PRIVACY RIGHTS UNDER THE LENS

Stakeholders' Joint Submission for Pakistan's Review under the Third Cycle of UPR

2017

www.bytesforall.pk

MediaMatters forDemocracy

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

PRIVACY RIGHTS UNDER THE LENS

Stakeholders joint submission for Pakistan's review under the third cycle of UPR

For consideration at the 28th Session UN Working Group - 2017

I. INTRODUCTION

The right to privacy plays a critical role as an enabling right to the exercise and enjoyment of other rights, as well as for the free development of an individual's personality and identity. It also protects and enhances an individual's ability to participate in political, economic, social and cultural life. It is to be noted with concern that any violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association, and in dire cases, the right to life.

This report is an overview of the state of privacy in Pakistan from 2012 – 2017, and is being jointly submitted by a coalition consisting of the following members: [1]

1. **Bytes for All, Pakistan**
2. **Media Matters for Democracy**
3. **Ending Violence Against Women and Girls (EVAWG) Alliance**
4. **Association for Progressive Communications**
5. **Vision Pakistan**
6. **Neengar Society**

II. METHODOLOGY

This report has been prepared with the help of primary and secondary research methods. These include expert interviews, consultations, independent studies, and media reports.

III. FOLLOW-UP TO FIRST AND SECOND UPR CYCLES

1. First cycle of Pakistan's UPR did not pay much attention to privacy rights or fundamental rights in digital spaces including access to internet and rights to freedom of expression and information. However, it took notice of the discriminatory laws and restrictions on the right to freedom of religion, highlighting the plight of religious minorities and women; and demanded for their equal rights.[2]

2. In the second UPR cycle, Pakistan received 166 recommendations in total under different thematic areas, including freedom of religion, freedom of expression, right to privacy, protection of human rights defenders and journalists, promotion of civil society and media, equal rights for women and minority groups and the internet rights.[3] During the review, the Netherlands recommended that Pakistan remove restrictions on accessing internet in the country, which runs counter to the criteria of the International Covenant on Civil and Political Rights (ICCPR) and the principle of proportionality (P-122.127). At least four recommendations were made to Pakistan to promote civil society, protect human rights defenders and bring the perpetrators of attacks to justice (P-122.56, P-122.75, P-122.101 & P-122.118). Austria urged Pakistan to introduce strong legislation to stop attacks on journalists and to investigate and prosecute the perpetrators (P-122.119).

3. In the second UPR cycle, the government committed to implement recommendations P-122.75, P-122.101 & P-122.118 to promote media and civil society, end impunity against journalists, bring the perpetrators of attacks on journalists to justice and enact legislation to stop such incidents in future. However, the government has not fully met the implementation of these recommendations. According to Committee to Protect Journalists (CPJ), 30 journalists and media workers have been silenced between 2012 and 2017 with confirmed and unconfirmed motives. Attacks on media offices were also recorded in the same period. Prominent columnist and anchor Raza Rumi[4] and television anchor and renowned journalist Hamid Mir received death threats and both survived in assassination attempts in 2014.[5]

IV. CONSTITUTION, LEGISLATION, AND INTERNATIONAL OBLIGATIONS

4. The State of Pakistan guarantees 'Privacy' as a fundamental right. Article 14 (1) of the 1973 Constitution of Pakistan[6] refers to 'privacy of home' and 'dignity of man' as 'inviolable', subject to law. Though the Constitution does not expressly protect privacy of communications, digital or otherwise, the principle of privacy extends to all forms. Moreover, Article 14 does not provide any limitations for laws that restrict the right to privacy to ensure that they are not arbitrary and that they comply with the principles of necessity and proportionality.

5. 'Freedom of Speech and Expression' is guaranteed as a fundamental right under Article 19 of the Constitution. While the Constitution officially limits the enjoyment of this right with "restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defense of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, [commission of], or incitement to an offense".[7] The limitations permitted under this provision are broad, vague and generally prone to abuse. The State has also actively used surveillance using these arbitrary indicators to undermine this right.[8]

6. Article 8 (1) and (2) of the Constitution provides that laws inconsistent with or in derogation of fundamental rights are void. However, Article 8 (3) puts forward a caveat ensuring that the provisions of the article do not apply to armed forces and police for the 'maintenance of public order, for the purpose of ensuring the proper discharge of their duties'.[9] This has allowed the state to enact clauses of laws such as the Telegraph Act 1885, Electronic Transactions Ordinance (ETO) 2002, Pakistan Telecommunications (Re-organization) Act 1996, and Investigation for Fair Trial Act 2013 to orchestrate broad surveillance to collect data with impunity.[10]

7. In 2015, the Supreme Court of Pakistan said that it may declare void any law that was in violation of the Articles 8 and 14 of the Constitution[11], however, no action has been taken to date.

