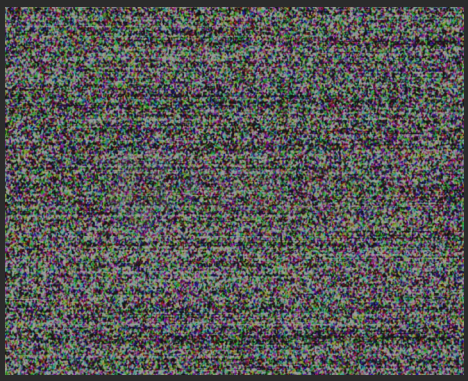
DANGERS OF DIGITAL SURVEILLANCE

An account of self-censorship by journalists and human rights defenders in Pakistan



Dangers of Digital Surveillance:

An account on self-censorship by journalists and human rights defenders in Pakistan

_ by Haroon Baloch & Amjad Qammar
_ design and art: Nida Meyer Mian

l. Haroon Baloch is a researcher with Bytes for All, Pakistan and freelance multimedia journalist based in Islamabad. Amjad Qamar is a seasoned media development professional, worked on this report as an independent consultant.

Table of Contents:

ABSTRACT

Pakistan legitimised digital surveillance by broadening the scope of existing legal framework and enacting new disproportionate laws, including the Investigation for Fair Trail Act 2013 and Prevention of Electronic Crimes Act 2016. Unbridled powers to conduct unlawful and arbitrary interceptions on digital communications of citizens, and personal and private data have been granted to law enforcement agencies (LEAs). Journalists and human rights defenders (HRDs) are subjects of digitally enabled surveillance of both the State and non-state actors, who often work hand-in-hand. This absurd relationship and proxy relationship has become the reason of losing their sources of information. It has also been cultivating a profuse environment of fear and intimidation, in the end resulting in self-censorship and restriction in their free movement. This paper maps out the underlying trends and challenges to freedoms of expression and of movement of journalists and HRDs due to digital surveillance. It also examines the roles of different actors involved in this process who are becoming responsible for self-censorship in Pakistan.

Keywords: Digital surveillance, privacy, self-censorship, security, journalists, human rights defenders.

I. Introduction

Prominent Pakistani journalist and host of the most rated television show Capital Talk, Hamid Mir believes that his telephones have turned out the most dangerous, yet important tool for his profession. Mir is one of the very few journalist survivors who were attacked with impunity. Mir had landed at Jinnah International Airport in Karachi through a domestic flight from Islamabad on April 19, 2014. With the apprehensions of being killed, Mir preemptively had changed his flight schedule twice and kept his final itinerary undisclosed. Even his office was in dark about the schedule, except his close aides. The evening he landed in Karachi and was on his way to the office, two assailants riding a motorbike chased his car and sprayed bullets.[2] Mir received six bullets, nonetheless, his luck was in and survived. He told Bytes for All, Pakistan that his movements were tracked through his mobile phone signals. According to Mir, both the State and non-state actors were behind this attack who had been keeping a close eye on his movements for a long time. Before attempt on his life, he had also received threatening calls, which he reported to authorities.

The confession of the State intelligence agencies in a long pending suo motu case of phone tapping of Pakistani citizens was not surprising for many in the country. Nonetheless, it testified the claims of journalists, human rights defenders, politicians and judges that their communications were being tapped and tracked by anonymous privacy trespassers. Inter-Services Intelligence (ISI) and Intelligence Bureau (IB), two prominent intelligence agencies, submitted their reports in the Supreme Court in June 2015 admitting that they were involved in tapping thousands of telephones calls across the country on monthly basis. [3]

1. *This template is work is made available under CCO 1.0 Universal (CCO 1.0) Public Domain Dedication, still original author is Michele Marrali from Studio Storti Srl.*
2. *AFP. (2014). Hamid Mir issues first statement after attack. The News. https://www.geo.tv/latest/71280-hamid-mir-issues-first-statement-after-being-attacked*
3. *Dawn. (2015). Nearly 7000 phones tapped in May, ISI tells SC. https://www.dawn.com/news/1186013*

Justice Saqib Nisar, the current chief justice of Pakistan, at that time had observed that the court cannot sweep this matter under the carpet as it concerns the rights of the people. However, it had no objection if the agencies enjoyed legal authority (LEAs) to record phone calls.

Here the question is whether the law enforcement agencies do have sufficient legal grounds to conduct surveillance on digital communications of Pakistani citizens? And if yes, then does the legal framework meet the global human rights standards, and the principles of necessity and proportionality?

Pakistan is in political transition, and Pakistan Peoples Party (PPP) bestowed with peoples' mandate in 2008 general elections completed the process of smooth transfer of powers to another democratically elected government of Pakistan Muslim League Nawaz (PML-N) after completing its constitutional term. A party of center-right, PML-N now claims the credit of the internet access expansion through quality broadband services to over 37.57 million citizens.[4] However, it brought strict regulations to stifle the enabling rights including freedoms of expression, and right of peaceful assembly and association in online spaces. In first four years of its becoming into power, the PML-N government aggressively reacted to circumcise online freedoms, and the right to privacy is one of them. In the guise of regulating online spaces, the government promulgated the Prevention of Electronic Crimes Act (PECA)[5] in July 2016. It was an attempt to legitimise arbitrary digital surveillance on citizens, enabling authorities for misusing its provisions to clampdown political dissent, suppress online assemblies and criminalise legitimate forms of expression.

Beside being in a political transition, terrorism has badly damaged the political infrastructure and socio-cultural fabric of the country during past 16 years.

4. *Yusufzai, A. (January 2017). 3G, 4G users in Pakistan reached 37.57 million. https://propakistani.pk/2017/01/18/3g-4g-users-pakistan-reached-37-57-million/*
5. *Prevention of Electronic Crimes Act, 2016. National Assembly. www.na.gov.pk/uploads/documents/1470910659_707.pdf*

The strenuous Pakistan-India ties have a long history of mistrust and violence on both sides of the border, ultimately setting the grounds for espionage activities both in and outside the country.[6] However, the State's espionage has now transpire to online spaces from physical monitoring. The modern spying technologies available in the market and the governing laws have even made it easier for the LEAs to carry out real-time surveillance on its citizens. Unbridled monitoring or profiling of citizens by the State has made the marginalised groups, especially journalists and human rights defenders more prone to threats.

Pakistan is among few countries across the globe that are unfortunately regarded as "deadliest for journalists" for various reasons. Among others, these include the lethal nexus between the State and non-state actors, divulging corruption of civil and military establishment, pressure groups including political and religious parties, etc.[7] Journalists' killings with impunity is intimidating and consequential threat for press freedom ultimately resulting in self-censorship, facts manipulation and toning down information.

