Submission in advance of the consideration of the periodic report of Pakistan, Human Rights Committee, 120th Session, 3 July to 28 July 2017

June 2017

1. Introduction

Privacy International (the organisation) notes the written replies by the government of Pakistan to the Committee's list of issues on Pakistan's laws, policies and practices related to interception of personal communications and protection of personal data.

The organisation remains concerned over the practices of surveillance by Pakistani intelligence and law enforcement agencies. National legislation governing surveillance is inadequate, unclear as to the powers, scope and capacity of state surveillance activities and thus it falls short of the required human rights standards to safeguard individuals from unlawful interference to the right to privacy.

In this submission, the organisation provides the Committee with their observations to the written replies of the Pakistani government and with additional, up to date information to that contained in the briefing submitted to the Committee in advance of the adoption of the list of issues in 2016 (hereinafter 2016 Submission.)[1] Unless otherwise stated, the concerns expressed then are on going and if they are not repeated here it is solely for brevity sake.

In particular, the Pakistan's National Assembly adopted the Prevention of Electronic Crimes Act (PECA 2016) on 11 August 2016. During the legislative process Pakistani and international human rights organisations criticised many provision of the bill (as summarised in the 2016 Submission). The UN Special Rapporteur on Freedom of Expression also expressed his concerns and urged Pakistan to "undertake a rigorous and thorough reassessment of the Bill to ensure its compliance with the international human rights law and standards".[2]

Regretfully some of the key concerns presented during the drafting process remained unaddressed. Some of these concerns are reflected in the following sections.

---

[1] Available at:
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fICO%2fP

[2] See OL PAK 8/2016, 8 July 2016. Available at:
http://www.ohchr.org/Documents/Issues/Opinion/Legislation/PAK_8_2016.pdf

2. Mass, indiscriminate retention of traffic data

Section 32 of PECA provides for mandatory mass retention of traffic data by service providers for a minimum of one year.[3]

This Committee has already recommended that State Parties should "refrain from imposing mandatory retention of data by third parties".[4]

This recommendation is further reinforced by the recent judgment of the Court of Justice of the European Union in the Tele2/Watson Case. Firstly, that judgment reaffirmed and expanded on the invasive nature of metadata collection in the context of the right to privacy: "That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular that data provides the means... of *establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."* (emphasis added).[5] Secondly, the Court noted that: "effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight."[6]

PECA imposes on service providers obligations to retain data indiscriminately, in violation of Article 17 of the ICCPR.

3. Government access to communications networks and limitation to encryption

As part of licensing requirements, service providers must make their communications networks 'lawful interception-compliant'. There are several ways a service provider can achieve such compliance. They can physically install on their network components that comply with various international interception protocols or, alternatively, they can install

---

[3] "32. Retention of traffic data.- (1) A service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the Court, provide that data to the investigation agency or the authorized officer whenever so required."

[4] Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014); *See also* Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1, para. 43 (27 April 2016) ("The State Party should... consider revoking or limiting the requirement for mandatory retention of data by third parties...").

[5] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment, para. 99 (21 December 2016). This position is in line with the Committee's approach to indiscriminate gathering of metada as reflected for example in Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016).

[6] *Id*., at para. 103.

external ‘probes’ somewhere along the transmission cables to allow signals carried on their network to be transmitted to monitoring facilities of requesting government agencies. Government authorities can also install high-powered probes without the knowledge or assistance of providers and gain access to the same data.

Since the creation of the Pakistan Internet Exchange - a communications system that keeps most of Pakistan’s communications within Pakistan - the majority of Pakistan’s internet traffic passes through a single core backbone with limited gateways, making it much easier to monitor internet traffic.

Censorship of online content is widespread and justified as a means to prevent the sharing of pornographic, obscene, and blasphemous material in the Islamic republic.[7] The same technologies that the Pakistani government uses for online censorship are also used for surveillance.

To this end, the Pakistani government has purchased a number of ‘packet inspection’ technologies, which can be programmed to search for particular terms, such as key words in emails.[8]

Spaces to communicate privately online are also narrowing. In 2010 and 2011, the Pakistan Telecommunications Authority (PTA) ordered all internet service providers and phone companies to ban encryption and virtual private networks (VPNs) except in limited circumstances and with the government’s permission.[9] If a company or individual wish to use encryption without being penalised, a formal request must be sent to the PTA and accepted. The PTA actively publicises its message that “non-standard means of communication” that are “hidden” or “[mechanisms] which conceal communication to the extent that prohibits monitoring” are presumptively illegal.

