The State of Privacy in Pakistan

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

Privacy is a fundamental constitutional right:

Article 14 (1): “The dignity of man and, subject to law, the privacy of home, shall be inviolable.”

Benazir vs Federation of Pakistan and Others (1998): Infringing on “the secrecy and privacy of a man...may ultimately be a source of danger and insecurity. In this way the liberty guaranteed to a person is also invaded, restricted and circumvented. Therefore, if this exercise is to be considered from any angle, be it constitutional, legal or moral, no justification can be afforded for such reprehensible acts by the officials or the persons at the helm of governance of the country.” http://jasoosibandkaro.pk/wp-content/uploads/2014/11/jbk-whitepaper.pdf

Pakistan does not have strict data privacy and protection legislation.

1. Electronic Transactions Ordinance 2002 criminalises unlawful information access.

2. Freedom of Information Ordinance (2002) states that certain forms of “information is exempt if its disclosure under this ordinance would involve the invasion of privacy of an identifiable, individual (including individual) other than the requester”

3. The Constitution, furthermore, affords Pakistan’s armed forces, police and other security agencies exceptions to article 8 should its provisions possibly hamper the “proper discharge” of their duties. By inference, this includes

The Prevention of Electronic Crimes Act 2016 contains provisions that purport to protect data privacy, but:

Affords “authorised” law enforcement access to personal data, if “reasonably required” for a criminal investigation (Section 28). Telecoms and ISPs are required to retain traffic data for a least one year, and can be penalised for not doing so (Section 29)

In cases that involve “cyber terrorism” (which has been defined very loosely) data can be seized without a warrant, provided the court is informed with 24 hours.

The PECA permits the sharing of user data with foreign governments and their respective agencies - even if the latter have not yet made requests.

The Fair Trial Act 2012 allows state agencies to collect data via “means of modern techniques and devices” in order to intercept emails, text messages and wire-tapping, to be permitted in court cases.

Ostensibly designed to tackle and track terrorist suspects, interception of private communications runs the risk of political abuse.

Discourse on privacy and privacy rights in Pakistan come up against national security narratives.

Terrorism et al bolster public support for greater surveillance powers and invasion of privacy

December 2014 attack on army-run school in Peshawar bolstered biometric re-verification drives in Pakistan, aided by media reports of terrorists tracked via CNICs

Pakistani & Int'l calls for respect for rights to be inserted into progressive legislation have been dangerously criticised in sectors as being "anti-state"

In 2012 the US NSA used the metadata from 55 million Pakistani mobile phone records to track down citizens within Pakistan and Afghanistan, via its SKYNET programme, on the assumption of links to terrorism, including a senior Al Jazeera journalist based in Islamabad. http://digitalrightsfoundation.pk/spectrum-eyes-the-nsa-pakistani-metadata/

British GCHQ infiltrated Pakistan's Internet Exchange in 2008, gaining "access to almost any user of the internet inside Pakistan" and the ability "to re-route selected traffic across international links towards GCHQ's passive collection systems."

http://digitalrightsfoundation.pk/press-release-british-intelligence-agency-hacked-into-pakistan-internet-exchange/

In November 2014 Digital Rights Foundation found that Pakistan was a customer of FinFisher, the commercial spyware company whose clients include governments. Their primary software package, FinSpy is designed to “remotely access and control” mobile phones and computers, as part of a complete toolset designed to take complete control of the systems belonging to targets.

Software from FinFisher was licensed for a three year period, with two command and control servers being installed on PTCL networks.

Leaked documents show the budget for this purchase was €432,120 or PKR 57 million (as of September 2014)

In July 2015, the data of Italian commercial spyware firm Hacking Team had been leaked onto the internet, revealing potential customers of their goods and services, the core being the Remote Control System (RCS), which allows customers the ability to infiltrate computer and mobile devices of mobile devices of targeted individuals and install backdoors, to allow for undetectable monitoring at will.

Potential customers included representatives of Pakistan’s intelligence agencies. Internal Hacking Team data indicates that they were unsuccessful.

(http://digitalrightsfoundation.pk/unlawful-interception/)

Contact Information:

Email: nighat@digitalrightsfoundation.pk

Twitter: https://twitter.com/nighatdad

Twitter: https://twitter.com/digitalrightsPK

Website: http://digitalrightsfoundation.pk/

DigitalRightsFoundation

"KNOW YOUR RIGHTS"