8. The recently promulgated Prevention of Electronic Crimes Act (PECA) 2016, which was widely criticized by local and international CSOs, legitimizes the State's ability to access digital communications of citizens, retain data service provider's specified data for a minimum of one-year and share it with foreign governments and agencies. PECA poses a serious threat to the right to privacy as it permits the Pakistan Telecommunication Authority (PTA) and the designated investigation agency to access traffic data of telecommunication subscribers and confiscate netizens' data and devices without prior warrants from the court under Section 31. Section 35 of PECA 2016 permits the authorized officer to decrypt information, making it impossible for persons to use anonymity. Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.[12]

9. 'Right to Information' has been guaranteed as a fundamental right 'in all matters of public importance, subject to regulation and reasonable restrictions imposed by law' in the Constitution under Article 19-A. Due to the lack of clear guidelines defining reasonable restrictions, matters of public importance are arbitrarily dismissed due to subjective interpretation of this vague clause.[13]

10. Currently, no comprehensive data and privacy protection laws exists in the country. A draft bill prepared in 2005 still remains to be tabled in the parliament.[14]

11. Pakistan is a signatory to the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic Social and Cultural Rights (ICESCR), the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), International Convention on the Elimination of All Forms of Racial Discrimination (CERD), Convention on the Rights of the Child (CRC), and Optional Protocol to the Convention on the Rights of the Child on the sale of children child prostitution and child pornography. Therefore, the State has an explicit obligation to promote, protect, and guarantee the right to privacy for all.

V. STATE PRACTICES

12. Phone calls are tapped in a routine manner by intelligence bodies and law enforcement agencies (LEAs) such as Inter Services Intelligence (ISI), Intelligence Bureau (IB), Military Intelligence (MI) and the police. In 2015, the IB and ISI admitted before the Supreme Court of Pakistan that they were monitoring nearly 6,000[15] and 7,000[16] phone lines every month respectively.

13. The former President of Pakistan, late Farooq Ahmed Khan Leghari highlighted the role of phone tapping as one of the reasons for the dismissal of late Benazir Bhutto's second government.[17] In the past, women members of the National Assembly had also complained against the tapping of their phone calls.[18]

14. Having issued over 101 million identity cards,[19] Pakistan has one of the largest centralized biometric citizen databases in the world managed by the National Database and Registration Authority (NADRA). Despite a consistent track record of mismanagement demonstrated by data breaches[20], fake ID registration, and corruption[21], NADRA refuses to make public the details of its citizen data privacy policies. This raises alarms over safety of individuals' private data, which they are forced to trust this body with.[22 23]

15. Given the allegations of corruption and mismanagement, it comes as a shock that NADRA has shut down its whistleblower program without providing any reason. This shutdown takes away a critical channel that promised accountability and transparency in this large organization.[24]

VII. ROLE OF CORPORATIONS

16. The government, through a collaboration of NADRA and Huawei, is in the process of executing an advanced surveillance program under the name of 'Safe City Project' in the capital and various other cities.[25] Over 1900 cameras with facial recognition capability have been installed in Islamabad to monitor the activities of passersby. These 32-megapixel cameras and their facial recognition software link to NADRA's biometric database, and can also utilize global positioning system (GPS) to trace people using their SIM or IMEI code.[26] [27]

17. Several pieces of evidence including a report[28] by Citizen Lab and a data leak by a hacker called PhineasFisher have indicated the use of FinSpy, FinUSB and FinIntrusion Kit which are modules of an advanced surveillance spyware called FinFisher. Licensed in Pakistan, this notorious technology was found operating on government-owned Pakistan Telecommunication Limited (PTCL) servers. FinFisher allows surreptitious access to private information through the recipient's digital devices enabling privacy violations such as remote keystroke logging, remote webcam/microphone access, password gathering, and hacking of public WiFi networks.[29] [30] A public interest petition filed by Bytes for All, Pakistan in the Lahore High Court in 2013 questioning the use of this malicious Trojan is still pending.[31] In addition, Pakistan also contacted the HackingTeam expressing interest in a similar type of intrusion tool, Remote Control System (RCS).[32]

