GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

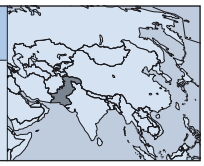
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

PAKISTAN

Pakistan dominates the surveillance hall of shame



Bytes for All, Pakistan
Furhan Hussain and Gul Bukhari
bytesforall.pk

Introduction

Nestled in the heart of South Asia, the Islamic Republic of Pakistan has had an intense history involving multiple wars, the splitting away of its eastern wing, military coups, political insurgency, ethnic cleansing and separatist movements; all in less than seven decades of existence.

Many of these afflictions have paved the way for the strengthening of institutions such as the military, resulting in the civilian system of checks and balances or oversight of these institutions becoming non-existent, while human rights violations by these powerhouses remain as rampant as before. Their reach has now also fully extended to information and communications technologies (ICTs).

Policy and political background

In 2013, for the first time in its 66-year history, Pakistan saw a democratic government complete its legitimate tenure of five years, before handing over the reins to another democratically elected government. This change came after a pattern of short bursts of democracy, followed by military dictatorships, spanning decades. Be that as it may, the military is widely understood to maintain control of certain key areas, in particular foreign policy and security. Civilian governments may not trespass on these areas. Compounding this is the non-accountability of the military establishment, with grave implications for fundamental rights, and a direct impact on communications surveillance. Civilian subordination and helplessness is epitomised by the National Commission for Human Rights Act 2012, which excludes the armed forces and the intelligence agencies from the purview of the planned commission.[1]

A parliamentarian, upon condition of anonymity, commented that today Pakistan is a security state, where a number of authorities, ambitious for control, have thrived unchecked by law. "Some intelligence agencies in Pakistan are without and beyond any law," he said, referring to the Inter-Services Intelligence agency (ISI), the military's premier spy agency believed to be highly active in illegal surveillance.[2] These sentiments are reflected in the fact that out of an ever-increasing military budget, no breakdown of portions allocated for intelligence and surveillance agencies is ever made available.[3]

Today, Pakistan is ranked as one of the most dangerous countries in the world for human rights defenders (HRDs), journalists and minorities,[4] who are threatened by acts of discrimination and violence with impunity by both state and non-state actors. According to some experts, the actions of the state suggest that it is strategically complicit in crimes committed by non-state actors, rather than being a silent onlooker.[5] Meanwhile, the massive surveillance in place – both online and off – is increasingly seen as a tool for repression, rather than meeting the government's narrative of protecting citizens from terrorism.

Surveillance in Pakistan is not just limited to the local authorities. Last year's data leaks by whistleblower Edward Snowden revealed that Pakistan is the second most spied-on country in the world.[6] The government of Pakistan determined that the country's sensitive data was at risk of being stolen by the United States (US) and decided to address the

1 FORUM-ASIA. (2013). Pakistan: Delay and uncertainty in establishing the National Commission for Human Rights. In B. Skanthakumar (Ed.), *2013 ANNI Report on the Performance and Establishment of National Human Rights Institutions of Asia*, p. 180. www.forum-asia.org/?p=16848

2 Interviewed by the authors in June 2014.

3 Sheikh, I., & Yousaf, K. (2014, June 3). Budget 2014: Govt announces 700bn defence budget. *The Express Tribune*. tribune.com.pk/story/716913/budget-2014-defence-budget-increasing-at-diminishing-rate

4 Pathak, A. (2014, May 14). PAKISTAN: Human rights defenders in Pakistan in need of defence. *Asian Human Rights Commission*. www.humanrights.asia/news/ahrc-news/AHRC-ART-036-2014; Haider, M. (2014, May 4). Pakistan most dangerous country for journalists: UN. *DAWN.com*. www.dawn.com/news/1104120; Hassan, S. (2014, May 5). Pakistan's Hindus, other minorities face surge of violence. *Reuters*. www.reuters.com/article/2014/05/05/us-pakistan-minorities-idUSBREA440SU20140505

5 Bukhari, G. (2014, May 12). Silent onlooker? No, Sir. *The Nation*. www.nation.com.pk/columns/12-May-2014/silent-onlooker-no-sir