Spaces for human rights defenders have also been shrinking rapidly when it comes to their expression and cause-oriented campaigns for common good, transparency in administrative affairs, and accountability. Monitoring of online activities, whether by employing intrusive technology or simply stalking through social media footprints, cultivates a hounding atmosphere, which torments them in their work of protecting and promoting civil liberties. The increased culture of prying on electronic communications restricts human rights defenders' activities both in virtual as well as physical spaces. In many cases, human rights defenders ended up as victims of tyranny and even received death threats for campaigning online.[8]

6. *Jacob, J. & Ahuja, R. (2017). Spy vs spy: India has never sentenced a Pakistani to death for espionage. HT. http://www.hindustantimes.com/india-news/spy-vs-spy-india-has-never-sentenced-a-pakistani-to-death-for-espionage/story-JOvyEOdxMvY69GmWtIISXM.html*
7. *The News. (2012). Pressure groups harassing media persons in Balochistan.*
8. *Zafar, A. & Baloch, H. (2016). Shrinking spaces: Online freedom of assembly and of association in Pakistan. B4A. http://www.netfreedom.pk/wp-content/uploads/2017/01/FoAA-Report_web.pdf*

The situation becomes even worse when women human rights defenders and journalists express their opinions on controversial issues in Pakistan such as their expression on religious issues, military policies, political ideologies, etc.[9]

The Oxford Dictionary defines surveillance as, "Close observation, especially of a suspected spy or criminal." Whereas "digital surveillance" can be broadly referred as to the act of meticulous monitoring, tracking, identification and acquiring of the content of a wire communication using a mechanical or electronic device without the consent of subject under surveillance.

The revelations by Julian Assange, Chelsea Manning and Edward Snowden made it clearer about the nature and extent of mass digital surveillance that the State apparatus and corporate moguls have been carrying out on the personal communications of the users.

In 2015, the Privacy International's report on Pakistan outlined the state of mass surveillance enabled through the vague and imprecise legal framework. Pakistan has also partnered with notorious international surveillance programmes being operated by the United States and the United Kingdom.[10]

Apart from the mass surveillance, there are other ways of monitoring and tracking on individuals, commonly referred as targeted digital attacks and focused surveillance. The Citizen Lab at the Munk School of Global Affairs, University of Toronto defines these targeted digital attacks as, "persistent attempts to compromise and infiltrate the networked devices and infrastructure of specific individuals, groups, organisations and communities." [11]

9. *Zafar, A. & Baloch, H. (2016). Op. cit.*
10. *Rice, M. (2015). Tipping the scales: Security & surveillance in Pakistan. https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf*
11. *Deibert, R. (2017). Journalism after Snowden: The growing digital threat. GIJN. http://gijn.org/2017/06/13/journalism-after-snowden-the-growing-digital-threat-to-the-press/*

Purposes of these attacks is to cultivate an intimidating environment by the perpetrators through their intended actions with ultimate goal of stifling free expression and restricting freedom of movement of marginalised groups, particularly journalists and human rights defenders who are the main focus of this research.

This research is a part of APC-IMPACT project that focuses on internet policies related to human rights and their implementation in India, Pakistan, and Malaysia. The research is significant for both training and advocacy outputs that have to be carried out throughout the project. This country report is the third extensive research based output and will consolidate information about legislative practices dealing with the issues of privacy breaches through digitally enabled surveillance affecting the rights to freedom of expression and of movement in general and the work of journalists and human rights defenders in particular.

The core objectives of this research are to explore that:

1. How digital surveillance is a cause of self-censorship and hence affecting the work of journalists and human rights defenders;
2. How digital surveillance puts limitations on freedom of expression online and undermining the right to privacy of target groups; and
3. To look into the knowledge of the target groups about the digital tools for securing their online communications and how much they care about its safety.

The entire data collection and analysis was done by Bytes for All consultant and in-house team.

II. Literature review

Electronically enabled surveillance and digital rights, particularly privacy and governing laws is a talk of the town since Snowden revelations. Today, people around the world are more concerned about privacy and other digital rights. As reported by the Guardian newspaper in June 2013 that the US National Security Agency (NSA) was collecting the telephone records of millions of people. The Washington Post[12] and the Guardian[13] also revealed that the NSA tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo to track online communication in a surveillance programme known as PRISM. As a result there have been extensive debates and considerations on some surveillance policies. Biometric and genetic database in UK, telephone tapping cases in Germany and NSA in United States were questioned in courts about surveillance. Pakistan has also introduced a legal framework which enables LEAs to intercept communications.

a. Privacy protection and legal framework in Pakistan

The Constitution of the Islamic Republic of Pakistan provides the right to privacy as a fundamental right. Article 14(1) of the Constitution provides that "the dignity of man and, subject to law, the privacy of home, shall be inviolable."[14]

In digital era, the life is rapidly being transformed by technology, huge databases have been constructed and data mining is in perpetuation without defining the legitimate boundaries. Pakistan also lacks data protection laws and effective legal framework to protect the privacy of its citizens. The only effort to this effect was made in 2005 when a draft of data protection bill was submitted in the parliament as private member bill.[15] Since then, no progress has been made in this direction.

12. *The Washington Post. (2013). Here's everything we know about PRISM to date. https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.d0348102051*
13. *The Guardian. (2016). Prism. https://www.theguardian.com/us-news/prism*
14. *The Constitution of Islamic Republic of Pakistan. http://www.pakistani.org/pakistan/constitution/part2.ch1.html*
15. *The Electronic Data Protection Act 2005. www.media.mofo.com/docs/.../PAKISTAN%20Draft%20Law%202nd%20Revision%20.pdf*

Considering the changes that have taken place starting from the smartphones and tablets to the Snowden revelations, it is baffling to see the government being so naive and failing miserably to implement the draft data protection bill 2005 with much needed alterations.

The Electronic Transactions Ordinance (ETO) 2002 was enacted by the military government of General Pervez Musharraf, but does not cover protection of personal data or digital communications, rather it criminalises "unlawful or unauthorised access to information". Section 36 of the ETO states:

"Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both."

The Prevention of Electronic Crimes Act (PECA) 2016 was passed by the National Assembly in April 2016 and the Senate approved it in July 2016. It received the formal assent of the President of Pakistan and was enacted as gazetted law on August 18, 2016. The law is controversial, yet significant in terms of governing Pakistani cyberspace. The law provides for the federal government to designate an investigation agency, which is the Federal Investigation Agency (FIA), to investigate technology driven offences. As given in the law, the agency will "establish its own capacity for forensic analysis of the data or in information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency". Powers of an investigating officer include access and search of information system and use equipment to make copies of the data. [16]

16. *National Assembly. The Prevention of Electronic Crimes Act 2016. http://www.na.gov.pk/uploads/documents/1472635250_246.pdf*

b. Laws governing digital surveillance in Pakistan:

Pakistani laws legitimise interception of digital communications, monitoring and tracking of digital data transmission through technology infrastructure under the pretext of national security. Section 54 of the Pakistan Telecommunication Act, 1996, under national security threat, enables the federal government to authorise any person or persons to intercept calls and messages or to trace calls through any telecommunication system.[17]

Moreover, the legal framework ambiguously provides the procedure of seeking approval from higher courts for carrying out surveillance on communications. The Investigation for Fair Trial Act (IFTS), 2013 permits Inter-Services Intelligence (ISI), the three Services Intelligence Agencies, Intelligence Bureau (IB) and Police to apply to a High Court judge for secret warrants authorising electronic interception, surveillance, and seizure of equipment. The law only kicks into action if the suspected individual's action relates to a terrorism related offence covered under the IFTA 2013. The law also makes it impossible for the service providers to deny the government access to their data. A service provider will have to pay a fine of up to 10 million rupees if it fails to comply with a request for access to data made under a warrant for surveillance authorised by the act.

c. Digital surveillance and global human rights standards

The right to privacy is comprehensively covered under global human rights law. Privacy rights provide an important safeguard of individual autonomy and human dignity, as it allows individuals to make choices about how they live their lives.[18]

