PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
28th Session – Pakistan

The Right to Privacy in the Islamic Republic of Pakistan

Submitted by Privacy International

March 2017

PRIVACY INTERNATIONAL

Introduction

1. This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. Privacy International wishes to bring concerns about the protection and promotion of the right to privacy for consideration in Pakistan's upcoming review at the 28th session of the Working Group on the Universal Periodic Review.

Follow up to the previous UPR

3. In Pakistan's previous review, no express mention was made of the right to privacy in the context of data protection and communications surveillance in the National Report submitted by Pakistan or the report of the Working Group.

4. However, concerns on the right to privacy in relations to privacy, communications surveillance and data protection were expressed by stakeholders.[1]

Domestic laws related to privacy

5. The Constitution of the Islamic Republic of Pakistan[2] accords the right to privacy as a fundamental right. Article 14(1) of the Constitution confirms that "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable."

6. As a fundamental constitutional right, the right to privacy is meant to take precedence over any other inconsistent provisions of domestic law as upheld by Article 8 of the Constitution.[3]

7. Yet Pakistan's Constitution also includes a wide-ranging exception to the primacy of fundamental rights. The provisions of Article 8 do not apply to

1 A group of NGOs raised concerns regarding challenging of protection citizens' information online and privacy with Pakistan currently hosing the world's largest online biometric database of its citizens as well as the expansive policies and practices of the Pakistani government to enable it to implement a massive surveillance regime in the name of national security and the fight against terrorism. See: A/HRC/WG.6/14/PAK/3. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G12/156/22/PDF/G1215622.pdf?OpenElement

2 http://www.pakistani.org/pakistan/constitution/part2.ch1.html

3 Article 8 reads "[a]ny law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred [under the Constitution], shall, to the extent of such inconsistency, be void." Article 8 (5), furthermore, states that "The rights conferred by this Chapter shall not be suspended except as expressly provided by the Constitution."

any law relating to the 'proper discharge' of the duties of the Armed Forces or the police. The breadth of this exception is troubling, especially given the central role that the Armed Forces have historically played in Pakistan's domestic political landscape.[4]

International obligations

8. Pakistan has ratified the International Covenant on Civil and Political Rights (ICCPR)[5] and the Convention on the Rights of the Child (ratified November 1990)[6], which both uphold the right to privacy. Furthermore, Pakistan has signed Cairo Declaration on Human Rights In Islam (signed August 1990) which also upholds the right to privacy.[7]

AREAS OF CONCERN

I. Communications surveillance

9. Surveillance across all of Pakistan's communications networks is becoming more widespread. Intermittent but devastating attacks within Pakistan's major cities by armed groups, such as the 2014 Peshawar school attack by a Taliban-affiliated group, have been cited as a reason to expand surveillance in Pakistan.[8]

10. Interception across Pakistani networks is therefore pervasive; some of it is also unlawful. A Supreme Court hearing about a case concerning phone tapping revealed that the ISI intelligence agency had tapped 6,523 phones in February, 6,819 in March and 6,742 in April 2015.[9]

11. The impact of surveillance in Pakistan by both the State and other actors has become increasingly reported on and documented by civil society groups, with some research conducted with particular groups in society such as female journalists,[10] and women.[11]

4 See: State of Surveillance (2016) published by Digital Rights Foundation and Privacy International. Available at: https://www.privacyinternational.org/node/964; and State of Privacy (2016) published by Bytes for All and Privacy International. Available at: https://www.privacyinternational.org/node/970

5 Article 17 provides that, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". The Human Rights Committee has noted that states party to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."

6 Article 16 provides that, "1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2) The child has the right to the protection of the law against such interference or attacks."

7 Article 18 provides that, "a) Everyone shall have the right to live in security for himself, his religion, his dependents, his honor and his property. (b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference. (c) A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted."

