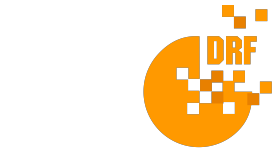

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

Submission to to UN Special Rapporteur on Freedom of Speech and Expression: The Surveillance Industry and Human Rights

February 15, 2019

1. Introduction

1.1 Surveillance in Pakistan has largely taken the form of state surveillance, with private companies and telecommunications providers facilitating these practices. This confluence between state and private actors exists with the context of broad powers granted by privacy-negating legislation as well as legal ambiguity.

1.2 This report submitted by Digital Rights Foundation (DRF), seeks to highlight the human rights concerns raised by Pakistan's surveillance capabilities and transfer of technologies with relation to international law norms. The report will conclude with recommendations at a national, regional and international level to secure the right of privacy and minimize governmental surveillance and intrusion.

1.3 DRF is a not for profit organization based in Pakistan working on digital freedom. DRF envisions a place where all people, especially women, can exercise their right of expression without being threatened. DRF works on issues of online freedom of expression, digital privacy, equal internet access and online violence against women through research-based advocacy, capacity-building and direct assistance.

2. Legal Landscape for Surveillance In Pakistan

2.1 This section will provide a quick overview of the legal regime in Pakistan that partially legitimizes digital surveillance and use of surveillance.

2.2 **Article 14 of the Constitution of Pakistan 1973** provides for the right to privacy which is couched in the language of dignity of man. The Constitution provides for "privacy of the home", which has been interpreted to extend to digital communications as well.[1] This Constitutional right to privacy however has been made "subject to law", which has meant that laws passed by the legislature can circumscribe the right to privacy in a meaningful manner. Furthermore, laws from the colonial regimes are still applied to provide legal cover for intrusive actions by the state.

2.3 The primary law in this regard is the **Telegraph Act from 1885**, and section 5 allows the government to order interception of messages and take possession of licensed telegraphs under the vague grounds of "the occurrence of any public emergency, or, in the interest of the public safety". In this backdrop, newer laws such as the **Pakistan Telecommunication (Re-organization) Act, 1996** allowed for the state to amass broad powers of surveillance and interception. Section 54[2] of the Act empowers the Federal Government to "intercept calls and messages or to trace calls through any telecommunication system" if the surveillance is "in the interest of national security or in the apprehension of any offence."

2.4 More recently the **Fair Trial Act, 2013** grants powers for collection of evidence through "interception" and "surveillance". The Act specifically allows for issuance of warrants for surveillance and interception, under section 11, if the standard of "reasonable threat

[1] Article 14: "Inviolability of dignity of man, etc.—(1) The dignity of man and, subject to law, the privacy of home, shall be inviolable. (2) No person shall be subjected to torture for the purpose of extracting evidence."

[2] Section 54. National Security: (1) Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorise any person or persons to intercept calls and messages or to trace calls through any telecommunication system.

or possibility of an attempt to commit a scheduled offence" is met. The warrants, once granted, provide sweeping and broad powers which allow: "interception and recording of telephonic communication of the suspect with any person"; "video recording of any person, persons, premises, event, situation, etc"; interception, recording or obtaining of any electronic transaction including but not limited to e-mails, SMSes, etc"; "interception or taking over of any equipment used in communication". While there are judicial safeguards for complaints against misuse of warrants (section 29) and prohibition of misuse of intercepted material (section 34), the Act allows for vast amounts of information to be collected and processed.

2.5 The judiciary has largely upheld the legislative regime in place, however there have been instances in which judicial review under the right to privacy has been granted. The most seminal of these examples has been the Benazir Bhutto v. Federation of Pakistan and Others, PLD 1998 SC 388 which held that wiretapping by the government of Benazir Bhutto was declared illegal.

2.6 The Prevention of Electronic Crimes Act (PECA) 2016, which is not the primary legislation governing online spaces, requires mandatory mass retention of traffic data by service providers for a minimum of one year (section 29) which has implications for data privacy and surveillance capacities of the state with reference to data stored by third parties. This indiscriminate, mass retention of data is in direct violation of Article 17 of the ICCPR. Additionally, section 36 of PECA allows for real-time collection and recording of data if a Court is "satisfied on the basis of information furnished by an authorised officer that there are reasonable grounds to believe that the content of any".