17. *National Assembly. The Pakistan Telecommunication (Re-organization) Act, 1996. http://www.na.gov.pk/uploads/documents/1329727963_180.pdf*
18. *Nyst, C. (2013). Internet rights are human rights: The right to privacy handout by APC. http://itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_Privacy_Handout.pdf*

According to Universal Declaration of Human Rights (UDHR), "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The same is reiterated in International Covenant on Civil and Political Rights (ICCPR). Nonetheless, it also introduced the exception of "lawful interference" and "lawful attacks to honour and reputation". This indicates that privacy rights are not absolute, but the states may limit the set of rights for protection and enjoyment of other fundamental rights. However, these lawful interferences must occur under prescribed circumstances, and must meet the requirements of:

i) in accordance with the law;
ii) pursue a legitimate aim; and
iii) necessary in a democratic society. [19]

However, the states have been found guilty of overstepping the boundaries of the right to privacy by employing sensitive surveillance technologies through communication infrastructures, and enacting disproportionate laws to circumcise right to privacy that provide legitimacy to their unjustified surveillance. The Special Rapporteur on the right to privacy Joseph Cannataci, in his annual report to the Human Rights Council (HRC) in February 2017, has drawn "an urgent and immediate attention to the worrying practice in some states concerning the use of privacy laws to muzzle the investigative journalism." [20]

Former Special Rapporteur on freedom of expression and opinion Frank La Rue also explored the relationship between free expression and right to privacy. In his annual report to 23rd session of HRC, he concluded that "the states cannot ensure that individuals are able to freely seek and receive information, or express themselves without respecting, protecting and promoting their right to privacy.

19. *Nyst, C. (2013). Op. cit.*
20. *OHCHR. Report of the SR on the right to privacy. Joe Cannataci. A/HRC/34/60. 34th session of UN Human Rights Council. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A_HRC_34_60_EN.docx*

Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and standards to ensure privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subjected to States' scrutiny." La Rue also concluded, "States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for States surveillance purposes or prohibiting the use of encryption."[22]

Further building upon La Rue's work, Professor David Kaye, the SR on freedom of expression and opinion worked on his first report to the UNHRC on the importance of encryption and anonymity for free expression and opinion. Underlining the use of encryption technology, Kaye said, "Where the States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment." He concluded that encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.

Kaye also addressed the question of drawing balance between human rights and the legality of possible interference. He suggested for the State practice and other relevant stakeholders that the national laws should recognise that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to

21. *OHCHR. Report of the SR on the promotion and protection opinion and expression. Frank La Rue. A/HRC/23/40. 23rd session of UN Human Rights Council. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf*
22. *OHCHR. Op. cit.*

use the technologies to secure their communications. [23]

Arbitrary interference is regarded as a serious threat to exercise of fundamental rights. In many countries, it has been found hindering in the work of HRDs and activists. UN General Assembly passed resolution in December 2016, called 70/161, also discouraged the States to enact laws impacting the freedoms of HRDs. "Information and communication technologies are not used in a manner that amounts to arbitrary and unlawful interference with privacy of individuals or the intimidation of human rights defenders", the resolution calls on the States.[24]

d. Digital surveillance on journalists & human rights defenders

Journalists and HRDs have a growing concern over continuous monitoring and interception of their communications by both the State and non-state actors.[25] Journalists have been one of the major victims of phone tapping by the State to trace out their sources, and to know about whistleblowers and political figures who frequently contact and share information with leading journalists. In a similar attempt in August 2015, the PML-N government had prepared two lists of journalists for intercepting telephonic conversations of 27 journalists including Arif Nizami, Hassan Nisar, Saleem Bukhari, Asad Kharral, and others.[26]

23. *FreedEx. Report of the SR on the promotion and protection opinion and expression. David Kaye. A/HRC/29/32. 29th session of UN Human Rights Council. https://freedex.org/encryption-and-anonymity/*
24. *Human rights defenders in the context of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms. A/RE/70/161. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/161*
25. *Express Tribune. (2012). Journalists highlight cyber intrusion, surveillance. https://tribune.com.pk/story/391805/journalists-highlight-cyber-intrusion-surveillance/*
26. *Zain, A. (2015). Government tapping phone calls of 27 noted journalists: Report. Daily Pakistan Global. https://en.dailypakistan.com.pk/pakistan/government-tapping-phone-calls-of-journalists-claims-newspaper-reporter-675/*

Interception of telephone calls is not only a source of intimidation for the journalists but also for their sources who share unauthorised information of public interest for ensuring transparency. Situation is not much different for human rights defenders because they often have been working on human rights related violations where often the perpetrator would be the government or its inline departments.[27]

e. Protection of journalists & human rights defenders

Pakistan has been ranked the fourth most dangerous country in the world on journalists protection index with a total of 115 assassinations since 1990 . On World Press Freedom Index of 180 countries, Pakistan is ranked at 139th position out of 180 countries.[29] The situation of human rights violations remained worst for so many years. According to Human Rights Commission of Pakistan's annual report 2016, the levels of self-censorship have risen manifolds. There have been reported killings of at least 3 HRDs, 6 journalists and a blogger only in 2016.[30] In general, it has brought a progression in the environment of intimidation among media and non-governmental organisations particularly working on human rights.

The emerging trends of technology driven violence against journalists and HRDs demand a certain level of anonymity and security of their online activities. It has become much easier for tech-enabled perpetrators in virtual spaces to trace down another individual in physical spaces following his or her digital footprints, which is also referred as 'targeted digital attacks'. Professor Ron Deibert, the director of Citizen Lab at Munk School of Global Affairs, University of Toronto writes, "these targeted digital attacks have become a more

27. *Imran, M. (2017). More than 1000 human rights defenders killed, harassed in 2016. The News. https://www.thenews.com.pk/print/177449-More-than-1000-Human-Rights-Defenders-killed-harassed-in-2016*
28. *Journalists and media staff killed 1990 – 2015. International Federation of Journalists. http://www.ifj.org/fileadmin/documents/25_Report_Final_sreads_web.pdf*
29. *Pakistan. World Press Freedom Index 2017. Reporters Without Borders. https://rsf.org/en/pakistan*
30. *HRCP Annual Report. (2017). State of human rights in 2016. http://hrcp-web.org/hrcpweb/wp-content/uploads/2017/05/State-of-Human-Rights-in-2016.pdf*

common threat across the civil society landscape, especially for journalists. It is important for every journalist to be aware of the character of targeted digital threats and how to equip him or herself for safe and secure digital communications."[31]

In Pakistan, there have been examples of this targeted digital attacks that ended up with life attempts. Renowned journalist and anchorperson of the most rated current affairs programme on Geo New, Hamid Mir blamed intelligence agency for attack on him where he received six bullets. Luckily he survived, but later in an interview with BBC, he said that the elements that are spying on journalists' movement and tap the telephone calls are responsible for this attack because they can better identify the place to attack. He said, he was actually pointing out at the presence of "ISI within ISI".[32]

Another trend of being monitored online relates to digital harassment and cyber-bullied by non-state actors or cyber armies being operated by political or non-political groups. According to UNESCO's report prepared by its division for Freedom of Expression and Media Development called "Building Digital Safety for Journalism", a Twitter account handle with the name Tehreek-e-Taliban threatened renowned female Pakistani journalists, as well as others, in a series of tweets, in response to their writings: such as 'These Tweets Must Stop Puking Against Taliban or We will Kill Them', or 'No Matter How Much Safe You Feel Inside Your Houses, Remember You Are Always in Our Access – Stop Propaganda Or Get Ready to Be Killed', etc.[33]

Pakistani journalist Rabia Mahmood, also fell victim of these cyber armies in 2015 when Sabeen Mahmud, a prominent human rights activist was murdered in Karachi. Ms. Mahmood had tweeted a three word rebuke against the country, and had to face online threats of rape and murder in bulk that left severe psychological impacts on her.