6 CIOL. (2013, June 13). India fifth most snooped country by US, Pakistan second. *CIOL*. www.ciol.com/ciol/news/190000/india-fifth-snooped-country-us-pakistan

crisis.[7] Most recently, the Pakistani Foreign Office officially protested against the US National Security Agency's (NSA) surveillance of its left-leaning political party, the Pakistan People's Party (PPP),[8] after recent revelations about the NSA having special permission from the US government to do so.[9]

Ironically, certain Pakistani laws also permit the execution of surveillance warrants in foreign jurisdictions[10] and the state has a history tainted with instances of collaboration with foreign intelligence agencies (including the NSA)[11] as well as corporations when it comes to information surveillance and controls.[12]

The state of surveillance/surveillance state: An analysis

The constitution of Pakistan largely supports fundamental rights to privacy and freedom of expression, assembly and information, meaning mass communications surveillance is essentially illegal. Pakistan is also a signatory to the United Nations Declaration of Human Rights (UDHR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the International Covenant on Civil and Political Rights (ICCPR), each of which focuses extensively on the rights of people to privacy, assembly and free speech, without fear of judgment or persecution. Yet some legislation and extra-legislative practices put in place by various arms of the executive contravene the letter and spirit of human rights protections as laid out in the country's own constitution, as well as of those in its international obligations.

Extra-legislative surveillance

The case of murdered journalist Saleem Shahzad, who was tortured and killed after being abducted from the heart of the country's capital, demonstrates the role of secret agencies that exist without any legislative underpinnings, and their almost absolute control over surveillance. Physical surveillance (security checkpoints and CCTV) of Shahzad's route to the television studios where he was headed did not help solve his case. It was made evident in subsequent reports and analysis, including that of Amnesty International,[13] that only those who controlled these surveillance tools and apparatuses could have avoided detection. The ISI, though a prime suspect in the case, was only partially investigated by the judicial commission formed to investigate the case. Conversely, it was claimed by human rights defenders and groups that Shahzad's mobile phone records went missing for up to 15 days before his murder, although the ISI has denied it. The independent judicial commission recommendations subtly hinted for the need to make "important intelligence agencies (ISI) more law abiding through a statutory framework carefully outlining their respective mandates and roles."[14]

These recommendations led to the draft Inter-Services Intelligence Agency (Functions, Powers and Regulation) Act of 2012 being proposed in parliament, in an attempt to give the spy agency a legal status and subject it to judicial and parliamentary oversight. However, the bill, which among other things would have laid the foundations against illegal surveillance by the ISI, was withdrawn[15] – the military remains all-powerful and continues to operate the ISI in a fashion after the Orwellian secret force in Animal Farm.

7 Mirza, J. (2013, September 26). Pakistan takes steps to protect itself from NSA style cyber attacks. *The News International*. www.thenews.com.pk/Todays-News-6-204384-Pakistan-takes-steps-to-protect-itself-from

8 Haider, M. (2014, July 6). Pakistan lodges formal protest with US against PPP surveillance. *Dawn.com*. www.dawn.com/news/1116802

9 Mail Today Bureau. (2014, July 2). America gave NSA permission to spy on BJP, claims whistleblower Snowden. *Mail Online India*. www.dailymail.co.uk/indiahome/indianews/article-2677247/America-gave-NSA-permission-spy-BJP-claims-whistleblower-Snowden.html

10 La Rue, F. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/23/40). United Nations Office of the High Commissioner for Human Rights. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

11 Gallagher, R. (2014, June 14). How Secret Partners Expand NSA's Surveillance Dragnet. *The Intercept*. https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

12 Bytes for All, Pakistan. (2012, June 17). Dr. Eric Schmidt, please don't advertise surveillance to Pakistan government. *Bytes for All*. content.bytesforall.pk/node/56; The Express Tribune. (2012, June 15). Gilani seeks Google's help in tracking cross-border movement. *The Express Tribune*. tribune.com.pk/story/394128/gilani-seeks-googles-help-in-tracking-cross-border-movement; Davies, S. (2013, July 18). Pakistan government admits secret "censorship arrangement" with Facebook. *The Privacy Surgeon*. www.privacysurgeon.org/blog/incision/pakistan-government-admits-secret-censorship-arrangement-with-facebook

13 Amnesty International. (2014). *"A Bullet has been chosen for you": Attacks on journalists in Pakistan*. London: Amnesty International, International Secretariat, United Kingdom.