Although no one is known to have been arrested for using encryption, human rights activists fear that Pakistani security agencies are watching people who use encryption to protect their communications.[10]

---

[7] “Pakistan’s Internet Landscape”, Bytes for All Pakistan, November 2013, http://content.bytesforall.pk/sites/default/ les/MappingReportFinal%20-%20Published.pdf

[8] Packet inspection technologies examine the constituent pieces of data that make up internet and communications traffic as they pass inspection points in the internet architecture, searching for signatures that the technologies recognize as abnormal, such as viruses and spam. For details of these technologies as they are employed in Pakistan, see Privacy International, Tipping the Scales: surveillance and security in Pakistan, https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%20150721_0.pdf

[9] A copy of the 2010 directive, which has the subject line “Use of VPNs/Tunnels and/or Non-Standard SS7/VoIP Protocols” and is dated 2 December 2010, is available at http://www.ispak.pk/Downloads/PTA_VPN_Policy.pdf. A copy of the 2011 directive, which has the subject line “Usage of Encrypted VPNs” and is dated 21 July 2011, is available at http://twicsy.com/i/NoxrL.

[10] See: *Securing Safe Spaces Online: Encryption, online anonymity, and human rights*, pp. 13, published by Privacy International, ARTICLE 19, and the International Human Rights Clinic (IHRC) at Harvard Law School. Available at: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_2.pdf

As the UN Special Rapporteur on Freedom of Expression has noted, *"Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attack*".[11] The Human Rights Council resolution on the right to privacy in the digital age, adopted in March 2017, calls upon states not to interfere with the use of encryption technology, *"with any restrictions thereon complying with States' obligations under international human rights law."* The almost total ban on encryption in Pakistan fails to comply with such obligations.

Further, as noted in our 2016 Submission, PECA contains a provision that allow an authorised officer to "require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence." (Section 35(g).)

Privacy International acknowledges that a judicial authorisation is needed before the authorised officer can require a key disclosure. However, the organisation remains concerned at the lack of judicial oversight of the implementation of this provision and the risk that such disclosure of encrypted communications may pose, including to the right not to incriminate one selves, if directed against a person suspected of a criminal offence.

As noted by the UN Special Rapporteur on the freedom of expression, "key disclosure or decryption orders often force corporations to cooperate with Governments, creating serious challenges that implicate individual users online. [...] In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight."[12]

4. Intelligence sharing

Section 42 of PECA allows for cooperation between the Federal Government and foreign governments, foreign agencies and others, including by permitting the Federal Government to forward information obtained from investigations under the Act to foreign agencies.

This broad power to share information with foreign entities is of significant concern. It covers "any information obtained from its own investigations" with "information" defined broadly under the Act to include "text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) and codes including object code and source code" (See Article 2 Definitions, (xix).)

---

[11] UN Doc. A/HRC/29/32, paragraph 16.
[12] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/29/32, 22 May 2015, paragraph 45.

The information shared could include particular sensitive information about individuals or large quantities of data involving significant numbers of people.

To share such information will all be at the sole discretion of the Pakistani government: no requirement of judicial authorization, either from the requesting foreign government or Pakistan; nor in fact any prior request from the foreign entity would not be required to exercise this power.

Privacy International notes that the government of Pakistan considers this provision "in line with the Budapest Convention and does not require any judicial authorization or oversight for its implementation."(see replies to the list of issues). Given the wide scope (covering inter alia content and communications data) and the unfettered discretion given to the government to share private information, Privacy International believes that this provision goes well beyond what may be required in order to implement under the Budapest Convention.

Significantly, this poses significant risks to the right to privacy. As noted by UN human rights experts, including the UN Special Rapporteur on counter-terrorism and human rights and this Committee, lack of adequate regulation of intelligence sharing have resulted in the sharing of individual's communications with foreign agencies without appropriate safeguards.[13] This Committee has specifically recommended that a robust oversight system over intelligence-sharing, is in place, "including by providing for judicial involvement in the authorization of such measures in all cases".[14]

As noted in our 2016 Submission, the US National Security Agency (NSA) especially values its relationship with Pakistan as one of the approved third party SIGINT partners. The Pakistani government is by far the largest known recipient of NSA funds.[15] Privacy International's 2015 report summarises the programs used (XKeyscore, Fairview), the type of communications intercepted (content and metadata) and the scale of NSA-led surveillance of communications in Pakistan.[16]

Despite some protests by Pakistani authorities when the scale of mass surveillance was revealed, no independent investigation has been initiated.[17]

---

[13] See report of the UN Special Rapporteur on counter-terrorism and human rights, UN doc. A/69/397, 23 September 2014.