31. *Deibert, R. (2017). Op. cit.*
32. *The News. (2014). Those who tap journalists' phones are behind attack: Hamid Mir. https://www.thenews.com.pk/archive/print/499191-those-who-tap-journalists-phones-are-behind-attack-hamid-mir*
33. *Building digital safety for journalist Published in 2015 by the United Nations Educational, Scientific and Cultural Organization, 7, place de Fontenoy, 75352 Paris 07 SP, France. www.unesdoc.unesco.org/images/0023/002323/232358e.pdf*

She had to delete the tweet and deactivate Twitter account for a certain time duration.[34]

III. Research methodology

A mixed research framework was deemed the most appropriate approach to explore the underlying trends to best answer the assumptions. The primary research method used for the study was a survey questionnaire to assess the understanding of journalists and human rights defenders with the prevalent trends of digital surveillance in Pakistan, its impacts on their work and movement, and to gauge their level of understanding with the concept of securing digital communications and personal data. Over 150 journalists and HRD's were approached over phone calls, emails and social media to complete the survey. The survey questionnaire was distributed among 10 respondent as dry run and test the assumptions. Seven respondents responded to the questionnaire and assessing the responses, some statements were changed and then distributed for the actual results. An online survey form was created for respondents' convenience and analyses of the data. A total of 92 respondents responded to the survey out of the sample of 150.

An extensive desk review was also part of the methodology to map out the trends and identify the challenges. Basing on the trends emerging out of the literature review and survey responses, a questionnaire was prepared for in-depth interviews with two mainstream journalists and HRDs who were subject to digital surveillance in recent years.

a.Target groups

Journalists and human rights defenders in all four provinces were the target groups of this study. It was intended to receive 60% journalists and 40% HRDs responses with aggregated number of 85 responses in total. However, 92 responses were received, which is 6.44% higher than the desired number. It was aimed to take at least 20 persons from each province, however, it was difficult to complete the number from Baluchistan province for several reasons, including poor digital literacy and access to internet.

34. *Zafar, A. & Baloch, H. (2016). Op. cit.*

b. Respondents' profile

Majority of respondents aged between 26 to 42 years, of which 79.1% were males and 20.9% were females. 59.3% of the respondents were journalists and media workers, whereas remaining 40.7% were human rights defenders.

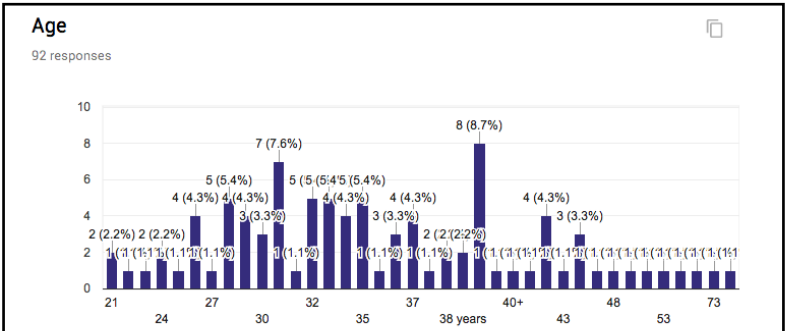


Illustration 1: Graphical summary of respondents' age group

IV. Key survey findings

The survey, in general, found that majority, 76%, of the respondents were aware of the term 'digital surveillance' with varied level of in-depth understanding. Some interpreted digital surveillance as an act of monitoring the internet and social media activities, while others believed that only phone tapping is the true reflection of this term in their context.

a. Digital surveillance breaches privacy, yet helpful for countering fake news & blasphemy issues, respondents believed

Majority of the respondents, 50%, believed that the surveillance should not be done either by the State or non-state actors because this breaches individuals' right to privacy. However, 41% of HRDs supported the idea of carrying out surveillance on digital communications. 20% journalists also believed it is helpful for countering issues related to fake news and blasphemy content online. HRDs also believed that privacy of individuals should be taken into consideration while conducting surveillance. 15% outrightly called it unethical and unlawful.

b.Media groups & civil society express least interest in digital safety

The survey responses showed that media and civil society organizations, and individuals did not pay heed to secure online communications. Majority of the respondents, 81.1%, answered that they never incorporated digital hygiene practices to protect their online communications. However, it was interesting to note that majority of female respondents had received basic level of digital security trainings, but only 32% were using secure online communications tools. Similarly, the literacy on email encryption was 68% higher in women than men.

c.Digital surveillance circumcises freedoms of expression and of movement.

The responses showed that the majority of journalists and HRDs, 83.4% collectively, believed that digital surveillance restricted their right of freedom of expression, whereas 75.8% believed that their freedom of movement was also hampered. One of the respondents also told that he had to change the house and office locations a few times due to surveillance.

d.Digital surveillance results in self-censorship and source disconnection

Majority of respondents, more than 63% collectively, believed that they had deleted or manipulated the actual content or information due to the fear of being surveilled digitally. Around 40.4% journalists and HRDs also lost their stories, content or sources. Sources of news are considered pivotal for any journalist and HRD. While answering the question related to the impacts of digital surveillance on source access, more than half of the journalists, 50.6%, responded that it resulted in complete disconnection or loss of sources.

V. Trends and challenges of digital surveillance

a.Understanding with digital surveillance

The survey results overall suggest pretty good familiarity of journalists and HRDs with term "digital surveillance". Around 77% of the respondents agreed to assumption that digital surveillance is a fact in Pakistan, being carried out through phones, emails, social media, computers, etc. Only 6.5% disagreed whereas 16.3% expressed probability of digital surveillance's existence in the country (See Illustration 2).

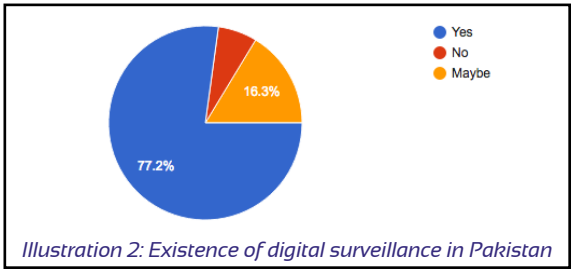


Illustration 2: Existence of digital surveillance in Pakistan

Majority respondents, 50%, rejected the idea of carrying out digital surveillance, while 29.3% responded in 'Yes', and 20.7% were not sure about its risks and benefits, hence responded in 'May be' (See Illustration 3).