3. Surveillance Projects

3.1 There has been sustained transfer of military surveillance technology between countries involved in the "War on Terror"—Pakistan being a major recipient of military aid from the United States has experienced the exchange of military surveillance technology at a large scale.[3]

3.2 **NADRA database**

3.2.1 Pakistan's National Database & Registration Authority (NADRA) maintains a comprehensive, centralized biometric database of it's citizens' personal information; i.e. biometric cards, containing biometric data such as iris scans, fingerprints, photographs, and a scan of the citizen's personal signature.

3.2.2 Since the tragic terrorist attack on the Army Public School (APS) in Peshawar in December 2014, all SIMS were required to have undergone biometric verification system (BVS).[4] The SIM cards are verified with the NADRA database, which connects telecommunications data with the centralized database as well.

---

[3] Mahvish Ahmad and Rabia Mehmood, "Surveillance, Authoritarianism and 'Imperial Effects' in Pakistan", *Surveillance & Society*, 2017, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/6721/6454/.

[4] "Over 10m SIMs face blockage as verification deadline ends tomorrow", *The Express Tribune*, April 11, 2015, https://www.thenews.com.pk/print/11936-over-10m-sims-face-blockage-as-verification-deadline-ends-tomorrow.

3.2.3 Digital security of the NADRA database has been the cause of anxiety due to reports of multiple breaches as well as data sharing practices with foreign governments. In June 2018 it was learnt that personal information of citizens was being sold online. The information stemmed from a data breach by the Pakistan Information Technology Board (PITB) and NADRA.[5] It has come to light, as per WikiLeaks documents, that both the GCHQ and the NSA acquired access to the NADRA database for the purpose of obtaining identification records of Pakistani citizens, under the pretext of tracking down "suspected terrorists".[6] In June it came to light that as part of the NSA's SKYNET program, call data from Pakistani telecommunications providers were harvested and phone records of 55 million Pakistani citizens were used by NSA for analysis.[7]

3.2.4 The Pakistan Internet Exchange (PIE) provides for a consolidated node through which a majority of Pakistan's internet traffic passes. This has facilitated the monitoring and blocking of internet content. For instance Privacy International has found that 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]

3.3 **Urban Surveillance**

3.3.1 The equipment for the Safe Cities Projects in Punjab and Islamabad has been procured from the Chinese company Huawei, a company whose links with the Chinese government and data sharing are well known. The projects, operational in both Islamabad and Lahore, largely consist of CCTV cameras installed across the cities—in Lahore 8,000 cameras have been installed so far.[9] There are plans to integrate facial recognition software into the surveillance project as well.

3.3.2 The details of the larger China-Pakistan Economic Corridor (CPEC) project have been a closely guarded secret, however documents obtained by the newspaper Dawn show that there are plans to build system of monitoring and surveillance Peshawar to Karachi, "with 24 hour video recordings on roads and busy marketplaces for law and order."[10] Furthermore, fibreoptic internet technology is being from the Chinese border along the

---

[5] Marvi Sirmed, "Is PITB clueless about Pakistan's largest data breach?", *The Daily Times*, May 11, 2018, https://dailytimes.com.pk/238533/is-pitb-clueless-about-pakistans-largest-data-breach/.

[6] Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim, "Top-secret NSA report details Russian hacking effort days before the election," *The Intercept*, June 6, 2017, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

[7] Privacy International, "Tipping the scales: Security & surveillance in Pakistan", *Special Report*, July 2015, https://privacyinternational.org/sites/default/files/2018-02/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf.

[8] Human Rights Committee 120th Session, "The Right to Privacy in Pakistan: Submission by Privacy International in advance of the consideration of the periodic report of Pakistan," 3 July - 28 July 2017, https://privacyinternational.org/sites/default/files/2017-12/120_Pakistan.pdf.

[9] "8,000 CCTV cameras installed in Lahore: Shahbaz inaugurates Safe City Project," *Dawn*, January 5, 2018, https://www.dawn.com/news/1380906.