18. State institutions have been carrying out surveillance on digital communications of individuals, groups and organisations without transparency, legal safeguards, and judicial and public

oversight. According to a report, mass network surveillance is being conducted by the State using technology obtained from domestic and foreign surveillance companies including Alcatel, Ericsson, Huawei, SS8, and Utimaco.[33]

19. Corporations such as Facebook and Google have been noted to comply with private user information requests from the State.[34][35] The absence of specific details about these disclosures from the State as well as the collaborating corporations points to lack of transparency and oversight in this process. This highlights serious implication for the safety of internet users in the country.

20. Pakistani telecommunication companies, many of whom are subsidiaries of international corporations, appear to have 'murky' privacy policies that endanger customer data safety.[36]

VIII. FOREIGN GOVERNMENT PARTNERSHIPS

21. In 2013, the thousands of confidential documents leaked by US Government contractor and whistleblower, Edward Snowden, revealed that Pakistan was listed as a 'third-party' partner in United States' National Security Agency's (NSA), clandestine RAMPART-A mass surveillance program. A 'third-party' partner is one which allows the NSA to install surveillance equipment on its fiber-optic cables.[37] It is also known that Pakistan's ISI partnered with NSA and UK's Government Communication Headquarter (GCHQ) and participated in execution of Fairview and SKYNET mass surveillance programs.[38] SKYNET is a controversial program that acquires cellular network metadata of 55 million people from Pakistani telecoms and applies a 'scientifically unsound' algorithm to identify terrorists to launch attacks using Predator drones and on-the-ground death squads. The algorithm is reported to piece together over 80 different properties extracted from metadata to assess how an individual could likely be a terrorist. One such example is that of Al Jazeera's Islamabad bureau chief, Ahmad Zaidan, who was falsely marked and surveilled as an 'Al Qa'ida member'.[39] These alarming matters of concern are a threat to the privacy and freedom of expression, and puts at risk the lives of people residing in Pakistan.

22. In May 2017, the Islamabad High Court (IHC) ordered the Interior Ministry and PTA to scrutinize the internet to remove all instances of 'blasphemous content' online 'even if it meant blocking all access to social media platforms'. The court also asked for names of those committing blasphemy to be put on the Exit Control List.[40] [41] Such an order carries an implication that LEAs would increase their monitoring of expression on the internet. In an attempt to appease the IHC, the Federal Investigation Agency (FIA) went a step further and issued a vague ad in national newspapers asking the masses to keep an eye on 'blasphemous content' on social media and report it. [42] This encourages a culture of vigilantism. This is an alarming development as Pakistan not only prescribes capital punishment for those who commit blasphemy, the parameters within which it is defined are open to interpretation. Given the nature of social media, it is not uncommon to hijack online accounts and misuse them against their owners. Furthermore, the country has also seen a distressing trend of labelling progressive-minded people as blasphemers in order to silence them.[43] Blasphemy allegations are also used to settle scores against religious minorities[44], as well to carry out vigilante attacks against the accused and their families.[45]

IX. SOCIAL SURVEILLANCE

22. Internet rights[46] activists report living in fear of being constantly monitored by the State and having their work or private information being made the reason to harm them. A legal provision[47] exists restricting encryption through unregulated use of VPNs and may be used to arbitrarily persecute individuals. According to one case, a minorities rights activist whose work involved advocacy on Facebook was contacted by LEAs and asked not to leave the city or switch off his mobile SIM. His increased surveillance resulted in his organization distancing itself from him and shutting down the project.[48]

23. There is a strong concern of growing online and offline surveillance over progressive and liberal academics, and literary figures, due to which many resort to self-censorship in place of questioning state policies, religious radicalisation, foreign relations, and issues around separatist movements. This poses a great risk for the country's academic, intellectual, and democratic spaces.[49]