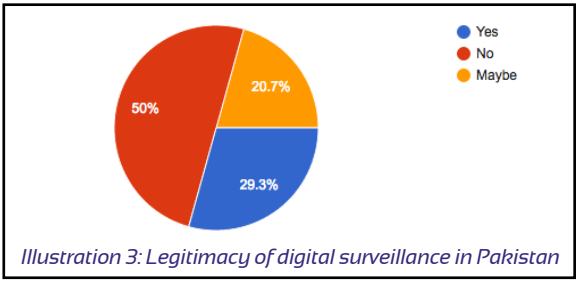


Illustration 3: Legitimacy of digital surveillance in Pakistan

Around 33.3% of the respondents said that they knew about the legal framework governing digital surveillance in Pakistan. When asked to name a few, most of them referred to PECA 2016. A few also named IFTA 2013. 66.7% did not know about the laws permitting or granting powers to LEAs to carry out digital surveillance on citizens (See Illustration 4).

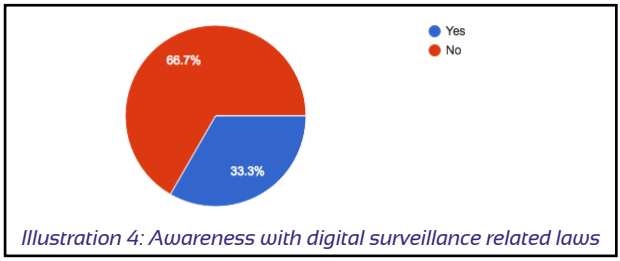


Illustration 4: Awareness with digital surveillance related laws

b.Impacts of digital surveillance on journalists & HRDs' professional duties

The survey also included sufficient numbers of questions to gauge the impact of digital surveillance on the work of journalists and HRDs. Around 45.7% respondents believed that they were subject of digital surveillance, and their privacy of communications was being compromised through emails and phone conversations. 54.3% responded in negation (See Illustration 5). When they were asked about the impact of the surveillance on their lives, most of them had received threats on cell phones. Some journalists responded that they would 'avoid' talking to their sources on phones. Some of them said surveillance can be life threatening at times therefore; they would 'avoid' exchange of sensitive information in telephonic conversations.

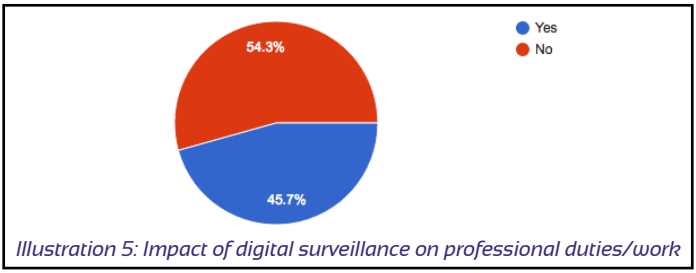


Illustration 5: Impact of digital surveillance on professional duties/work

A sweeping majority, over 87.2% believed that State institutions, including Pakistan Telecommunication Authority (PTA), interior ministry, civil and military agencies were involved in carrying out digital surveillance whereas a small proportion of respondents, 12.8%, felt that non-state actors also carried out surveillance on their digital communications (See Illustration 6). When asked about data theft, only 11.1% responded in affirmation, and of these majority said the perpetrators were unknown. 34.1% respondents faced hacking of email accounts, whereas 65.9% said they had never been a victim of email hacking. The ratio of HRDs was comparatively higher than the journalists being victim of hacking.

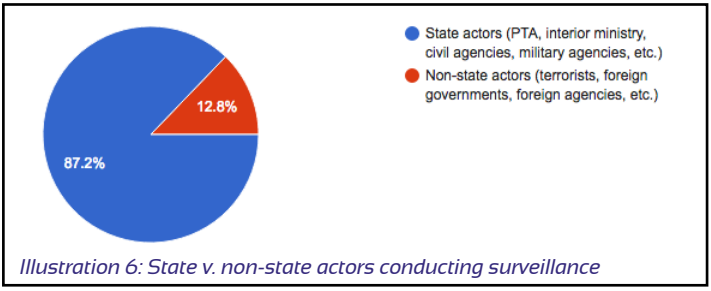


Illustration 6: State v. non-state actors conducting surveillance

Responding to the question of phone tapping, 46.7% respondents believed they were also victim of phone tapping; 21.7% said "No" and 31.5% said they were 'Unaware' of any phone tapping (See Illustration 7). Out of 46.7% respondents who said 'Yes' they were victim of phone tapping, majority, 94.7% believed phone tapping was done by the State institutions. Only 5.3% said foreign governments, foreign agencies or terrorists were also tapping their telephones.

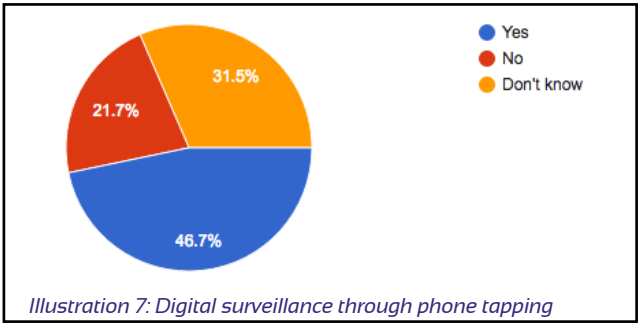


Illustration 7: Digital surveillance through phone tapping

On the question of seeking legal recourse, only 4.3% respondents said 'Yes' they sought legal recourse. One of them, also received threats from the perpetrator.

A large number of respondents, 79.4%, said they faced psychological impacts due to digital surveillance. A significant number, 34.9%, also faced social impacts while 7.9% faced legal impacts of digital surveillance.

c. Impacts of digital surveillance on freedom of expression and of movement

Questions related to impacts of digital surveillance on freedoms of expression and of movement were asked in the survey to examine the cause and effect relationship. These included questions related to any intimidation resulting in quit from journalism or activism; manipulation of facts during storytelling or documenting human rights violation cases; data theft or loss; source disconnection; switching off telecommunication devices during in-person meetings with sources, change in communication patterns, and organizational policies to prevent digital surveillance and improve data protection.

This section was key for the study, and presented a clear picture of impacts of digital surveillance on journalists and human rights defenders' expression and free movement. 83.7% respondents said their expression was affected by the digital surveillance, only 6.5% said 'No' and 9.8% were 'Unsure' of any relationship between digital surveillance and freedom of expression (See Illustration 8).

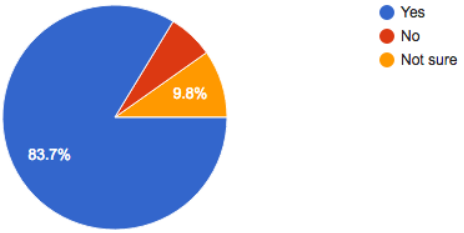


Illustration 8: Cause & effect relationship of digital surveillance & expression

A similar pattern was also witnessed when the respondents were asked if their freedom of movement was affected by the digital surveillance. 75% said 'Yes', 10.9% said 'No' and 14.1 were 'Unsure' about any relationship between these indicators (See Illustration 9).

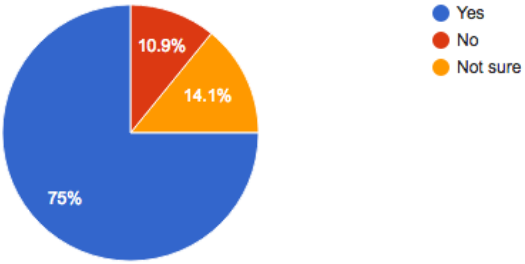


Illustration 9: Cause & effect relationship of digital surveillance & freedom of movement

Despite all impediments and limitations to their freedom of expression and of movement during the line of duties, both the journalists and human rights defenders were committed to their professions, which is reflected through their responses. More than two-third, 68.5%, said they never thought to give up on their professions.

