24, 2015. http://www.hindustantimes.com/india/facebook-trouble-10-cases-of-arrests-under-sec-66a-of-it-act/story-4xKp9EJjR6YoyrC2rUUMDN.html.

Fink, Naureen Chowdhury. "Bombs and Ballots: Terrorism, Political Violence and Governance in Bangladesh." Country report. Oslo, Norway: International Peace Institute, February 2010. https://www.ciaonet.org/attachments/16071/uploads.

France-Presse, Agence. “Bangladesh Court Convicts British Journalist for Doubting War Death Toll.” *The Guardian*, December 2, 2014, sec. World news. http://www.theguardian.com/world/2014/dec/02/bangladesh-convicts-british-journalist-david-bergman.
“G1215325.pdf.” Accessed March 30, 2016. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.
Gabol, Dawn com | Imran. “Police Take down Offensive Anti-Minority Poster in Lahore after Outrage,” December 11, 2015. http://www.dawn.com/news/1225696.
Ghosh, Snehashish. “The Telecom Regulatory Authority of India Act, 1997 — The Centre for Internet and Society.” NGO Websites. *The Center for Internet and Society*, March 2013. http://cis-india.org/telecom/resources/trai-act-1997.
Gopal, Priyamvada. “This Is a Watershed Moment for India. It Must Choose Freedom over Intolerance.” *The Guardian*. February 17, 2016, Online Edition, sec. Opinion. http://www.theguardian.com/commentisfree/2016/feb/17/india-kanhaiya-kumar-watershed-freedom-intolerance-bjp-hindu.
“Government to Launch Internet Spy System ‘Netra’ Soon.” *The Economic Times*, June 6, 2014. http://economictimes.indiatimes.com//articleshow/28440192.cms.
Hashim, Asad. “Surveilling and Censoring the Internet in Pakistan - Al Jazeera English.” *Aljazeera English Op-Ed*. May 13, 2015, Online Edition, sec. Internet. http://www.aljazeera.com/indepth/features/2015/05/pakistan-internet-censorship-150506124129138.html.
Human Rights Council. “The Declaration on the Right of Individuals, Groups of Power in Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms.” United Nation. Accessed March 27, 2016. http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Defender.aspx.
“ICTFactsFigures2015.pdf.” Accessed March 29, 2016. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
IFSEC International. “Internet Surveillance Picks up Speed in India.” Online Newspaper. *IFSEC Global*, January 1, 2014. http://www.ifsecglobal.com/internet-surveillance-picks-speed-india/.
“In Demand: 3G User Base Expanding, Market Surges Forward.” *The Express Tribune*, September 16, 2014. http://tribune.com.pk/story/762745/in-demand-3g-user-base-expanding-market-surges-forward/.
“Indicator-Reports-Mar12082015.pdf.” Accessed March 29, 2016. http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator-Reports-Mar12082015.pdf.
Indu, Nandakumar. “Government Can Now Snoop on Your SMSs, Online Chats - Times of India.” *The Times of India*. May 7, 2013, Online Edition, sec. Tech News. http://timesofindia.indiatimes.com/tech/tech-news/Government-can-now-snoop-on-your-SMSs-online-chats/articleshow/19932484.cms.
Intellectual Property Watch. “UN General Assembly Adopts Resolution On Privacy And Surveillance.” *Intellectual Property Watch*, January 8, 2014. http://www.ip-watch.org/2014/01/08/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/.
“International Covenant on Civil and Political Rights.” Accessed March 26, 2016. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