24. The monitoring of cyberspace by religiously radicalized individuals and organisations to pursue their violent agenda is alarming. According to journalist and researcher, Rabia Mehmood, *'In an interview with me, Shuhada Foundation's spokesperson admitted to monitoring social media networks, namely Twitter and Facebook for criticism of their activities. Furthermore, it is quite evident that they have monitored commentary of and carried out attacks against bloggers, journalists, human rights defenders and civil society members who identify as liberals or leftists.'* [50] Furthermore, many of these groups, including Islami Jamiat-e-Talaba and Khatm-e-Nubuwwat Lawyers Forum have been engaging in active surveillance of activists, especially the expression and activities of those belonging to minority religions. Such breaches of digital privacy eventually manifest in forms of cyber harassment and physical threats. For instance, a Christian boy was charged under blasphemy for 'liking' a post on Facebook.[51]

25. A crackdown on social media activists and secular bloggers was carried out in early 2017 by unidentified persons where

at least five activists, who ran social media pages which were considered 'controversial,' were abducted. These included Salman Haider[52], Waqas Goraya[53], Aasim Saeed[54], Ahmed Raza Naseer[55] and Samar Abbas[56]. No recourse has since been offered to them by the state[57]. An online counter campaign backed by nationalist pages on social media was run to malign these individuals and fan hatred in cyberspace. Waqass Goraya after his release disclosed that a state institution with links to the military held and tortured him.[58]

26. Anonymity provided in online spaces has allowed a large number of women, and marginalised religious and sexual minorities to participate in mainstream debates, strengthening the promise of inclusivity. However, it is a concern that the increase in online surveillance has started to force such individuals and communities to self-censor, retreat, or be targeted and attacked for their views or identities. While one reason for these receding spaces is the enactment of draconian laws such as PECA 2016 that enable surveillance without safeguards, radical religious groups have also started to sift the cyberspace looking to deliver 'mob justice' on the spot where possible.[59]

X. GENDER BASED DISCRIMINATION AND PRIVACY

27. As per consultative consensus from gender rights activists, lack of privacy and resulting implications remain one of the biggest barriers in the establishment of gender equality. Victim blaming is commonplace, and any breach of personal information including pictures can result in dire consequences for the victim, including lifelong character assassination, sex-shaming,, workplace and societal discrimination, damage to psychosocial health, forced marriage, and child marriage.[60]

28. The understanding of 'consent' remains largely unclear in the Pakistani society, and it is not uncommon for individuals to take pictures, make videos, record audios, or violate privacy through other means in personal and professional spaces. This is especially problematic if the target is a woman or a girl. In some instances, such activities result in sexual vio-

lence through blackmail or doxing of private information.[61] One such example is that of slain social media celebrity, Qandeel Baloch, whose personal information was leaked by popular journalists, which contributed to her murder by her own brother.[62]

29. In some conservative rural and urban pockets of the country, the family's 'honour' is traditionally tied with the girls and women in the household. Privacy breaches have led to their murders in the name of 'save the family honour'. In Gilgit Baltistan's town of Chilas, a woman and her two minor daughters were murdered over an audio recording of the mother talking to a male friend.[63] In Kohistan, four women and a minor girl were murdered after a video with a group of girls singing and clapping as two men performed a traditional dance in a wedding went public.[64]

30. A number of cases have been reported where women have been monitored and attacked with charges of blasphemy, anti-State activities or liberal expression by organized groups of online trolls. In these cases, propaganda via distribution of screenshots of their tweets or personal information to incite violence against them has been frequently reported. [65]

31. The lack of effective child protection and privacy safeguards are a matter of urgent concern as they often lead to sexual violence against minors. In what was named as 'the worst child abuse scandal in Pakistan's history,' at least 280 children were reported to have been abused on camera and later blackmailed along with their families in Kasur, Punjab.[66] A similar child abuse ring was uncovered in Swat, Khyber Pukhtunkhwa, where children were forced to have sex while being filmed.[67] In another case from South Punjab, a young girl was gang raped, and the perpetrators blackmailed her over a period of months after a group of men secretly filmed her with her lover.[68] In the province of Khyber Pukhtunkhwa, a 16 year old was sentenced to prison for sexually assaulting a minor girl on camera, and later distributing the footage and pictures via online and offline means.[69] Pakistan has ratified the Convention on the Rights of the Child and Optional Protocol

to the Convention on the Rights of the Child on the sale of children child prostitution and child pornography,[70] thereby committing to protecting children's rights in all possible ways. Continuing breaches of safety and privacy of minors reflect poorly on the state's efforts to fulfill its obligations.