[10] Khurram Husain, "Exclusive: CPEC master plan revealed: Details from original documents laying out the CPEC long term plan are publicly disclosed for the first time", *Dawn*, June 21, 2017, https://www.dawn.com/news/1333101.

CPEC route.[11] The "Pak-China fibre optic", the 820-kilometer fibre optic cable project, from Rawalpindi to Khunjerab was recently made available for commercial use.[12]

3.3.3 Governmental tech-based schemes such as HotelEye combine surveillance technologies and government databases to keep track of activities of hotels and their visitors. The project, piloted in Punjab, is not being scaled up in Khyber Pakhtunkhwa and Sindh.[13] There is no transparency regarding the data collection and retention policies of this software and the level of access provided to law enforcement agencies.

3.4 Transfer of Surveillance Technologies

3.4.1 In 2015, Privacy International posited that the surveillance capacity of the Pakistani state exceeded the powers enshrined under the legal structure.[14] Furthermore, as pointed out by Ahmad and Mehmood, the surveillance capacities of the Pakistan government are grounded in the context of extensive exchange of military technologies under the rubric of the War on Terror, which has resulted in covert and unchecked transfer of surveillance capacity that is justified by broad anti-terrorism laws.[15]

3.4.2 Section 42 of the Prevention of Electronic Crimes Act allows for cooperation between the Federal Government and foreign governments, foreign agencies and others, in terms of information exchange, i.e. "any information obtained from its own investigations." This allows for legal cover for a reciprocal relation between the Pakistan government and its allies, where information is exchanged for "technical solutions (e.g. hardware or software) and/or access to related technology."[16]

3.4.3 According to a 2015 report by the UK-based organization Privacy International, Pakistan "is by far the largest known recipient of NSA funds".[17] Furthermore, the Pakistan government is the part of the NSA's approved third-party SIGINT partners, which "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.'"[18]

3.4.4 Pakistan has also cooperated with private companies to gain access to surveillance and interception technologies. According to Privacy International, the Pakistani government

---

[11] Ibid.

[12] Haider Nasim, "Pak-China fibre optic link activated for commercial use", *The Express Tribune*, February 2, 2019, https://tribune.com.pk/story/1901975/8-pak-china-fibre-optic-link-activated-commercial-use/.

[13] "Peshawar Police launch 'Hotel Eye' software", *The News International*, January 15, 2019, https://www.thenews.com.pk/print/419236-peshawar-police-launch-hotel-eye-software.

[14] Privacy International, "Tipping the scales: Security & surveillance in Pakistan", Special Report, July 2015, https://privacyinternational.org/sites/default/files/2018-02/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf.

[15] Mahvish Ahmad and Rabia Mehmood, "Surveillance, Authoritarianism and 'Imperial Effects' in Pakistan", *Surveillance & Society*, 2017, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/6721/6454/.

[16] Privacy International, "Tipping the scales: Security & surveillance in Pakistan", *Special Report*, July 2015, https://privacyinternational.org/sites/default/files/2018-02/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf.

[17] Ibid.

[18] Ibid.

has worked with Alcatel (France), Atis (Germany), Ericsson (Sweden) and Huawei (China).

4. Recommendations

4.1 Need for effective and human rights compliant national legislation on digital privacy and data protection that provides for robust safeguards against intrusion from surveillance technologies;

4.2 Review of national laws regarding surveillance and privacy of laws to ensure that they are in line with international human rights standards and Pakistan's commitments under international law, i.e. the International Covenant of Civil and Political Rights (ICCPR);

4.3 International commitments from nation states for transparency around sale and transfer of surveillance technology;

4.4 Effective oversight at the regional and international level for use and transfer of surveillance technologies by both state and private actors;

4.5 Meaningful implementation of the ICCPR frameworks around privacy and liberties, as Pakistan has ratified ICCPR and submitted itself to periodic reviews under international law;

4.6 International cooperation to develop guidelines for international transference of surveillance technologies between private companies and national governments, ensuring that use of technologies are regularly audited for human rights compliance.