8 Privacy International (2015), Tipping the Scales: surveillance and security in Pakistan. Available: https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

9 The case, dating from 1996, was brought following evidence that the then-Chief Justice's phone had been tapped. At time of publication, no details about the procedures and process for intercepting communications had yet been publicly released. See: https://tribune.com.pk/story/904267/phone-tapping-sc-to-take-up-isis-plea-for-in-camera-hearing-on-wednesday/

10 See: Digital Rights Foundation (2016) Surveillance of Female Journalists in Pakistan. Available at: http://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf

11 Khan, S., Surveillance as a Feminist Issue, 1 December 2016, Guest feature published by Privacy International. Available at: https://www.privacyinternational.org/node/1007

Shortcomings of the legal regime

12. A number of laws regulate communications surveillance in Pakistan.

13. The Investigation for Fair Trial Act (2013)[12] allows for access to data, emails, telephone calls, and any form of computer or mobile phone-based communication, subject to a judicial warrant. However, under Chapter 2 Section 5 a warrant can be requested wherever an official has "reasons to believe that any person is likely to be associated with or is beginning to get associated with, any act leading to a scheduled office, or is in the process of beginning to plan such an act, or is indulging in such a conduct or activity that arises suspicion that he is likely to plan or attempt to commit any scheduled offence". This weak threshold ("reasons to believe") fall short of the standard of "reasonable suspicion" set by human rights law and it provides too broad a discretion to allow for the request of a warrant.

14. The Prevention of Electronic Crimes Act (2016) was passed by Pakistan's National Assembly on 11 August 2016. Introduced in the wake of the deadly December 2014 terrorist attack on a Peshawar school, the PECA was drafted as part of the government's National Action Plan to combat terrorism. It was designed to tackle cyberstalking, online harassment, forgery, blasphemy and forms of cyberterrorism. As has been analysed at length by Pakistani and international human rights organisations[13], the PECA utilises such overly broad legal language that it further weakens the right to privacy of Pakistani citizens, and potentially criminalises freedom of expression. During the legislative process, the UN Special Rapporteur on Freedom of Expression presented 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, and keep the public informed of how any future amendments ensures such compliance."[14]

15. Key concerns presented during the drafting process which now constitute provisions of the PECA include:

    - Section 29, which provides for mandatory mass retention of traffic data by service providers for a minimum of one year;

    - Section 34, which gives the Pakistan Telecommunications Authority the power to block or remove access to information "if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality.";

    - Section 36, which allows for "real-time collection and recording" of data if a Court is "satisfied on the basis of information furnished by an

12 See: http://www.na.gov.pk/uploads/documents/1361943916_947.pdf
13 Including Privacy International, Digital Rights Foundation, Human Rights Watch, and Amnesty International, See: https://www.privacyinternational.org/node/881
14 Reference: OL, PAK 8/2016, 8 July 2016. Available at: http://www.ohchr.org/Documents/Issues/Opinion/Legislation/PAK_8_2016.pdf

authorised officer that there are reasonable grounds to believe that the content of any";

- Section 39(1), which permits the sharing of "electronic communication or data or for the collection of evidence in electronic form" with any "foreign agency or any international organisation or agency for the purposes of investigations or proceedings";

- Section 39 (2), which gives the government the permit to "forward to a foreign government….any information obtained form its own investigations if it considers that the disclosure of such information might assist the other government, agency or organisation etc.,".

Obligations on service providers

16. As part of licensing requirements, service providers must make their communications networks 'lawful interception-compliant' by installing on their network components that comply with various international interception protocols, or 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.

17. The retention of communications data is part of the operating license requirement for Pakistani providers. Since 2004 network providers have been required to comply with requests for interception and access to network data as a standard condition of the Pakistan Telecommunications Authority (PTA)'s award of operating licenses to phone companies.[15] The 2002 Electronic Transaction Ordinance (ETO) in points 5 and 6 imposes data retention requirements.[16] The recently adopted PECA 2016 requires service providers to retain subscriber data under Section 29 for a period of one year.

15 See: Mobile Cellular Policy, IT and Telecommunication Division, Ministry of Information Technology Government of Pakistan, 28 January 2004. Available at: http://www.pakistanlaw.com/mobilepolicy28012004.pdf

