PRIVACY INTERNATIONAL

Suggestions for right to privacy-related questions to be included in the list of issues on Pakistan, Human Rights Committee, 118th Session, October 2016

July 2016

Introduction

Privacy International encourages the Committee to seek information from the government of Pakistan on the impact of communications surveillance with the right to privacy.

Surveillance across Pakistani communications networks is technologically advanced and comprehensive. Pakistan's important geopolitical role countering insurgent and Islamist groups has resulted in the Pakistani military and intelligence establishment receiving high levels of funding from overseas governments to develop advanced communications surveillance infrastructure.

Intelligence functions are dispersed across a number of government agencies that collect and/or use intercepted communications. Each branch of the Pakistani armed forces has its own intelligence service conducting signals intelligence. Other agencies include the Inter-Services Intelligence (ISI) and Joint Signal Intelligence Bureau. Relevant agencies within the Pakistani government have moved toward the mass capture and storage of communications of ordinary citizens, whereas previously they had mainly used tactical military surveillance tools, which are far more targeted.

The capacity for mass automated interception of ordinary citizens' communications has been expanded and framed as an essential condition for ensuring citizens' security.

Surveillance and censorship of communications

Surveillance across all of Pakistan's communications networks is becoming more widespread. This is justified both as an anti-terrorism measure and to prevent sharing of content prohibited in Pakistan (including blasphemous content.)

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 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.

The same technologies that the Pakistani government uses for censorship are also used for surveillance. 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.[1]

To this end, the Pakistani government has purchased a number of 'packet inspection' technologies. 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. Packet inspection technologies can also be programmed to search for particular terms, such as key words in emails.[2]

Spaces to communicate privately online are also narrowing. In 2010 and 2011, the Pakistan Telecommunications Authority (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.[3] 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.

Tactical surveillance – IMSI catchers and hacking

Pakistani law enforcement and intelligence agencies also use a number of different tactical communications surveillance technologies. 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.

IMSI Catchers

Such equipment includes IMSI Catchers. 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. 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. 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.

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

[2] 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%2020150721_0.pdf

[3] 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.

Mobile monitoring equipment for identification and/or interception is particularly widely used by law enforcement agencies across Pakistan.[4] The Pakistani government has imported many of these tactical communications surveillance technologies from Europe.[5]

Hacking

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. Malware provides its operator with extraordinary access to an individual target's computer. They can view an individual's actions in real time on their computer, enabling the user to records passwords, and even impersonate the target. The user can also 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.

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.[6]

Intelligence sharing and cooperation

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."[7]

The NSA especially values its relationship with Pakistan. The Pakistani government is by far the largest known recipient of NSA funds.[8] 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.[9]

[4] 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 track- ing 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/

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

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

[7] "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

[8] "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

[9] Privacy International, Tipping the Scales: surveillance and security in Pakistan, 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.[10]

Prevention of Electronic Crimes Bill

On April 13, 2016 the National Assembly's Standing Committee on Information Technology and Telecommunication approved the Prevention of Electronic Crimes Bill (PECB). As of July 2016, PECB was being discussed before a Senate Committee.

The PECB has been criticised by several Pakistani and international organisations, as well as the United Nations' Special Rapporteur on freedom of opinion and expression, for provisions contained therein that, if adopted, would violate the right to privacy and to freedom of expression.[11]

Privacy International is particularly concerned by provisions in the Bill that provide for:

- Mandatory mass retention of traffic data by service providers (draft Section 29);
- Broad powers of the authorized officers, including power to request decryption of information (draft Section 32);
- Imposition of secrecy to service providers (draft Sections 35 and 26)
- Information sharing and cooperation with foreign governments without judicial authorisation and oversight (draft Section 39).

A full analysis of the PECB by Privacy International, Article 19 and the Digital Rights Foundation is contained here:
https://privacyinternational.org/sites/default/files/PEC_Update.pdf

Lack of data protection law

The 2002 Electronic Transaction Ordinance (ETO) criminalises unauthorized interception of personal data.[12] However, there are no laws in Pakistan that specifically deal with the protection of personal data.

This lack of adequate and comprehensive legislation on data protection is of particular concern given that registration of personal data is widespread in Pakistan.

Pakistan has one of the world's most extensive citizen registration regimes – over 96 % of citizens reportedly have biometric ID cards[13], including the Smart National Identity

[10] 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).("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/).

[11] "UN expert urges Pakistan to ensure protection of freedom of expression in draft Cybercrime Bill", Statement of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye, United Nations Office of The High Commissioner for Human Rights, December 14, 2015 http://bit.ly/1TRCaz2

[12] Section 36. See http://www.pakistanlaw.com/eto.pdf

Card (SNIC)[14], which contains its owner's biometric photo, a computer chip, address and parental information. ID cards are commonly required to access services ranging from opening a bank account to getting a passport. SIM cards must be registered to their user.[15] Unlike in most countries with mandatory registration, SIM cards are also biometrically verified against the National Database and Registration Authority's (NADRA) national database.[16]

List of issues

Based on the above observations, Privacy International proposes the following questions for the List of Issues on Pakistan:

- What measures is Pakistan taking to ensure that its state security and intelligence agencies respect the right to privacy?
- In particular, how does Pakistan ensure that all interception activities are only carried out in ways that comply with the principles of legality, proportionality and necessity?
- What are the mechanisms of oversight over the surveillance practices of its state security and intelligence agencies? How is their effectiveness assessed?
- What types of surveillance technologies are employed by Pakistani law enforcement and intelligence agencies and how is the acquisition and use regulated and monitored?
- How does the PECB conform with Pakistan's obligations under the ICCPR (Articles 17 and 19)?
- How does Pakistani law protect personal data and is the government considering adopting a comprehensive data protection law?

[13] See "Pakistan's experience with identity management", BBC News, 8 June 2012, http://www.bbc.co.uk/news/world- asia-18101385

[14] See "Solutions", National Database and Registration Authority (NADRA), 2015, https://www.nadra.gov.pk/index.php/ solutions

[15] "Pakistani SIM users given until 17 May to register", Telegeography, 27 April 2011, https://www.telegeography.com/products/commsupdate/articles/2011/04/27/pakistani-sim-users-given-until-17-may-to-register/

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