The Right to Privacy in Pakistan's Digital Spaces: April 2018 Human Rights Council Report

Civil Society Submission by: Digital Rights Foundation, Pakistan

1. This submission from Digital Rights Foundation seeks to map out the landscape of digital privacy rights and data protection in Pakistan and highlight issues that are inherent in this part of the world.

A. About Digital Rights Foundation

2. Digital Rights Foundation (DRF) is a registered research-based advocacy non-governmental organization in Pakistan. DRF focuses on ICTs to support human rights, inclusiveness, democratic processes, and digital governance. DRF works on issues of online free speech, privacy, data protection, surveillance, tech, gender and online violence against women.

B. Introduction

3. The right to privacy continues to shrink dramatically in Pakistan. In digital spaces this corresponds to the government's strict control and over-regulation of the internet[1], causing the nation to be ranked as "fairly repressive" and "not free", as per Freedom House's annual Freedom on the Net report. [2] In fact, quite ironically, access to this study undertaken annually by Freedom House was banned in the country by the Pakistan Telecommunications Authority (PTA) -- authority for internet regulation and governance-- in 2017[3].

4. The right to privacy is also eroded by legislation and practices such as the Prevention of Electronic Crimes Act 2016 and the Fair Trial Act 2013. These laws have provided legal cover for intrusive practices which have undermined the right to privacy guaranteed under the Constitution of Pakistan.[4]

5. This report aims to reflect on the larger issue of lack of policy-making around privacy in Pakistan, particularly the extent to which it allows pervasive collection of personal information by the government as well as private companies. It also identifies the government as the primary regulator of online spaces and its relationship with private regulators -- internet regulators, social media platforms and the telecommunication sector -- particularly to highlight the growing surveillance apparatus in Pakistan.

6. While assessing the shrinking spaces and lack of privacy rights in Pakistan, this report takes into account the prevailing national security narrative -- particularly of the National Action Plan and the Prevention of Electronic Crimes Act (PECA)[5].

---

[1]For more information check State of Privacy - https://privacyinternational.org/type-resource/state-privacy

[2]"Freedom on the Net 2016, Country Profile: Pakistan." *Freedom on the Net 2016*, Freedom House, 14 Nov. 2016, www.freedomhouse.org/report/freedom-net/2016/pakistan

[3] PTA blocks Freedom on the Net Report, https://propakistani.pk/2017/11/17/pta-blocks-freedom-net-report-pakistan/

[4] The right to privacy is guaranteed under Article 14(1) of the Constitution of Pakistan.

[5] Prevention of Electronic Crimes Act August 2016 (PECA), http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

7. As a result, a large fraction of data protection cases, are overlooked or dealt with under narrow provisions of domestic law that confine privacy and free speech within restrictive statutory contours.

8. This report aims to focus on a few critical provisions pertaining to data retention, encryption, surveillance and interception, that will be followed by recommendations.

B. Existing Legislative and Regulatory Framework

a. Law and Policy Overview

9. The existing legal regime provides no safeguards against collection of personal data as there are no proper constitutional and statutory provisions on privacy in Pakistan. The most recent attempt at legislation was the Electronic Data Privacy Bill, 2005 which did not go through, despite assurances as recent as April, 2017 that it would be passed in the next few months. So as of April, 2018, Pakistan has not enacted any data protection laws.

10. DRF has made significant headway over the past year in regards to data protection legislation by bringing the need of data protection legislation at the national forefront, in spite of the passage of PECA 2016. We have been working directly with the relevant government ministries to advocate for domestic data protection legislation, with the help and support of the Open Government Partnership (OGP) process.

11. DRF also disseminated a policy brief to all relevant ministries[6], hoping that the government would review the legislation on data collection and surveillance -- by public and private sectors -- particularly, PECA 2016, to bring it in line with its obligations under the Covenant and that it would also establish independent oversight mechanisms on the implementation of the law, including judicial review of surveillance activity, to make the process inclusive and transparent.

a. Surveillance and Interception

12. Digital surveillance of journalists, human rights activists, women and ordinary citizens at large is becoming increasingly common place. As penetration of ICTs is increasing in countries such as Pakistan, government is harnessing technologies for purposes of surveillance en masse, as well as targeted individuals. Furthermore, it is important to note that surveillance does not operate in isolation, rather it is part of a larger network of transnational partnerships and exchange of technologies.

13. Law enforcement and intelligence agencies in Pakistan are actively expanding their surveillance capabilities, ostensibly to counter terrorism and maintain law and order under the mandate given by the larger framework of the National Action Plan.[7] However these measures often come at the cost of civil liberties and infringement of rights, such as the right to privacy.