International Telecommunication Union. “Internet World State 2014: Pakistan, Asia Marketing Research, Internet Usage, Population Statistics and Facebook Subscribers.” Accessed March 28, 2016. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
———. “Percentage of Individuals Using the Internet, 2000-2014.” Accessed March 28, 2016. http://data.un.org/Data.aspx?d=ITU&f=ind1Code%3AI99H.
“Internet Subscribers in Bangladesh June 2015 | BTRC.” Dhaka, Bangladesh: BTRC. Accessed March 29, 2016. http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2015.
“Internet Subscription in Bangladesh,” n.d.
Irwin, Sarah. “Data Analysis and Interpretation: Emergent Issues in Linking Qualitative and Quantitative Evidence.” In *Handbook of Emergent Methods*, edited by S. N. Hesse-Biber and P. Leavy, 415–540. New York, NY, US: Guilford Press, 2008.
Islam, Maidul. *Limits of Islamism*. Cambridge University Press, 2015.
Islam, Muhammad Zahidul. “Viber, Tango Blocked in Bangladesh | Dhaka Tribune.” Accessed March 30, 2016. http://www.dhakatribune.com/bangladesh/2015/jan/18/govt-shuts-down-viber.
Islam, Rezwan. “Bangladesh Authorities Go After Bloggers, Claim They Are ‘Anti-Muslim’ · Global Voices.” Human Right Community. *Global Voices*, April 1, 2013. https://globalvoices.org/2013/04/01/bangladesh-authorities-go-after-anti-muslim-bloggers/.
“ISPAK : Internet Service Providers Association of Pakistan.” Accessed March 29, 2016. http://www.ispak.pk/.
Issacharoff, Samuel. “Fragile Democracies.” *Harvard Law Review* 120, no. 6 (2007): 1405–67.
Kelly, Sanja, Madeline Earp, Reed Laura, Adrian Shahbaz, and Truong. “Privatizing Censorship, Eroding Privacy :Freedom on the Net 2015.” Human Rights Report. New York: Freedom House, October 2015. https://freedomhouse.org/report/freedom-net/freedom-net-2015.
Khan, Aby Saieed. “Bangladesh Telecommunication (Amended) Act, 2010.” In *Internet Freedom in South Asia*. Dhaka, Bangladesh, 2013.
Kovacs, Anja, and Dixie Hawtin. “Cyber Security, Surveillance and Online Human Rights - Publication | Global Partners Digital,” 4–5. Sweden: Global Partners Digital and Internet Democracy Project, 2013. http://www.gp-digital.org/publication/second-pub/.
Lara, Stacy Dry-. “The Right to Privacy in the Digital Age.” *FAWCO*. Accessed March 26, 2016. https://www.fawco.org/fawco-the-un/what-we-do/current-initiatives/human-rights/human-rights-council/hrc-27-blog/3149-privacy-on-the-right-to-privacy-in-the-digital-age.
Lyon, David. *Surveillance After Snowden*. John Wiley & Sons, 2015.
McIntyre, T. J. “Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2015. http://papers.ssrn.com/abstract=2694512.
Miller, Daniel. “Could the Internet Defetishise the Commodity?” *Environment and Planning D: Society and Space* 21, no. 3 (June 1, 2003): 359–72. doi:10.1068/d275t.
Ministry of Planning, Development and Reform, Government of Pakistan. “Pakistan 2025: One Nation One Vision.” Planning Commission, Government of Pakistan, May 29, 2014. http://www.pc.gov.pk/wp-content/uploads/2015/05/Pakistan-Vision-2025.pdf.
Mir, Waqqas, and Niazi Hassan. “Surveillance Laws & Practices in Pakistan: History, Current Legislation & Lessons from the United Kingdom.” *Online Publication*, n.d., 22–23.
“Myth of the 84 Bloggers ‘Hit’ List in Bangladesh: Busting the Media Narrative | Turkey Agenda.” Accessed March 30, 2016. http://www.turkeyagenda.com/myth-of-the-84-bloggers-hit-list-in-bangladesh-busting-the-media-narrative-2842.html.

"New Age." *New Age*, November 2, 2014. http://newagebd.net/63052/rab-seeking-to-purchase-powerful-mobile-phone-spy-tool/.
New Age Report. "Youth Jailed for Parody on Sheikh Mujib, PM." *New Age*. September 25, 2014, Online Edition, sec. Front Page. http://newagebd.net/52448/youth-jailed-for-parody-on-sheikh-mujib-pm/.
Norris, Pippa. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press, 2001.
Omanovic, Edin. "Eight Things We Know so far from the Hacking Team Hack | Privacy International." Advocacy. *Being Stealth and Untraceable*. Accessed March 28, 2016. https://www.privacyinternational.org/node/619.
"O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-Based Newspapers' Role in Pakistan's Censorship Regime." *The Citizen Lab*, June 20, 2013. https://citizenlab.org/2013/06/o-pakistan/.
"Pakistani Couple Get Death Sentences for Blasphemy." *BBC News*. Accessed March 30, 2016. http://www.bbc.com/news/world-asia-26901433.
"Pakistan-Vision-2025.pdf." Accessed March 28, 2016. http://www.pc.gov.pk/wp-content/uploads/2015/05/Pakistan-Vision-2025.pdf.
Parkinson, Charles. "Trapped Between Murder and Repression: Life as an Atheist Blogger in Bangladesh." *VICE News*. December 9, 2015, Online Edition, sec. Asia Pacific Section. https://news.vice.com/article/trapped-between-murder-and-repression-life-as-an-atheist-blogger-in-bangladesh.
Parmer, Sejal. "Towards an Effective Framework of Protection for the Work of Journalists and an End to Impunity," 2014. http://dare.uva.nl/record/1/448153.
Patry, Melody. "India: Digital Freedom under Threat? Online Censorship." *Index on Censorship*, November 21, 2013. http://bit.ly/1LnnVAI.
Policing-and-Social-Media-Social-Control-in-an-Era-of-New-Media. Accessed March 30, 2016. https://rowman.com/ISBN/9781498533720/Policing-and-Social-Media-Social-Control-in-an-Era-of-New-Media.
Prime Minister Office. "Digital Bangladesh | Access to Information (a2i) Programme." Access to Information Program, November 5, 2009. http://www.a2i.pmo.gov.bd/digital-bangladesh.
Privacy International in cooperation with Centre for Internet and Society. "Communications Surveillance | Privacy International." Accessed March 30, 2016. https://www.privacyinternational.org/node/10.
———. "Communications Surveillance | Privacy International." Accessed March 30, 2016. https://www.privacyinternational.org/node/10.
———. "State of Surveillance: India." Summary Report. State of Surveillance. United Kingdom and India: Privacy International, March 2, 2016. https://www.privacyinternational.org/node/738.
Privacy International. "The 2007 International Privacy Ranking." Survey report. United Kingdom: Privacy International, July 2007. https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings.
Rahi, Gaikwad. "Over 100 Held for Vadodara Violence." *The Hindu*. September 30, 2014. http://www.thehindu.com/news/national/other-states/over-100-held-for-vadodara-violence/article6458715.ece.
Rahman, Md Rezaur. "Human Rights Defenders at Risk: The Case of 10th Parliamentary Election - 2014 in Bangladesh." Academic Thesis, University of Sydney, 2014.