32. Marginalised or persecuted sexual minorities find more space for exercising their freedom of association more privately in online spaces as compared to offline spaces. This is because, in offline spaces, the threat of physical violence in reaction to social taboos is a constant danger. However, several cases have surfaced where individuals were murdered after they revealed their identities to another individual on social media and mobile dating applications.[71] In one instance of a massive breach of privacy, over 250 individuals belonging to sexual minorities were outed without their consent when their private pictures that they had shared earlier on a dating application were posted on an Instagram account by unknown person(s). The account was deleted by Instagram after activists used back channels and international contacts to flag the issue[72] as social media platforms' direct reporting mechanisms are often ineffective and slow which can lead to dangerous consequences for the victim.

XI. RECOMMENDATIONS TO THE GOVERNMENT OF PAKISTAN

33. Enhance the capacity of the National Commission for Human Rights (NCHR) to monitor, analyse, and address privacy rights violations and other fundamental rights in online spaces, and extend the NCHR Act to include law enforcement institutions for better transparency and accountability;

34. Amend the Prevention of Electronic Crimes Act 2016 and Investigation for Fair Trial Act 2013 to incorporate privacy safeguards, and remove clauses that restrict openness and accountability in law enforcement procedures;

35. Develop and enact an effective privacy and data protection legislation which meets constitutional and international

obligations, and establish an independent and well-resourced Privacy Commission to ensure protection of citizen's privacy rights in offline and online spaces;

36. Amend Article 19 of the Constitution to remove unreasonable restrictions which allow monitoring of individuals on vague premises;

37. Ensure effective implementation of Punjab Transparency and Right to Information Act 2013, Khyber Pakhtunkhwa Right to Information Act 2013 and Sindh Transparency and Right to Information Bill 2017, and replace Balochistan Freedom of Information Act 2005 and the Federal Freedom of Information Ordinance 2002 with strong and effective RTI legislation;

38. Revisit chapter XV of Pakistan Penal Code 1860, which deals with desecration of religion to eradicate formalized monitoring of online spaces and violent vigilantism, and protect and promote free speech to meet international guarantees;

39. Ensure that protection of privacy and other fundamental rights is a part of the core design and management of mass data collection initiatives such as NADRA and the Safe City Project;

40. Ensure that private sector, in both policy and practice, comply with international human rights law and standards with regard to privacy and data protection;

41. 41. Introduce topics on digital security, privacy rights and other fundamental rights in school and university curricula;

42. Introduce effective legislation to ensure protection of whistleblowers in order to promote transparency and accountability in public institutions;

43. Ensure due process, judicial oversight, proportionality, transparency in matters of digital surveillance so that it does not infringe upon the privacy and freedom of expression

of citizens, in particular political activists, journalists, and human rights defenders;

44. Ratify the Optional Protocol of the Convention of All Forms of Discrimination Against Women, and develop an effective national policy to eliminate technological divide between all genders, as well as technology driven gender based violence, and dangerous speech.

END NOTES

i. [1] Bytes for All, Pakistan (B4A) is a human rights organization and a research think tank with a focus on Information and Communication Technologies (ICTs). It experiments with and organizes debates on the relevance of ICTs for sustainable development, democracy, social justice and strengthening human rights movements in the country. It focuses on securing digital rights and freedom of expression for civil liberties, strengthening digital security of human rights defenders & media professionals, ending technology-driven gender-based violence, and network building at national, regional and global level.
Website: www.bytesforall.pk

ii. Association for Progressive Communications (APC) is a network of organisations across the world, primarily advocating for the protection, promotion and respect of human rights on the internet. APC aims to empower and support organisations, social movements and individuals in and through the use of ICTs, to build strategic communities and initiatives for the purpose of making meaningful contributions to equitable human development, social justice, participatory political processes and environmental sustainability. It is actively engaged in internet governance mechanisms and processes at the WSIS, UNHRC and the regional and international internet governance forums.