[14] See Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015.) See also Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7, paras. 36-37 (28 April 2016); Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6 (13 August 2015).

[15] "FAD FY 12 CCP Funding of Partners", National Security Agency slide reproduced in Glenn Greenwald, No Place to Hide, p. 124. http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf

[16] Privacy International, Tipping the Scales: surveillance and security in Pakistan, https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%20150721_0.pdf

[17] In 2013, Pakistani Senators expressed concern after initial revelations about the scale of NSA surveillance in Pakistan ("Report of the Senate Committee on Defence and Defence Production", Senate of Pakistan, August-September 2013, http://www.senate.gov.pk/uploads/documents/1378101374_113.pdf), and in 2014, the Pakistani Foreign Office of officially protested against the NSA's surveillance of the Pakistan People's Party

5. Lack of adequate data protection legislation

Despite the current lack of a comprehensive data protection law, Pakistan has one of the world's most extensive citizen registration regimes, known as National Database & Registration Authority (NADRA), which was established in 2000 with plans in advanced stage to replace all the existing cards with biometric cards, containing biometric data such as iris scans, fingerprints (both hands); a photograph taken at a NADRA centre, and a scan of the citizen's personal signature.[18]

Since its adoption and with its expansion over the years, there have been regular reports of NADRA's data being breached as well as reports of corruption at NADRA centres, where the biometric verification/application process can be bypassed as well as concerns of misidentification errors and forgery.[19] For example, in 2010, the Shah Faisal, Karachi, branch of NADRA reported a data breach that resulted in the theft of "computers and other equipment", including hard drives. The data breach was low-tech, and involved a physical break-in. In 2014, NADRA reportedly received a report from the head of the ISI concerning the possibility of data leaks through the Pakistan government's reliance on third party companies database and verification software and hardware.[20]

Further, SIM card registration is mandatory in Pakistan. Unlike in most countries with mandatory registration, SIM cards are also biometrically verified against NADRA. According to the latest figures available, as of March 2015, 68.7 million SIMs had been biometrically verified out of 103 million SIMs in use at that time. [21]

6. Conclusions

Based on the above observations and those contained in the 2016 Submission, Privacy International proposes the following recommendations to the Pakistani government:

- Review the laws governing surveillance in Pakistan, notably the Prevention of Electronic Crimes Act, to ensure they comply with the International Covenant on Civil and Political Rights, including article 17;

(PPP).("Pakistan lodges formal protest with US against PPP surveillance", DAWN, 6 July 2014, http://www.dawn.com/ news/1116802). In contrast, civil society in and out of Pakistan reacted vehemently to the revelations (See for example "Pakistan responds to the NSA Surveillance of PPP", Digital Rights Foundation, 8 July 2014, http://digitalrightsfoundation.pk/2014/07/pakistan-responds-to-the-nsa-surveillance-of-ppp/ and "Press Freedom Groups Denounce NSA Spying on AJ Bureau Chief", Inter Press Service, 12 May 2015, http://www.ipsnews.net/2015/05/press-free- dom-groups-denounce-nsa-spying-on-aj-bureau-chief/).

[18] See: https://www.nadra.gov.pk

[19] See Privacy International, *Identity theft persists in Pakistan's biometric era*, 22 July 2014. Available at: https://www.privacyinternational.org/?q=node/334

[20] See Hussain, D., *NADRA warned: Fears raised over potential data leaks to hostile agencies*, 14 September 2014. Available at: https://tribune.com.pk/story/956305/nadra-warned-fears-raised-over-potential-data-leaks-to-hostile-agencies/

[21] Pakistan Today, *National Action Plan: 53 million SIMs verified via biometric system*, 22 February 2015. Available at: http://www.pakistantoday.com.pk/2015/02/22/national-action-plan-53-million-sims-verified-via-biometric-system/

- Establish independent accountability mechanisms and clear standards for Pakistan's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;
- Review the laws and practice of intelligence sharing with foreign agencies to ensure its compliance with the right to privacy, under Article 17 of the Covenant. In particular, the Government should aim to ensure greater transparency surrounding intelligence sharing arrangements, subject such arrangements to detailed primary legislation and parliamentary scrutiny, and establish independent oversight mechanisms to prevent abuses in the course of these arrangements and to ensure that individuals have access to effective remedies.
- Review all licensing requirements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international human rights standards, in particular in relations to requirements for blanket, indiscriminate data retention;
- Dismantle the legal regime that require state permission to use encryption or anonymity tools, and ensure its laws, policies, and practices that affect use of encryption and online anonymous speech are consistent with its international human rights obligations;
- Adopt and enforce a comprehensive data protection law.