16 See: http://www.pakistanlaw.com/eto.pdf
5. Requirement for original form.—
(1) The requirement under any law for any document, record, information, communication or transaction to be presented or retained in its original form shall be deemed satisfied by presenting or retaining the same if:
(a) there exists a reliable assurance as to the integrity thereof from the time when it was first generated in its final form ; and
(b) it is required that the presentation thereof is capable of being displayed in a legible form.
(2) For the purposes of clause (a) of sub-section (1);
(a) the criterion for assessing the integrity of the document, record, information, communication or transaction is whether the same has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display ; and
(b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the document, record, information, communication or transaction was generated and all other relevant circumstances.
6. Requirement for retention.—The requirement under any law that certain document, record, information, communication or transaction be retained shall be deemed satisfied by retaining it in electronic form if :
(a) the contents of the document, record, information, communication or transaction remain accessible so as to be usable for subsequent reference;
(b) the contents and form of the document, record, information, communication or transaction are as originally generated, sent or received, or can be demonstrated to represent accurately the contents and form in which it was originally generated, sent or received; and
(c) such document, record, information, communication or transaction, if any, as enables the identification of the origin and destination of document, record, information, communication or transaction and the date and time when it was generated, sent or received, is retained.

18. Such provisions are indiscriminate in their nature and expensive, and increase the scope of state surveillance.[17] There could be significant interference with the rights of individuals caused by a regime that requires companies to retain immense quantities of their communications data, not based on reasonable suspicion.[18]

Surveillance capabilities

19. The extent of Pakistan's surveillance capabilities remain unknown but there have been some reports documenting some of use of a number of different tactical communications surveillance technologies.[19]

IMSI Catchers

20. IMSI Catchers are monitoring devices that transmit a strong wireless signal, which work to entice nearby phones to connect to the IMSI catcher, rather than mobile phone towers.[20] While these devices are used to 'target' a particular individual's device by, for example, being aimed at his or her workplace they work by identifying all phones in the vicinity of the IMSI Catcher's operations.[21]

21. Mobile monitoring equipment for identification and/or interception is particularly widely used by law enforcement agencies across Pakistan.[22] The Pakistani government has imported many of these tactical communications surveillance technologies from Europe.[23]

Internet Protocol monitoring centre

22. In 2013 the Inter-Services Intelligence (ISI), Pakistan's intelligence agency, sought to commission a mass surveillance system to tap international undersea cables at three cable landing sites in southern Pakistan, according to documents obtained by Privacy International.[24] This system[25] would allow

18 A/HRC/23/40
As noted, by the Court of Justice of the European Union (CJEU), in 2014 and most recently in 2016, metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and so it concluded that the retention of metadata relating to a person's private life and communications is, in itself, a disproportionate interference with the right to privacy. More information at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

19 Tactical interception technologies are surveillance tools that collect intercepted communications data either wirelessly or directly from a target device rather than from the service provider's network architecture.

20 For more information on IMSI catchers see: Privacy International, Phone Monitoring, Explainer. Available at: https://www.privacyinternational.org/node/76

21 This means they could be used to identify unknown persons attending demonstrations and other gatherings because as many mobile phones as the system can accommodate will connect to the IMSI catcher and transmit it information about the mobile phone user, including the location of a target to within one metre.

22 For example, in 2014, the Sindh police forces reportedly acquired a Caller Location Identification System (CLIS) that they had been trying to acquire since 2010. The Punjab police also acquired IMSI/IMEI and location tracking technology in 2015. See "CID gets mobile phone caller locator system", DAWN, 13 October 2014, http://www.dawn.com/news/1137548/cid-gets-mobile-phone-caller-locator-system and "Punjab police to have mobile phone tracking units", News- Lens Pakistan, 8 June 2015, http://newslens.pk/punjab-police-mobile- phone-tracking-units/

23 For more information on companies supplying IMSI catcher technologies to Pakistan, see Privacy International (2015) Tipping the Scales: surveillance and security in Pakistan. Available: https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

24 Privacy International (2015) Tipping the Scales: surveillance and security in Pakistan. Available: https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

25 "Targeted IP Monitoring System and COE [Common Operations Environments]"

Pakistan to collect and analyse a significant portion of communications travelling within and through the country, including through Wi-Fi, broadband internet traffic, and any data transmitted over 3G, at a centralized command centre. According to the documents, the interception activities were to be "seamless" and "must not be detectable or visible to the subscriber".

Intrusion malware

23. The Pakistani government is also a confirmed user of intrusion technologies which enable the remote hacking of targeted devices. Intrusion technologies are capable of collecting, modifying and extracting all data communicated and stored on a device. They can view an individual's actions in real time on their computer, enabling the user to records passwords, and even impersonate the target, turn on the camera and microphone on a target's computer, thereby seeing and hearing everything in the vicinity of the target's computer, without the target ever being aware.