14 ANI. (2011, June 19). 'Prime suspect' ISI to probe Pak journalist murder case. *Yahoo News*. https://sg.news.yahoo.com/prime-suspect-isi-probe-pak-journalist-murder-case-071918521.html; Abbasi, A. (2011, June 19). ISI to probe Saleem Shahzad murder. *The News International*. www.thenews.com.pk/TodaysPrintDetail.aspx?ID=6829&Cat=13; Nisar, M., Khan, A. A., Iqbal, J., Khan, B. A., & Shaukat, P. (2012). *Judicial Inquiry Report on Saleem Shahzad's Murder*. Islamabad.

15 Zaafir, M. S. (2012, July 13). Farhatullah withdraws bill in Senate about ISI control. *The News International*. www.thenews.com.pk/Todays-News-6-120149-Farhatullah-withdraws-bill-in-Senate-about-ISI-control

Legalised surveillance?

According to the Pakistan Telecommunication (Re-organization) (Amendments) Act, 2006, the government can authorise any person(s) to intercept calls and messages, or trace location or movement through any telecommunication medium, giving the authorities a free hand to conduct communications surveillance, and with no mention of any governance parameters ensuring a due process. The ordinance also states that no cyphering hardware or software used within the country may be considered "approved" unless authorisation has been granted by the Electronic Certification Accreditation Council established under the Electronic Transaction Ordinance, 2002.[16] This suggests that the fundamental right to online privacy through encryption is subject to the approval of the authorities. According to the Pakistan Telecommunications Authority's (PTA) policy on the use of virtual private network (VPN) tunnels, use of all "non-standard modes of communication like VPNs [...] by which communication becomes hidden or modified to the extent that it cannot be monitored, is a violation," as per the Monitoring and Reconciliation of International Telephone Traffic (MRITT) Regulations 2010.[17] An interesting intersection between legal vs illegal surveillance can be observed by noting that while the PTA has legal authority to conduct communications surveillance, it denies doing so by itself.[18] Instead, it has confirmed that the ISI monitors "grey traffic" over the internet,[19] despite the fact that it has no legal mandate to do so.

Similarly, another act called the Investigation for Fair Trial Act, 2013, can be criticised for being worse than US's "Patriot Act" because it bypasses requirements for surveillance to be necessary and proportionate. The law encompasses and permits collection of all imaginable forms of data,[20] taking state surveillance of communications to previously unheard of levels. The act obviates the need to serve a warrant permitting the authorised surveillance body to collect data when the nature of the surveillance or interception "is such that it is not necessary to serve the warrant on anyone," which is vague and unspecific.[21] Further, the law takes away the option of service providers refusing to provide user data to spy agencies. Failure to cooperate by allowing backdoors into private user data, or by disclosing information about such cooperation, carries the punishment of imprisonment of one year and/or a fine of up to 10 million rupees (roughly USD 101,000). The secrecy implicit here has obvious implications for any user-notification mechanisms pertaining to the issuing of any surveillance warrant.[22]

While the Act provides for some public and judicial oversight, these are feared to remain theoretical as most operations undertaken by intelligence agencies remain beyond the reach of law and oversight as pointed out earlier. Also, the level of well-documented intimidation tactics and influence that impact on court decisions in Pakistan[23] would bear negatively on the efficacy of such oversight.