14. The integrated nature of these systems of surveillance also allows for unparalleled access to information and monitoring capacity than at any time in history. In Pakistan the

[6] A Data Protection Law in Pakistan: Policy Recommendations by Digital Rights Foundation October 2017, https://digitalrightsfoundation.pk/wp-content/uploads/2017/10/Policy-Brief-for-MOIT.pdf

[7] The National Action Plan (NAP) was formulated in wake of the attack on Army Public School in 2014. The NAP included measures such as the establishment of Military Courts, lifting of the moratorium on the death penalty, clamp down on funding sources for terrorist groups and operations to militarily remove terrorists.

integrated biometric Nadra system is one of the biggest biometric databases in the world. Integration of these system with other surveillance networks allows for individuals to be identified immediately and tracked in increasingly intrusive ways. Serious concerns have been raised regarding the Nadra data breaches and capacity of the Pakistani government to secure this data.[8]

15. Surveillance can also be facilitated by social media companies. In July 2017, Facebook conducted a meeting with the Government of Pakistan ostensibly to tackle blasphemy in online spaces.[9] Digital rights watchdogs have raises serious concerns regarding a potential data-sharing agreement with the government. The Islamabad High Court has ordered the government to monitor social media websites and the content to check for blasphemous material and hate speech.[10] The Punjab Safe Cities Authority (PSCA) has its own social media monitoring cell.[11]

16. In 2015, it was reported that government's surveillance capability, particularly that of the Inter-Services Intelligence Agency, outstrips domestic and international legal regulation. [12] Several companies have been engaged to develop technologies for mass surveillance, including "Alcatel, Ericsson, Huawei, SS8 and Utimaco."[13] The Safe Cities projects in both Islamabad and Lahore are contracted to Huawei, a Chinese company.

---

[8] Shaheera Jalil Albasit, "Is Nadra keeping your biometric data safe?", *Dawn*, October 17, 2016, https://www.dawn.com/news/1290534.
[9] Asif Shahzad and Saad Sayeed, "Facebook meets Pakistan government after blasphemy death sentence", *Reuters*, July 7, 2018, https://www.reuters.com/article/us-pakistan-facebook/facebook-meets-pakistan-government-after-blasphemy-death-sentence-idUSKBN19S2BF .
[10] Faisal Kamal Pasha, "Govt must block blasphemous content on social media: IHC", The News International, March 9, 2017, https://www.thenews.com.pk/print/191191-Govt-must-block-blasphemous-content-on-social-media-IHC.
[11] "684 social media IDs objectionable", The News International, July 7, 2017, https://www.thenews.com.pk/print/214937-684-social-media-IDs-objectionable.
[12] "Briefing on Privacy International Legal Case: 10 Human Rights Organisations v. the United Kingdom," Privacy International, July 21, 2015, https://www.privacyinternational.org/sites/default/files/2018-02/Privacy-International-Legal-Briefing-10-Human.pdf.
[13] ibid.

b. Foreign Surveillance

17. Pakistan has also been the target of surveillance from foreign intelligence agencies. In June 2015, it was revealed that the Pakistan Internet Exchange (PIE) was hacked and infiltrated by Britain's GCHQ. This interception made the user data of Pakistani citizens vulnerable to being accessed and stored.[14] Other leaks have down that the Pakistani government offered intelligence agencies in the United States to make available the entire Nadra database containing identity information of Pakistani citizens.[15]

18. There is evidence of large-scale collaboration between the Pakistani government and the United States in that the National Security Agency (NSA)'s SKYNET programme harvested caller data from Pakistani telecommunications providers, i.e. 55 million phone records.[16]

c. Data Retention

19. Activities that restrict privacy can only be justified if they are necessary to achieve a legitimate aim and are proportionate to the aim pursued[17]. PECA requires a service provider to retain its specified traffic data for a minimum period of one year or "such period as the authority may notify". However, the retention of traffic data for as long as a

---

[14] "Spies Hacked Computers Thanks To Sweeping Secret Warrants, Aggressively Stretching UK Law", The Intercept, June 22, 2015, http://bit.ly/1VMfTZN.
[15] "Pakistan government's alleged leaking of citizens' private data is unacceptable", *IFEX*, June 22, 2017, https://www.ifex.org/pakistan/2017/06/21/leak-private-data/.
[16] Cora Currier, Glenn Greenwald and Andrew Fishman, "U.S. government designated prominent Al Jazeera Journalist as a 'member of Al Qaeda'", The Intercept, May 8, 2015, https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/.
[17] International Principles on the Application of Human Rights to Communications Surveillance, July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

year is in contravention with the OHCR's interpretation of Article 17 of the ICCPR and is rendered arbitrary and inadequate practice[18].