24. In April 2013, computer forensic research by The Citizen Lab revealed the existence of a command and control server for FinFisher, an intrusion malware suite, operating within Pakistan.[26] In 2014, documents obtained from a FinFisher server revealed support requests from an apparent Pakistani client – identification number 'ID 32' – dating back to 2011.[27]

25. Pakistani companies attempted to contract business with Hacking Team, an Italian company, for sale to Pakistani law enforcement or intelligence clients in March 2015, according to analysis by Digital Rights Foundation of leaked data. Hacking Team's core business centred around their Remote Control System (RCS) software suite, which allows customers to infiltrate the computer and mobile devices of targeted individuals and install backdoors, in turn allowing for undetectable monitoring at will.[28]

Limitations on use of encryption

26. Spaces to communicate privately online are also narrowing. In 2010 and 2011, the PTA ordered all ISPs and phone companies to ban encryption and virtual private networks (VPNs) except in limited circumstances and with the government's permission.[29] 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.[30]

26 The Citizen Lab, For Their Eyes Only: The Commercialization of Digital Spying, 30 April 2013. Available at: https://citizenlab.org/2013/04/for-their-eyes-only-2/

27 In 2013, following this revelation, Pakistani civil society group, Bytes for All, filed a petition in the Lahore High Court. The court ordered the PTA to look into the matter and produce a report within one month. The PTA has not yet filed their report, and attempts to gain further hearings on the issue have been unsuccessful.

28 Digital Rights Foundation, Unlawful Interception: Pakistan's intelligence agencies, Hacking Team, & the abuse of communication surveillance powers, 24 July 2015. Available at: http://digitalrightsfoundation.pk/unlawful-interception/

29 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

30 Dawn, Govt asks telecom firms to check use of encrypted VPN, 5 September 2011. Available at: https://www.dawn.com/news/656853/govt-asks-telecom-firms-to-check-use-of-encrypted-vpn

27. If a company or individual wishes to use encryption without being penalised, a formal request must be sent to the PTA and accepted. In 2015 Blackberry and its encrypted messaging service, Blackberry Messenger (BBM) were banned and asked to leave Pakistan, as Blackberry would not hand over access to its user base and servers. Blackberry was permitted to stay, although the details of the agreement have not been made public.[31]

28. Human rights activists fear that various intelligence agencies are watching people who use encryption to protect their communications. Although no one is known to have been arrested for using encryption.[32] 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".[33] 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.

Intelligence sharing and cooperation

29. Pakistan is one of the US National Security Agency (NSA)'s approved third party SIGINT partners. Being a third party partner means that the NSA considers the relationship a long- term one involving "higher degrees of trust" and "greater levels of cooperation" such that the NSA would be "willing to share advanced techniques...in return for that partner's willingness to do something politically risky." A third party partner can expect to receive "technical solutions (e.g. hardware or software) and/or access to related technology."[34]

30. The NSA especially values its relationship with Pakistan. The Pakistani government is by far the largest known recipient of NSA funds.[35] 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.[36]

31 Gibbs, S., Pakistan bans BlackBerry services in privacy crackdown, 27 July 2015. Available at: https://www.theguardian.com/technology/2015/jul/27/pakistan-bans-blackberry-messaging-internet-services-privacy-crackdown

32 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

33 A/HRC/29/32, para 16

34 "What are We After with Our Third Party Relationships – And What Do They Want from Us, Generally Speaking?" National Security Agency slide, 15 September 2009, https://s3.amazonaws.com/s3.documentcloud.org/documents/1084762/third-party-relationships.pdf

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

36 Privacy International (2015) Tipping the Scales: surveillance and security in Pakistan. Available: https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

Despite some protests by Pakistani authorities when the scale of mass surveillance was revealed, no independent investigation has been initiated.[37]

II. Data protection regime

31. Pakistan does not have a comprehensive data protection legal framework. This lack of adequate and comprehensive legislation on data protection is of particular concern given that registration of personal data is widespread in Pakistan.