Jahanzaib Haque, editor of Dawn.com, says of the recent pro-surveillance legislation: "Due to a mixture of both fear and ignorance, parliament has passed extremely regressive legislation that leaves the public, and especially journalists, exposed to the threat of state surveillance that will inevitably result in misuse in the current form."[24]

Indeed, most known instances of harassment of civilians through surveillance, especially women politicians[25] and HRDs, have taken place without the expression of any legitimate aim and without appropriate measures. Indicative of an absolute lack of transparency, there still are few or no official records available pertaining to the procurement of advanced surveillance technologies such as FinFisher, the presence of which (in the country's cyberspace) was revealed by a detailed report published by the Citizen Lab at the University of

16 Pakistan Telecommunication (Re-organization) (Amendments) Act, 2006.

17 Pakistan Telecommunication Authority (PTA). (2010, December 2). No.17-1/2010/Enf/PTA (VPN) | Use Of VPNs/Tunnels and/or Non-Standard SS7/VoIP Protocols. Retrieved from Internet Service Providers Association of Pakistan (ISPAK): www.ispak.pk/Downloads/PTA_VPN_Policy.pdf

18 Pakistan Telecommunication Authority. (2014). PTA response. bolobhi.org/wp-content/uploads/2014/05/PTA-response.jpg

19 Abbasi, A. (2014, December 5). Grey phone traffic: IT authorities passing the buck to ISI. *The News International*. www.thenews.com.pk/Todays-News-13-27079-Grey-phone-traffic-IT-authorities-passing-the-buck-to-ISI

20 "[D]ata, information or material in any documented form, whether written, through audio-visual device, CCTV, still photography, observation or any other mode of modern devices or techniques, [...] e-mails, SMS, IPDR (internet protocol detail record) or CDR (call detail record) and any form of computer based or cellphone based communication and voice analysis. It also includes any means of communication using wired or wireless or IP (internet protocol) based media or gadgetry." Investigation for Fair Trial Act, 2013. www.na.gov.pk/uploads/documents/1361943916_947.pdf

21 Ibid.

22 Ibid.

23 Deutsche Welle. (2014, March 11). Pakistan postpones Musharraf trial amid threats from al Qaeda, Taliban. *Deutsche Welle*. www.dw.de/pakistan-postpones-musharraf-trial-amid-threats-from-al-qaeda-taliban/a-17487157; Sattar, B. (2014, April 12). Lawyer Babar Sattar critiques Pakistan Protection Ordinance. *Siyasat aur Qanoon*. (M. Pirzada, interviewer). tune.pk/video/2592131

24 Interview with Jahanzaib Haque, July 2014.

25 Dawn.com. (2011, August 5). No end to phone tapping of women MNAs. *Dawn.com*. www.dawn.com/news/649648/no-end-to-phone-tapping-of-women-mnas

Toronto.[26] A court case by Bytes for All, Pakistan attempting to resolve the questions pertaining to the elusive usage of this Trojan technology has been pending in the Lahore High Court since 2013. The Pakistani government is also known to be a client of Narus, a company that sells internet monitoring solutions.[27] Further, in an attempt to "eradicate crimes", the government has also purchased a state-of-the-art monitoring and surveillance system from a company known as GCS.[28]

According to Gulalai Ismail, a women's rights defender and chairperson of Aware Girls who is based in the conflict-affected province of Khyber Pakhtunkhwa, "Last December, when I was launching an intensive peace programme in the Malakand Division, the state agencies came to inquire about the programme. I was shocked when I was told that I and my social media communications had been under surveillance for the last three years... In my communication with the agencies it was clear that my work for peace and human rights was seen as 'anti-state', and I was seen as an enemy rather than an activist."[29]

The most recent reinforcement for conducting communications surveillance has come in the form of the Pakistan Protection Bill (PPB) 2014. Apart from legitimising a number of violations, it is essential to note that the bill discusses "crimes against computers including cybercrimes, internet offences and other offences related to information technology, etc." as scheduled offences, despite that fact that no form of cyber/electronic crimes ordinance exists in the country that could comprehensively define the nature and scope of these offences. Existing individual protection mechanisms and safeguards against illegitimate access also need re-examining in light of the current possibilities of misuse.[30]

Conclusion

The residents of Pakistan are subject to mass surveillance by local and international governments. Recent laws that focus on dealing with terrorism, such as the Fair Trial Act 2013 and Pakistan Protection Bill 2014, are feared to legitimise pernicious and wide-ranging communications surveillance.

While apparently intended to address issues arising from the war against terror and national security, surveillance has been and is being used for political reasons, leading to invasions of privacy, intimidation and blackmail, often targeted at civil society actors such as journalists and HRDs, as well as political activists and elected politicians.