However, the alarming trend in this section was that they were also found manipulating or altering the facts and self-censoring the original content. 64.1% respondents said they were deleting and editing the actual information due to fear of surveillance on their digital communications and data (See Illustration 10). Two-third is a substantial number and profusely testifies the assumption of digital surveillance being the major reason of self-censorship by the journalists and human rights defenders.

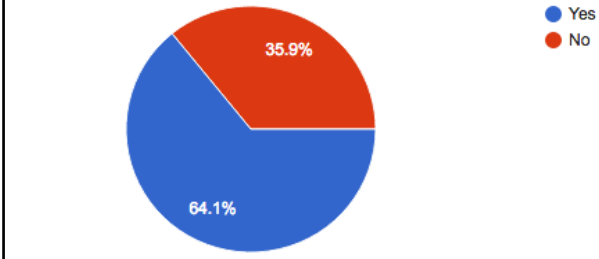


Illustration 10: Journalists & HRDs self-censoring information/news

To the question of loss of information, digital content or source, only 40% responded similar instances whereas 60% responded in 'Negative'. However, 50% expressed their apprehension of losing or disconnecting from their sources because of digital surveillance. 37.8% were 'Unsure' about this whereas 12.2% responded in 'Negative'. More or less the same respondents who had expressed their apprehensions of losing their sources also said they changed their communications methods to prevent any risk to their sources. 62.2% responded in 'Yes' whereas 37.8% said 'No'. To the question of switching off communications gadgets during in-person meetings or conversations, 38.5% respondents said they exercised this practice, whereas 61.5% responded in 'Negative' (See Table 1).

(Table 1: Responses on assumption related to impacts of digital surveillance)

Assumption	Yes	No	Unsure
Loss of information, content or source?	40%	60%	-
Disconnection with source?	50%	12.2%	37.8%
Switching off mobile phone/tablets during in-person meetings?	38.5%	61.5%	-

To quantify organizational interest in securing digital communications of their employees (journalists and human rights defenders), the numbers were generously discouraging. 76.1% outrightly re-

sponded in 'Negative', whereas only 23.9% said their media houses or non-governmental organizations were serious about the security of their digital communications.

Regarding protection of digital data, again an overwhelming majority of respondents, 85.4%, said their organisations were not interested in security of their data, whereas remaining 14.6% respondents said their organisations had internal security protocols, standing operating procedures (SOPs), or information and communication technology (ICT) policies in place. Regular data backups and use of updated anti-viruses was also part of their internal IT protocols.

d. Digital surveillance and secure online communications tools

To understand some advanced level of digital literacy of journalists and human rights defenders, particularly with reference to our subject of interest i.e. digital surveillance, and use of digital security tools to secure online communications, a set of questions was also made part of the questionnaire. 81.3% of the respondents never heard about malware FinFisher, which exists in Pakistani internet spaces.[35] Only 18.7% responded in 'Positive', whereas remaining did not know about this intrusive spyware. 25.3% respondents said that they knew about digital security tools to protect online privacy and communications, whereas 74.7% responded in 'Positive'. Of these 25.3%, when asked about the tools they were using to secure their online communications, majority named WhatsApp, Signal and Strong Passwords. A few respondents were also using Telegram, Proxy Servers, Incognito Windows, Tor Browser, JITSI Meet, KeePass, Encryption for emails, and Two-factor authentication. Only 33% respondents said they had attended digital security trainings, whereas 67% did not encounter digital security sessions. The ratio of respondents who incorporated digital hygiene after receiving digital security trainings was almost 40% low.

35. *Haque, J. (2014). Customer 32 – who used FinFisher to spy in Pakistan. Dawn. https://www.dawn.com/news/1127405*

In comparison to responses of previous questions, 19.8% said they had incorporated secure communication practices, whereas 80.2% had responded in 'Negative'. Almost 50% of the respondents said that they knew about email encryption.

Assumption	Yes	No	Unsure
Did you hear about FinFisher?	18.7%	81.3%	-
Digital security tools?	25.3%	74.7%	-
Attended digital security training?	33%	67%	-
Using digital security skills?	19.8%	88.2%	-
Do you know email encryption?	50%	50%	-

(Table 2: Responses on questions about awareness with digital security)

e.Self-censorship: Journalists v. human rights defenders

Regarding self-censorship and manipulation of facts, HRDs' group was imposing more restrictions on free expression and opinion due to the fear and the entailing consequences of digital surveillance. Around 47% HRDs responded that they had been manipulating or restricting their expression, whereas 36% journalists were compromising on their expression. This trend is also suggestive of the fact that HRDs were more prone to digital surveillance than the journalists. One of the important reasons for self-censorship was also the fear of losing source or putting the life of source in danger.

f. Digital literacy: Journalists v. human rights defenders

One of trends that relates to digital literacy and seriousness of securing digital communications and data emerged from comparative analysis of responses received from journalists and HRDs. Very surprisingly, majority of HRDs, 41%, supported the idea of surveillance on communications platforms without compromising the right to privacy. This trend was a bit complex to understand as it simultaneously pointed out to two possibilities;

a) Either the lack of awareness of HRDs about surveillance issues and privacy rights; or

b) They actually referred to the need of drawing balance between protection of right to privacy and lawful surveillance of communications.

Nevertheless, they argued that due to fragile security situation and threats from external enemies, digital surveillance was useful to monitor their online activities of criminals and terrorists. They seemingly borrowed the argument from the State narrative who has been using the 'national security' lingo excessively as an eyewash for enacting legislations and policies to circumcisie fundamental rights. For example, digital surveillance was legitimised by the government through the IFTA 2013 whereby overbroad surveillance powers were granted to civil and military intelligence agencies. Similarly, PECA 2016 was promulgated to combat internet driven crimes, however, it also allows to restrict online expression and remove online content arbitrarily to protect 'national security'. Around 20% journalists also expressed the same opinion.

Regarding literacy on surveillance technology, 93% journalists were ignorant of intrusive malwares such as FinFisher. HRDs' group was relatively more informed than the journalists about these technologies being used by the States to intrude into digital devices and act as surveillance agents for leaking out passwords and private data, and for creating backdoors.

To the question where the respondents were asked to identify laws that were governing digital surveillance in Pakistan, majority who named any law belonged to HRDs group. They comprised 50% whereas 23% journalists referred to any law related to digital surveillance in Pakistan. Almost 20% journalists responded that they had been victim of data loss in the past while HRDs were again on higher side with 38%. Similarly, HRDs had been on the higher side when asked about data loss and victim of hacking of their e-mail or social media accounts.

Higher number of journalists, 92%, replied that their organizations were not serious in protecting their data to prevent the risks of digital surveillance, while 74% HRDs also replied the same. Overall, this trend suggested that neither media, nor civil society organisations were sensitised enough with the dangers of privacy breach of their organisational or private data of their employees. Overall, HRDs' group was more literate than journalists about the right to privacy and issues pertaining to digital surveillance.