Rahman, Rezaur. “Mapping Trends of and Counter Responses to ‘Terrorism’ in Asia after 9/11: Analyzing the Impact of Anti-Terrorism Laws and Policies.” MA Thesis, Sungkonghow University, 2012. Sungkonghoe University library.
Rehman, Jahanzaib Haque | Atika. “Hacking Team Hacked: The Pakistan Connection, and India’s Expansion Plan.” *Online Publication*. July 28, 2015, online Edition, sec. op-ed. http://www.dawn.com/news/1196767.
Reporters without Border (Sans Frontiers). “2015 World Press Freedom Index.” Interactive. *2015 World Press Freedom Index*. Accessed March 27, 2016. http://index.rsf.org.
Reporter Without Border. “The Enemies of Internet.” NGO Websites. *The Enemies of Internet*, July 2013. http://surveillance.rsf.org/en/.
“REPORT on ‘Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries’ - A8-0178/2015.” Accessed March 28, 2016. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0178+0+DOC+XML+V0//EN.
Riaz, Ali. *Religion and Politics in South Asia*. Routledge, 2010.
Rice, Matthew. “Tipping the Scales: Security and Surveillance in Pakistan | Privacy International.” Special Report. Big Brother Project. London, United Kingdom: Privacy International, July 2015. https://www.privacyinternational.org/node/624.
“Seminar and Inter-Regional Dialogue on the Protection of Journalists (3 November 2014).” *Freedom of Expression*. Accessed March 27, 2016. http://www.coe.int/web/freedom-expression/seminar-inter-regional-dialogue.
“Shame on Sunitha Krishnan: 5 Reasons Why Sharing the WhatsApp Rape Video Is Wrong - Firstpost.” Accessed March 30, 2016. http://www.firstpost.com/living/shame-on-sunitha-krishnan-5-reasons-why-sharing-the-whatsapp-rape-video-is-wrong-2086323.html.
Singer, Jane B. “The Political J-Blogger ‘Normalizing’ a New Media Form to Fit Old Norms and Practices.” *Journalism* 6, no. 2 (May 1, 2005): 173–98. doi:10.1177/1464884905051009.
“South_asia_roundtable_report.pdf.” Accessed March 29, 2016. http://www.ichrp.org/files/assets/260/south_asia_roundtable_report.pdf.
“South_asia_roundtable_report.pdf.” Accessed March 29, 2016. http://www.ichrp.org/files/assets/260/south_asia_roundtable_report.pdf.
“Statement on Arrest of Adilur Rahman Khan, Secretary of Odhikar | Odhikar.” Accessed March 30, 2016. http://odhikar.org/statement-on-arrest-of-adilur-rahman-khan-odhikar-secratary/.
“Statistics - Academic and Community Studies.” *Stop Street Harassment*. Accessed March 30, 2016. http://www.stopstreetharassment.org/resources/statistics/statistics-academic-studies/.
Subramanian, Samanth. “The Hit List.” *The New Yorker*, December 21, 2015. http://www.newyorker.com/magazine/2015/12/21/the-hit-list.
“Surveillance and the Indian Constitution - Part 1: Foundations.” *The Centre for Internet and Society*. Accessed March 30, 2016. http://cis-india.org/internet-governance/blog/surveillance-and-the-indian-consitution-part-1.
“Surveillance-Industry-India.pdf.” Accessed March 28, 2016. http://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf.
Telecom Regulatory Authority of India. “The Indian Telecom Services Performance Indicators.” Quarterly Report. New Delhi: Telecom Regulatory Authority of India, March 2015. http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator-Reports-Mar12082015.pdf.