iii. Media Matters for Democracy (MMFD) is a not for profit, 'Media Matters for Democracy' with a vision and a belief that a liberal, professional media industry is the cornerstone of a progressive, democratic society. MMFD strives for an inclusive, democratic media industry that is tech-friendly, progressive diverse, professional and secure, and work towards a digitally advanced, sustainable and empowered media.
Website: http://mediamatters.pk

iv. Ending Violence Against Women and Girls (EVAWG) Alliance is a network of civil society organizations and individuals. The Alliance aims to Lobby and Advocacy for the achievement of cause "End Violence against women and girls". This alliance is envisaged to function as a coordination platform on ending violence against women particularly in relation to provincial, national and international commitments on gender equality through making EVAWG a priority at national level, monitoring state commitments on EVAWG at all levels, and lobbying and advocacy for policy and legislative reforms on EVAWG through involvement and engagement of National Women machineries.
Website: http://bit.ly/2nO7Wbn

v. Vision Pakistan is a Pakistan based NGO that focuses on the rights of children and sexual minorities through research, capacity building, and advocacy.

vi. Neengar Society is a Pakistan based NGO that focuses on creating awareness about the rights and health of sexual minorities using theatre and other alternate means.

2. UPR Review (2008). Report of the Working Group on the Universal Periodic Review Pakistan. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/8/42&Lang=E
3. Universal Periodic Review. Second Cycle – Pakistan http://www.ohchr.org/EN/HRBodies/UPR/Pages/PKSession14.aspx
4. Columnist, anchor Raza Rumi attacked, driver loses life. https://www.dawn.com/news/1096198
5. I had threats from state and non-state actors: Hamid Mir. https://tribune.com.pk/story/699778/i-had-threats-from-state-and-non-state-actors-hamid-mi
6. The National Assembly of Pakistan. Constitution of Pakistan. (1973). http://na.gov.pk/uploads/documents/1333523681_951.pdf
7. Ibid.
8. Radio Pakistan. (2017). Nisar Vows to Block Blasphemous Content on Social Media. http://www.radio.gov.pk/16-Mar-2017/culprits-of-blasphemy-enemies-of-humanity-nisar
9. Bytes for All, Pakistan. (2014). Conflicting with the Constitution – Privacy Rights and Laws in Pakistan. http://content.bytesforall.pk/PrivacyLawsPakistan
10. Bytes for All, Pakistan. (2016). Internet Landscape of Pakistan 2016. https://content.bytesforall.pk/node/195
11. The Express Tribune. (2015). Over 5,000 phones being tapped by IB, SC told. https://tribune.com.pk/story/890674/over-5000-phones-being-taped-by-ib-sc-told/
12. The National Assembly of Pakistan. The Prevention of Electronic Crimes Act 2016 (Act No.XL of 2016). (2016). http://www.na.gov.pk/uploads/documents/1472635250_246.pdf
13. Bytes for All, Pakistan filed 11 RTI requests with NADRA asking for a range of information public interest information, including names and selection criteria of the NADRA's board members, a copy of NADRA's organogram, and NADRA's privacy policies. All of these requests were dismissed as information that did not fall under 'public record.' More information: http://rtirequests.pk/subject-of-rti-request-national-database-and-registration-authority-nadra/
14. Draft Electronic Data Protection Act 2005. http://media.mofo.com/docs/mofoprivacy/PAKISTAN%20Draft%20Law%202nd%20Revision%20.pdf
15. The Express Tribune. (2015). Over 5,000 phones being tapped by IB, SC told. https://tribune.com.pk/story/890674/over-5000-phones-being-taped-by-ib-sc-told/