VI. Discussion on Trends and Challenges

Trends emerging out of the survey data present a complex landscape related to digital surveillance impacting rights to freedoms of expression and of movement, self-censorship, fear, State and non-state actors' role and interest in intercepting communications and hunting for private and personal data. Digital literacy and security of human rights defenders and journalists also linked to the organisational responsibility of protecting their privacies, and of those who are associated with them.

Majority of the human rights defenders and journalists' belief that the State surveils on them for harassing them and their sources to limit their expression, and collecting information by employing arbitrary means of surveillance on their phone conversations, text messaging and emails. This trend demonstrates the State's distrust over journalists and HRDs, which is literally the reflection of on-ground hostile environment for journalists and HRDs in Pakistan. Killing of journalists and activists with impunity is a reiterated account. It has been a tooth for a tooth situation when comes to trusting the State vis-à-vis protection of their privacies. Journalists and human rights defenders are equally reluctant in posing trust in the State and its arms because they know that the State is resolute in its stance of denying their due roles in democracy strengthening in the country. Another reason is that the State is fearful of media and civil society's role of criticising and holding the State institutions accountable for their public policymaking and raising questions on its affairs pertaining to development of social sector, national security, counter-terrorism, economy, foreign relations, and other critical areas. The distrust in return of distrust puts the State in a position where it starts misusing its powers and snoops into the communications of journalists and human rights defenders, which at the end results in cultivation of fear environment and self-censorship. Azaz Syed is an investigative journalist and mentor based in Islamabad, who regularly covers defense and counter-terrorism beats.

Inter-Services Intelligence (ISI) officials contacted him in 2009 and surprised him by revealing on him an in process investigative work on a story related to the then ISI chief Lieutenant General Ahmad Shuja Pasha.

"I was astonished to know that they specifically talked about my mobile conversations and exchange of text messages with my source in the Presidency." Syed believes that digital surveillance has increased comparatively in modern era, and it has become part and parcel of journalists' lives in Pakistan who work on counter-terrorism, defense, national security, foreign affairs, Baluchistan issues and other controversial topics.

Self-censorship is a common product of digital surveillance and the State institutions are well-aware of its cause and effect relationship, which is being exploited by them purposefully. The State is in denial of breaking the status quo of its outdated narrative with regards to national security, civil-military imbalance, relationships with its eastern and western neighbours, religion, etc. Until recently, it was easier for the State to drive national discourse by manipulating economic interests and employing pressure tactics on conventional media. However, now the debate has entered into new media spaces after their emergence as powerful and primary medium of communications and expression. Syed says, "**Twitter and the Facebook are also being monitored by the State. Abduction of five bloggers on January 5, 2017, and following crackdown on political dissenters is product of this monitoring and social media surveillance. The abducted bloggers were actually criticising the State for its policies on Baluchistan, and the military."** Since then an environment of fear has overcome the openness of digital spaces as well, yet people are expressing themselves but after manipulating information because they want to vent off, Syed adds. This self-censorship is quite evident from the work of good journalists in Pakistan who despite having excellent command over their subject areas, do not reflect actually in their investigative stories. Mir believes that digital surveillance is increasingly being used in Pakistan as tool for censorship.

National security in Pakistan is a broad domain with very blurred boundaries. The State works hand-in-hand with non-state actors to further the objectives of its national security concept. Mir says a non-state actor who attacked him in 2014 used to intimidate him on phone calls every time he visited Karachi. Later the same non-state actor was found to threaten other journalists as well. Some of his aides told Mir that the perpetrator was tracking his locations via his mobile phone movements, and the State actors were providing him these tips. "**I also received threats from non-state actors when he visited Khuzdar Press Club in Baluchistan and did a TV show. The non-state actors active in Baluchistan called me on behalf of the establishment and warned for the dire consequences since they were tracking my movements"**, Mir tells. Conflict prone districts of Baluchistan province including Khuzdar, Awaran, Turbat and others are completely inaccessible for journalists and activists because of ongoing military operation. Some also interpret the situation as a case of the missing news.[36] However, Mir believes that freedom of expression is the appropriate remedy for ending the conflict and bringing the enraged nationalists into mainstream, instead of a complete media blackout.

National security term is frequently used by law makers in Pakistan, and that too without defining its scope and boundaries, such as in IFTA 2013 and PECA 2016. IFTA granted unnecessary powers to LEAs to intercept digital communications of Pakistani citizen under the ambit of national security and counter-terrorism. This legitimises digital surveillance without paying due consideration to the principles of necessity and proportionality. Syed also discusses the important principle with respect to clarity in objectives and intentions of the State to conduct digital surveillance on journalists and activists. He believes if the objectives of such surveillance are to stop terrorist activities, then there is nothing wrong. However, the case is different in Pakistan because the State is more interested in usurping peoples' right to speak and curtailing down civil liberties, Syed underlines.

36. Nasir, A. (2016). Case of the missing news. Dawn. https://www.dawn.com/news/1281641

UN Human Rights Committee after completing Pakistan's first human rights review under ICCPR in July 2017 has observed, **"the State party should review its data collection and surveillance legislation, especially PECA 2016 and bring it in line with ICCPR guidelines."** It also calls upon the State to ensure that the surveillance activities comply with its obligations under the Covenant.[37]

The Covenant's Article 17 clearly talks about any interference that is 'unlawful' and 'arbitrary interference' shall be considered privacy violation. The General Comment No. 16 of Human Rights Committee further provides the explanation of these terminologies. The term 'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant. Whereas the expression 'arbitrary interference' is also relevant to the protection of right provided for the Article 17. In the Committee's view, the expression 'arbitrary interference' can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, reasonable in the particular circumstances. It further says, **"Compliance with Article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."**[38]

37. *Human Rights Committee. Concluding observations on Pakistan's ICCPR review. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fPAK%2fCO%2f1&Lang=en*
38. *General Comment No. 16. Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation). HRI/GEN/1/Rev.9 (Vol. I)*

Nonetheless, the domestic lawmakers completely disregard these guidelines. Recently enacted PECA 2016 also provides justification for real-time collection and recording of information under Section 39. **"PECA 2016 is the Official Secret Act[39] of modern times, and the objective is the same to block information and usurp civil liberties. If this Act is implemented strictly then the State will find journalists and activists violating this law everyday"**, Syed says.

A set of concerns arises where it mentions the Authorized agency, as notified under the IFTA 2013, can intercept or carry out surveillance on communications of any person after getting permission from the Court[40]. According to Section 3 of IFTA 2013, the authorized agencies also include non-civilian intelligence agencies including the ISI and three Services Intelligence Agencies, which are intelligence wings of three armed forces. The only civilian intelligence agencies included in the list are the Intelligence Bureau and the Police. In Pakistan, it has been witnessed that questioning non-civilian intelligence agencies and holding them accountable for misuse of powers even by the higher courts is an uphill task[41].

Moreover, the language of IFTA 2013 is overbroad and employs subjective terminologies. It potentially violates the internationally recognised principles of human rights, the Constitution of Pakistan and principles of natural justice.[42] IFTA allows that the authorised intelligence agencies can seek surveillance warrants from the Court in a private hearing in chamber of the Judge against any individual without giving him or her a chance to present his or her opinion on the matter. Also the law lacks provision of any mechanism under which the individual subject to surveillance can challenge the issuance of warrants.