Communications surveillance by intelligence agencies such as the ISI – the existence of which itself is not covered by any act of parliament and is therefore without any legal basis – is entirely extra-legal. Attempts at bringing such agencies within the purview of law have failed so far. This has grave implications for transparency and the rule of law, and has paved the way for continuing human rights violations with impunity.

Owais Aslam Ali, secretary general of the Pakistan Press Foundation (PPF), sums it up by calling the scale of surveillance in Pakistan "breathtaking". Highlighting the lack of awareness of this issue amongst the public, he says, "Right now, there's some awareness about mobile phones being risky. The awareness of the internet and email being equally dangerous has not yet permeated the journalist community... [It needs to be understood that] nothing is private [anymore]. [Without] confidentially of sources [...] all you'll be left with are different forms of press releases."[31]

Action steps

The following advocacy steps are recommended in Pakistan:

- An overarching framework needs to be developed for issues of free expression, privacy, data protection, security, surveillance, etc. Civil society should advocate for the alignment of existing fragmented pieces of ICT policies, and the drafting of a comprehensive policy through a multi-stakeholder process. Such a policy should replace the current non-transparent inter-ministerial committees that function in lieu of transparent policy.[32] The policy should ensure independent public oversight of any acquisition of surveillance technologies. Such oversight should be designed to take into account the

26 Bytes for All, Pakistan. (2013, May 1). Notorious spy technology found in Pakistan. Bytes for All. content.bytesforall.pk/node/99; Khan, A. Z. (2013, May 22). Big fish. *The News International*. www.thenews.com.pk/Todays-News-9-178951-Big-fish

27 Privacy International. (n.d.). Narus sells Internet Monitoring technology. *Privacy International*. https://www.privacyinternational.org/sii/narus/#action

28 P@SHA. (2014, April 17). GCS delivers Pakistan's largest citywide surveillance center. P@SHA. pasha.org.pk/2014/04/17/news/gcs-delivers-pakistans-largest-citywide-surveillance-center

29 Interview with Gulalai Ismail, July 2014.

30 Protection of Pakistan Ordinance, 2014. www.dhrpk.org/wp-content/uploads/2014/02/PPO-with-amendments.pdf

31 Interview with Owais Aslam Ali, 26 May 2014.

32 Bajwa, F. (2009, June 29). National Security and Surveillance - Implications for an ICT Policy. *ProPakistani*. propakistani.pk/2009/06/29/national-security-and-surveillance-implications-for-an-ict-policy

potential for human rights violations inherent in these technologies.

- Certain surveillance-focused provisions in laws such as the Investigation for Fair Trial Act 2013 that are considered predatory to human rights need to be examined against international human rights benchmarks, such as the International Principles on the Application of Human Rights to Communications Surveillance,[33] and challenged in courts of law.[34]
- With regard to international surveillance, Pakistani civil society must become active in relevant international forums to pressure foreign governments to cease mass surveillance of Pakistani citizens.[35]
- Public awareness needs to be raised regarding the risks of communications surveillance and ways to counter it through digital security tools and skills.
- Public awareness about how communications surveillance violates fundamental human rights standards needs to be raised in order to pressure the government and influence policy change.
- Civil society must lobby to bring extra-legal intelligence agencies within the purview of law.
- The link between various forms of electronic communications surveillance and offline methods of surveillance needs to be highlighted for traditional HRD organisations not necessarily well-versed in the latest issues on internet governance, online privacy, modern technology and human rights.

33 https://en.necessaryandproportionate.org/text

34 Bytes for All's petition challenging the FTA 2013 is currently under review in the Lahore High Court, Pakistan.

35 Bytes for All in collaboration with Privacy International and other international human rights groups challenged the GCHQ on mass surveillance of Pakistani citizens at the Investigatory Powers Tribunal in February 2014. See: Clark, L. (2014, January 19). Pakistani human rights group sues UK government for discriminatory GCHQ surveillance. *Wired.co.uk*. www.wired.co.uk/news/archive/2014-01/09/pakistan-human-rights-sues-uk