20. Further, the Monitoring and Reconciliation of Telephony Traffic Regulations 2010 (MRTTR) require network providers to comply with requests for interception and access to network data as "a standard condition of the PTA's award of operating licenses to telecom companies.[19]"

21. While, Telenor Pakistan and other telecoms operating in Pakistan have, as a part of their updated privacy policy listed PECA among "the legal frameworks in which we operate." The list of "legal frameworks", however, does not make explicit reference to the above mentioned MRTTR, containing License conditions, in particular its sections on the requirement of network operators to incorporate hardware and software that "monitor, control, measure and record traffic in real-time.[20]"

22. Further, these telecom companies provide no information on what they will do in the event of a government request for user data, or if personal data has been stolen by hackers.

23. For instance, Telenor Pakistan's parent company, the Norway-based Telenor Group, have listed on their website with clarity and detail the measures that they take to safeguard user data protection, as well as indicating what government requests entail. The

---

[18] Data Protection Law in Pakistan: Policy Recommendations by DRF, https://digitalrightsfoundation.pk/data-protection-law-in-pakistan-policy-recommendations-by-drf/ [accessed 3 April 2018]

[19]Monitoring and Reconciliation of Telephony Traffic Regulations 2010 (MRTTR), http://www.pta.gov.pk/en/laws-&-policies/regulations

[20]Adnan Chaudhry, Content Regulation in Pakistan's Digital Spaces: June 2018 Human Rights Council Report December 2017, https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/DigitalRightsFoundationSubmissionSpecialRapporteurFreedomofExpression.pdf accessed

website for Telenor Pakistan, their local subsidy, however, does not indicate what government requests for customer data would entail[21].

24. This indicates how the government tries to regulate content indirectly by pressuring local telecom companies to comply with their guidelines and requests, as one of the licensing conditions.

d. Gender Issues

25. Social surveillance of certain genders and minority groups can be particularly intrusive and damaging. There is a need to also develop policies to cater to the specific privacy violations that women experience when using digital technologies, and the unique ways in which they are monitored. DRF's survey of female journalists[22] revealed that women are targeted and monitored by state and non-state actors in different way.

26. The gendered and cultural impact of such interferences can be set forth in a nutshell by giving a very everyday example of how the culture relating to cellular phone and internet usage is, in Pakistan. The use of internet, indeed the access to it, is a rarity in the majority of households for females, especially use that is singular and private. This is not anomalous and is keeping in line with the patriarchal culture that exists in full force, a woman is not seen as someone with the right to the best amenities, often enough is not educated enough to fully enjoy the use of a phone and internet connectivity but in the instances that she can, there is strong discouragement on the sharing of personal images on social media. In such a setting, a privacy leak can and has lead to situations where images have been misused and held as leverage for blackmail and can have a severely damaging impact.

---

[21] Ibid

[22] "Surveillance of Female Journalists in Pakistan", Digital Rights Foundation, December 31, 2016,http://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf.

27. Here the spread of compromising pictures or videos does not lead only to personal embarrassment but can lead to girls being removed from school, being forcefully married to save face or in extreme circumstances, having bodily harm inflicted. So the need for a safer internet and safer and more trustworthy access to internet is crucial in our region.

e. Encryption

28. As reflected under the UN's interpretation of Article 17[23], states should promote strong encryption and anonymity by enacting laws that ensure that the right to privacy is extended equally to secure digital communications through the use of encryption technology and tools that allow anonymity online.

29. However, the government's attempt to legislate the usage and proliferation of Virtual Private Networks (VPNs) and other encryption mechanisms is a blatant violation of the right to privacy of the Pakistani people. It adversely impacts their ability to connect through an encrypted network and protect their information and also impacts businesses that rely on secured network and encrypted communications.

30. It also highlight the continuation of repeated attempts by the government to block the use of VPNs and other encryption mechanisms as a part of anti-terrorism efforts under the larger security narrative.
31. For instance browser add-ons such as HTTPS Everywhere -- which are also tools for encrypting communications on browsers to ensure that users are not susceptible to hacking attempts -- surprisingly remain in place[24].

---

[23] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015), Also, see the Guide to International Law and Surveillance, August 2017, https://privacyinternational.org/feature/993/guide-international-law-and-surveillance

[24] Adnan Chaudhry, Content Regulation in Pakistan's Digital Spaces: June 2018 Human Rights Council Report December 2017,

32. In 2011, the PTA issued a directive to internet service providers ordering them to inform the government if any of their customers are using VPN to browse the web and called for the banning of encryption mechanisms except on a case by case basis, provided a formal request has been made to the PTA[25].