39. *The Official Secret Act, 1923. 1 Act No. XIX of 1923. www.fia.gov.pk/en/law/Offences/3.pdf*
40. *Investigation for Fair Trial Act, 2013. www.na.gov.pk/uploads/documents/1361943916_947.pdf*
41. *SC orders: ISI, MI granted more time to produce missing persons. https://tribune.com.pk/story/334795/sc-orders-isi-mi-granted-more-time-to-produce-missing-prisoners/*
42. *Unfair trial act. http://nation.com.pk/columns/19-Apr-2013/unfair-trial-act*

With all these apprehensions on IFTA 2013, Section 39 of the PECA is problematic when comes to accessing private data or information where another law legitimises the collection and recording of information in real-time.

These provisions in the existing legal framework grant disproportionate powers to the authorities and LEAs to go beyond the recognised global standards on digital surveillance, and make the journalists and human rights defenders more vulnerable. Moreover, the absence of fair oversight mechanisms is making the situation rather grave when comes to the State's arbitrary interference on the communications of journalists and HRDs, particularly when communicating with their sources. These insecurities have been resulting in 'pervasive form of self-censorship' and fear among them. Syed tells that the government officials give them news, and there was a time when his sources stopped taking his phone calls and responding the text messages because they knew their conversations were bugged.

"Subsequently, I changed my way of communications, and instead of talking to my sources on phone, I started meeting them in person, which at times was difficult and time consuming. But still it is my preference to meet them in-person", Syed narrates. Although secure ways of communications are available and most of them are open source, however, digital literacy and building capacity of journalists and HRDs on secure digital means is still an impediment in many ways. The survey data reflects that some of the journalists and HRDs were aware of secure communication tools, but a very few were using them. There are several reasons for this, including but are not limited to the lack of organisational interest in making it part of their communication policies, technology fear, behavioral issues and lack of digital literacy in general.

Media organisations in Pakistan are least interested in investing in security of their journalists and other staff, and incorporating digital security protocols in their organisational policies. This is why the country has witnessed higher number of attacks on journalists in recent years.[43] Similarly, the organisational email accounts of journalists are not secure from the hackers and snoopers. Mir who had compromised his email account several times, still believes his organisational account is not secure from hackers. In December 2016, the evening Indian external affairs minister Sushma Swaraj arrived in Islamabad, Mir's verified Twitter and email accounts were hacked, and a derogatory tweet about Ms. Swaraj and Prime Minister Nawaz Sharif had been tweeted by the hackers from Mir's account, saying, **"According to sources, sushma swaraj is having secret relationship with PM Nawaz Sharif and she is here to have some fun".**

43. *Mohal, S. Nawaz. (2016). Training of journalists to ensure safety & security held. Pakistan Today. https://www.pakistantoday.com.pk/2016/09/21/training-of-journalists-to-ensure-safety-and-security-held/*

Similarly, the hackers also made the personal email communications from Mir's account and bank statements public.[44]

Contrary to media groups, human rights organisations are more willing to equip their defenders and staff by their active inclusion in capacity building trainings on digital security, which is also reflected in our survey results. The ratio of human rights defenders was relatively higher than the journalists who had attended digital safety and security trainings and were also using secure communications tools and applications, including email encryption. Encryption is a bit complicated and time consuming component of digital security modules, but some of the respondents out of HRDs group also mentioned that they were using email encryptions. However, not a single respondent out of journalist group said that he or she incorporated encryption as practice to improve digital hygiene and protection of personal data. The complexity of encryption technologies is another reason of reluctance of journalists and HDRs, and other vulnerable users including sexual minorities for not incorporating it into their routine digital communications.

The State has already expressed its disproportionate interest in accessing any encrypted information which it would deem as part of any digital offense. Section 35(g) of PECA 2016 grants powers to the authorised officer to seek access to an encrypted data or information for investigation purposes. However, the law vesting powers to the authorised officer without seeking warrants from a court and without providing exceptions of journalists and human rights defenders is dangerous for their work related expression and movements.

44. *Talal, S. (2016). Hamid Mir's Twitter account hacked, private emails, bank statement leaked online. ProPakistani. https://propakistani.pk/2015/12/08/hamid-mirs-twitter-account-hacked-private-emails-bank-statement-leaked-online/*

VI. Reccomendations

a. The State and legislature

1. The State should revisit the Prevention of Electronic Crimes Act 2016 and the Investigation for Fair Trail Act 2013 to remove arbitrary and disproportionate powers from the intelligence agencies for intercepting digital communications and private data of journalists and human rights defenders in order to mitigate the risks of self-censorship and restrictions on their free movements;
2. The State should narrow down the scope of laws relating to digital surveillance, and explicitly defines situations where interception is inevitable in the pretext of national security and counter-terrorism. Strict guidelines should be introduced in the statues for seeking warrants to surveil on the communications of journalists and HRDs;
3. The State should introduce exceptions of journalists and HRDs in the statutes where the State tends to seek access to unencrypted communications and data with relation to investigation of any technology driven offense;
4. The State should end the practice of carrying out mass digital surveillance on its citizens, particularly on vulnerable groups including journalists and HRDs. Targeted digital surveillance should only be carried out in cases where the probability of digitally enabled terrorism is 'very high' and the objective is to avert the dangers of such activity and protect citizens' lives;
5. The State should introduce judicial and parliamentary oversight mechanisms to monitor the implementation of PECA 2016 and IFTA 2013 laws. It should also ensure effective redressal mechanisms to address the apprehensions related to misuse of powers by the authorised officer or investigation agency under PECA and IFTA;

6. The State should encourage the media groups and civil society to promote the culture of encrypted communications and encrypted data in order to improve safety and security of vulnerable groups and their digital communications;
7. The State should introduce secure communications training modules in public sector education institutions, especially in the journalism, and law and human rights curricula of the universities and colleges;
8. The State should respect the right to privacy of its citizens in general and the journalists and HRDs in particular in the age of technology to strengthen democracy and promote freedom of speech, access to information, source protection and free movement;

b. Media groups, civil society, journalist bodies & NGO

1. Media groups and civil society organisations should take cognizance of the massive 'arbitrary interference' by the State and non-state actors with digital communications and data of journalists and HRDs to ensure their unfettered speech and free movement, as well as the security of their sources;
2. Media groups and civil society organisations should build capacity of their journalists and HRDs to secure their digital communications and private and personal data;
3. Media groups and civil society organisations should incorporate digital security policies and SOPs in their organisational policies to avert the risks of external attacks on organisations' communication infrastructure and private data;
4. Journalist bodies and NGO networks should take measures to confront unnecessary and disproportionate vesting of powers to the LEAs and authorities to intercept the communications at judicial level;

5. Journalist bodies including Pakistan Federal Union of Journalists, press clubs, All Pakistan Newspapers Society, and NGO networks should engage the parliamentary bodies to revisit disproportionate laws authorising 'unlawful' and 'arbitrary interception' powers on digital communications and data to LEAs;
6. Journalist bodies and NGO networks should engage UN Human Rights mechanisms including Universal Periodic Review (UPR), Human Rights Committee, special mandate holders on right to privacy and protection and promotion of opinion and expression to report threats, dangers and violations related to privacy, expression, access to information and protection of sources;
7. Journalists bodies and NGO networks should engage with National Commission for Human Rights and report violations on freedom of expression and right to privacy in digital spaces.


www.bytesforall.pk


APC
IMPACT
DIA, MALAYSIA, PAKISTAN
ADVOCACY FOR CHANGE THROUGH TECHNOLOGY