"The Global Competitiveness Report 2013-2014." *World Economic Forum*. Accessed March 26, 2016. https://www.weforum.org/reports/global-competitiveness-report-2013-2014.
"The Guardian Website Inaccessible in Parts of Pakistan." *The Express Tribune*, February 3, 2014. http://tribune.com.pk/story/666959/the-guardian-website-reportedly-inaccessible-in-pakistan/.
"The Johannesburg Principles on National Security, Freedom of Expression and Access to Information," 1996. U.N. DOC. E/CN.4/199639. https://www1.umn.edu/humanrts/instree/johannesburg.html.
"The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points." Open Society Justice initiative, June 2013. http://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points.
"The Universal Declaration of Human Rights | United Nations." Accessed March 26, 2016. http://www.un.org/en/universal-declaration-human-rights/.
"TRAI Spectrum Price Proposal May Fetch Rs 5.36 Lakh Crore for Govt." *The Indian Express*, January 28, 2016. http://indianexpress.com/article/india/india-news-india/trai-spectrum-price-proposal-may-fetch-rs-5-36-lakh-crore-for-govt/.
"Trai Wants Auction of 3G Spectrum after Formation of New Govt - Indian Express." Accessed March 28, 2016. http://archive.indianexpress.com/news/trai-wants-auction-of-3g-spectrum-after-formation-of-new-govt/1225198/.
Tribune Online Report. "Bangladesh Sought Data on 17 Facebook Users | Dhaka Tribune." *The Dhaka Tribune*. November 5, 2014, Online Edition. http://www.dhakatribune.com/bangladesh/2014/nov/05/bangladesh-sought-data-17-facebook-users.
"Überwachungsexporte: Die Bangladesh-Connection," September 3, 2014. https://www.woz.ch/-53af.
"UN General Assembly Adopts Resolution On Privacy And Surveillance." *Intellectual Property Watch*, January 8, 2014. http://www.ip-watch.org/2014/01/08/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/.
United Nations Human Rights Council. "International Principles on the Application of Human Rights Law to Communications Surveillance." Electronic Frontier Foundation and Article 19, May 28, 2014. https://en.necessaryandproportionate.org/LegalAnalysis/communications-surveillance.
———. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," n.d. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.
———. "The Promotion, Protection and Enjoyment of Human Rights on the Internet." United Nation, July 16, 2012. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.
United Nations Special Rapporteur for Freedom of Expression. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." United Nation, May 16, 2011. United Nations Special Rapporteur for Freedom of Expression.
Unknown. "Creeping Censorship: Spotflux Claims Its Service Is Being 'Actively Blocked' in Pakistan - The Express Tribune." *The Express Tribune*. January 28, 2014, Online Edition, sec. Web desk. http://tribune.com.pk/story/664341/creeping-censorship-spotflux-claims-its-service-is-being-actively-blocked-in-pakistan/.
"Vision 2021." *Wikipedia, the Free Encyclopedia*, December 27, 2015. https://en.wikipedia.org/w/index.php?title=Vision_2021&oldid=696993924.

"Woman Files Complaint against Man Who Called for 'Women like Her to Be Raped by Rapists.'" *The News Minute*, January 16, 2015. http://www.thenewsminute.com/socials/114.

World Bank. "Pakistan | Data." International. *Pakistan: Internet Users (per 100 People)*. Accessed March 29, 2016. http://data.worldbank.org/country/pakistan.

Wu, Tim. "Network Neutrality, Broadband Discrimination." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, June 5, 2003. http://papers.ssrn.com/abstract=388863.

Xynou, Maria. "Big Democracy, Big Surveillance: India's Surveillance State." Community. *Open Democracy*, April 16, 2015. http://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state.

———. "The Surveillance Industry in India." NGO Websites. *The Surveillance Industry in India*, March 2014. http://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf.

Yameen, Ahsan. "P@SHA Aims to Energize IT Industry of Pakistan through Variety of Events." *Tech Mag – Pakistani Online IT & Technology Magazine & News Platform*, January 10, 2016. http://techmag.pk/psha-aims-to-energize-it-industry-of-pakistan-through-variety-of-events/.

"Youth Arrested for Making Anti-Mamata Remark on Facebook - Times of India." *The Times of India*. Accessed March 27, 2016. http://timesofindia.indiatimes.com/city/kolkata/Youth-arrested-for-making-anti-Mamata-remark-on-Facebook/articleshow/44828692.cms.