33. Furthermore, in 2014, the PTA published a notification in newspapers announcing that unregistered VPNs be registered, which paved the way for businesses to register their VPNs in order to use them legally. However, the ban on encryption remains.

f. Collection of Biometric Data

34. Pakistan's National Database & Registration Authority (NADRA) maintains one of the world's most extensive citizen registration databases, with over 96% of the population holding biometric CNICs (Citizens National Identity Card)[26].

35. A CNIC is mandatory to get a sim card, broadband connection, driver's license, passport, bank account and so forth. After the APS attack in 2015, biometric thumb impression was made a mandatory registration requirement for SIM cards.[27]

36. Lack of legal safeguards to protect citizens' personal data from surveillance by law-enforcement agencies (LEAs) raises red flags[28]. The extent to which the data is shared with and beyond government agencies and LEAs makes it imperative to question

---

https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/DigitalRightsFoundationSubmissionSpecialRapporteurFreedomofExpression.pdf

[25] State of Surveillance Pakistan January 2018, https://privacyinternational.org/state-privacy/1014/state-surveillance-pakistan

[26] Bytes for all, State of Privacy in Pakistan, January 2018, https://bytesforall.pk/sites/default/files/State-of-Privacy%20Pakistan.pdf

[27] Ahmad Fuad, "Biometric SIM verification: a threat or opportunity for cellular firms?" The Express Tribune, February 1, 2015, http://bit.ly/1LbAtJe

[28] Is Nadra keeping your data safe? October 2017, https://www.dawn.com/news/1290534

the level of security and confidentiality provided for the protection of personal data by NADRA.

37. These concerns are not unfounded given the growing surveillance apparatus, under which human rights defenders and journalists operate.

g. Emerging Issues

38. Law enforcement is employing technology for urban policing and counter-terrorism. For instance Sindh Police's Counter Terrorism Department (CTD) acquired phone locator technology to track calls.[29] The Punjab Safe Cities Authority launched a "Public Safety application" to facilitate tackling urban crime. The project has installed 8,000 CCTV cameras throughout the city of Lahore for policing purposes.[30] The Islamabad Safe Cities Project, under the Interior Ministry and National Database and Registration Authority (Nadra), has installed 1,800 surveillance cameras installed throughout the city.[31] The privacy implications of measures such as these are often ignored.

39. The involvement of the Chinese government in surveillance project is part of the larger the China-Pakistan Economic Corridor (CPEC) plan. According to leaked documents obtained by Dawn, the CPEC has a major focus on digital development—including e-governance, internet connectivity along the CPEC route, urban surveillance and telecommunications.[32] Contracts for these developments have been awarded to Chinese companies. Given the restrictive approach of the Chinese government towards digital

---

[29] Masroor Afzal Pasha, "Sindh Police to Get Mobile Tracking Technology," *Daily Times*, October 29, 2010, http://bit.ly/16TKfLY; "Punjab Police Lack Facility of 'Phone Locator', PA Told," *The News*, January 12, 2011, http://bit.ly/1bRl6bx

[30] Ather Ali Khan, "Another landmark achievement", The Nation, January 22, 2018, https://nation.com.pk/22-Jan-2018/another-landmark-achievement

[31] "Nisar inaugurates Safe Cities project in Islamabad", Dawn, June 6, 2016, https://www.dawn.com/news/1263107

[32] Qurat ul ain Siddiqui and Jahanzaib Haque, "Exclusive: The CPEC plan for Pakistan's digital future", *Dawn*, October 3, 2017, https://www.dawn.com/news/1361176.

freedoms and its intrusive approach to privacy citizens, there is a fear that these policies will filter through to Pakistan.

C. Recommendations

In order to address the right to privacy in the digital age, a two-tiered approach at both the local and international level will have to be undertaken to ensure that the right is protected from increasingly fluid and global trends.

1. At the the national level, strong and robust legislation will need to be enacted to ensure that the right to privacy and data protection are upheld, especially in relation to emerging technologies.

2. Establishment of an independent oversight of government bodies in the form of a Privacy Commission that can hold government bodies accountable for violations of privacy violations.

3. It has been noted that surveillance and data sharing across borders exploits loopholes for data protection and privacy, and there is little international oversight regarding these issues. Thus, cognizance over cross-border surveillance needs to be taken and measures should be taken to ensure that data sharing by governments is curtailed.

4. International law needs to develop mechanisms and remedies for when citizen's data is illegitimately accessed by foreign governments.

5. International bodies need to consider gendered surveillance is a form of surveillance and violation of privacy, and thus develop structures to address the different ways in which women, sexual minorities, disabled persons and other minorities experience surveillance.