NADRA

32. Pakistan has one of the world's most extensive citizen registration regimes known as National Database & Registration Authority (NADRA), which was established in 2000.[38] In 2012 NADRA announced a so-called chip-based Smart NIC (SNIC), which contains its owner's biometric photo, a computer chip, address and parental information. Biometric data collected by NADRA includes iris scans; fingerprints (both hands); a photograph taken at a NADRA centre, and a scan of the citizen's personal signature. NADRA has said that it aims to replace all current CNICs with SNICs by 2020.

33. Since its adoption and with its expansion over the years, NADRA has found itself at the heart of a number of controversies regarding a lack of proper checks and balances. There have been various reports of corruption at NADRA centres, where the biometric verification/application process can be bypassed as well as concerns of misidentification errors[39] and forgery.[40]

34. 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, according to Alertboot Endpoint Security. The data breach was low-tech, and involved a physical break-in.[41] In 2012, a Turkish hacker claimed to have accessed NADRA's servers as well as those of the Federal Investigation Agency (FIA) by spawning backdoors.[42] In 2014, NADRA 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.[43]

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

38 See: https://www.nadra.gov.pk

39 Craig, T., and Hussain, S., Pakistan's mobile phone owners told: be fingerprinted or lose your sim card, 3 March 2015, The Guardian, Available at: https://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users

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

41 See: http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/05/19/data-encryption-software-nadra-pakistan-has-data-breach.aspx

42 Baloch, F., Cyber vandalism: Turkish hacker claims gaining access to NADRA, FIA servers, 15 December 2012. Available at: https://tribune.com.pk/story/480044/cyber-vandalism-turkish-hacker-claims-gaining-access-to-nadra-fia-servers/

43 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/

Mandatory SIM Card registration

35. SIM card registration is mandatory in Pakistan. Unlike in most countries with mandatory registration, SIM cards are also biometrically verified against NADRA[44], often by fingerprint[45]. As of March 2015, 68.7 million SIMs had been biometrically verified out of 103 million SIMs in use at that time.[46]

36. SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups. It also facilities surveillance and makes tracking and monitoring of users easier for law enforcement authorities.

Poor data protection policies of telecommunication providers

37. Studies have also shown that telecommunication providers operating in Pakistan have weak or inconsistent data protection and privacy policies. As reported by the Digital Rights Foundation key concerns include:[47]

    - inconsistency in regards to the public availability of said privacy policies, as well as an apparently lack of proper updates and oversight;

    - lack of awareness of new legal obligations such as those included in 2016 Prevention of Electronic Crimes Act;

    - where provisions in the policies indicated that customers could contact the companies concerning possible privacy breaches, there were again inconsistencies, with Mobilink, for example, being unable to provide a privacy breach form on its website, despite stating so only a few paragraphs earlier.

44 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/

45 Craig, T., and Hussain, S., Pakistan's mobile phone owners told: be fingerprinted or lose your sim card, 3 March 2015, The Guardian, Available at: https://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users

46 Unfortunately, NADRA has not provided up to date numbers since. However, there have been reports of corruption as well as honest incompetence on the part of the verification system resulting in some SIMs escaping being deactivated. This number has been shrinking however, given the aggressiveness of the re-verification drive. See: https://tribune.com.pk/story/851092/biometric-system-two-thirds-of-103-million-sims-verified/

47 Digital Rights Foundation (2016) Telecoms Privacy and Data Protection Policies in Pakistan. Available at: http://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Telecoms-Privacy-and-Data-Protection-Policies-in-Pakistan-1.pdf

RECOMMENDATIONS

38. We recommend that the government of the Pakistan to:

1. Take measures to ensure that its state security and intelligence agencies respect the right to privacy;

2. Ensure that all interception activities comply with the principles of legality, proportionality and necessity;

3. Provide clarity and review mechanisms of oversight over the surveillance practices of its state security and intelligence agencies to ensure compliance with the right to privacy, and integrate monitoring and audit of these;

4. 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;

5. Review the Prevention of Electronic Crimes Act to ensure conformity with Pakistan's obligations under the ICCPR (Articles 17 and 19), and its national obligations;

6. Review all licensing agreements 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 law and standards, in particular in relations to requirements for blanket, indiscriminate data retention;

7. Dismantle legal regimes that require state permission to use encryption or anonymity tools, and ensure its laws, policies, and practices that affect personal use of encryption and online anonymous speech are consistent with its international human rights obligations;

8. Adopt and enforce a comprehensive data protection law to ensure the protection of personal data of it citizens.