16. Dawn. (2015). Nearly 7,000 phones tapped in May, ISI tells SC. Dawn. https://www.dawn.com/news/1186013
17. Ibid.
18. Dawn (2011). No end to phone tapping of women MNAs. https://www.dawn.com/news/649784
19. ProPakistani. (2016). NADRA Has Issued 101 Million ID Cards, Blocked 125K Fake Cards. https://propakistani.pk/2015/11/26/nadra-has-issued-101-million-id-cards-blocked-125k-fake-cards/
20. Pakistan Today. (2017). SBP looking into NADRA-MasterCard agreement over concerns of possible breach of security of national database. http://profit.pakistantoday.com.pk/2017/01/26/sbp-looking-into-nadra-mastercard-agreement-over-concerns-of-possible-breach-of-security-of-national-database/
21. Dawn. (2015). FIA to go after 'corrupt' Nadra officials. https://www.dawn.com/news/1180042
22. PakWired. (2016). How Secure Are NADRA's Critical Information Systems? https://pakwired.com/how-secure-are-nadras-critical-information-systems/
23. Bytes For All, Pakistan. (2016). RTI Requests - National Database and Registration Authority (NADRA). http://rtirequests.pk/subject-of-rti-request-national-database-and-registration-authority-nadra/
24. ProPakistani. (2016). NADRA Shuts Down Its Whistleblower Program. https://propakistani.pk/2016/04/13/nadra-shuts-down-its-whistleblower-programme/
25. Bytes for All Pakistan and APC. (2015, 17 November). Safe City Project or Mass Digital Surveillance? https://content.bytesforall.pk/node/181
26. Dawn. (2014). High tech surveillance system to be launched in Islamabad. https://www.dawn.com/news/1108273
27. The Express Tribune. (2016). Safe City Project gets operational: Islooites promised safety. https://tribune.com.pk/story/1117621/safe-city-project-gets-operational-islooites-promised-safety/
28. Citizen Lab. (2013). For Their Eyes Only: The Commercialization of Digital Spying. https://citizenlab.org/2013/04/for-their-eyes-only-2
29. Elaman German Security Solutions. FinFisher IT Intrusion Products. https://wikileaks.org/spyfiles/files/0/310_ELAMAN-IT_INTRUSION_FINFISHER_INTRODUCTION_V02-08.pdf
30. Dawn. (2014). Customer 32 — who used FinFisher to spy in Pakistan?. https://www.dawn.com/news/1127405
31. Bytes for All, Pakistan. (2014). Loss of privacy is always permanent - Snags in hearing of FinFisher case at Lahore High Court. http://content.bytesforall.pk/node/143
32. Dawn. (2015). Hacking Team hacked: The Pakistan connection, and India's expansion plan. https://www.dawn.com/news/1196767
33. Privacy International. (2015). Tipping the Scales: Security and Surveillance in Pakistan. https://www.privacyinternational.org/?q=node/624

34. Facebook Transparency Report. 2012 – 2016. https://govtrequests.facebook.com/country/Pakistan/2016-H1/
35. Google Transparency Report. 2012 – 2016. https://www.google.com/transparencyreport/userdatarequests/PK/
36. Dawn. (2016). Pakistani telecoms' murky policies put users' privacy at risk: report. https://www.dawn.com/news/1305364
37. The Intercept. (2014). How secret partners expand NSA's secret dragnet. https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/\
38. The Hindu. (2015). Pakistan has built a massive surveillance state: report. http://www.thehindu.com/news/international/south-asia/pakistan-has-built-a-massive-surveillance-state-report/article7462002.ece
39. arsTECHNICA UK. (2016). The NSA's SKYNET program may be killing thousands of innocent people. https://arstechnica.co.uk/security/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/

"In addition to processing logged cellular phone call data (so-called "DNR" or Dialled Number Recognition data, such as time, duration, who called whom, etc.), SKYNET also collects user location, allowing for the creation of detailed travel profiles. Turning off a mobile phone gets flagged as an attempt to evade mass surveillance. Users who swap SIM cards, naively believing this will prevent tracking, also get flagged (the ESN/MEID/IMEI burned into the handset makes the phone trackable across multiple SIM cards). Even handset swapping gets detected and flagged, the slides boast. Such detection, we can only speculate (since the slides do not go into detail on this point), is probably based on the fact that other metadata, such as user location in the real world and social network, remain unchanged. Given the complete set of metadata, SKYNET pieces together people's typical daily routines—who travels together, have shared contacts, stay overnight with friends, visit other countries, or move permanently."

40. The Express Tribune. (2017). Blasphemy: IHC directs authorities to block all social media if necessary. https://tribune.com.pk/story/1348784/ihc-directs-authorities-block-social-media-necessary/
41. The Nation. (2017). 'Put blasphemers on Exit Control List,' IHC tells govt. http://nation.com.pk/national/08-Mar-2017/put-blasphemers-on-exit-control-list-ihc-tells-govt
42. The News. FIA issues vague ads to please court in blasphemy case. (2017). https://www.thenews.com.pk/print/191638-FIA-issues-vague-ads-to-please-court-in-blasphemy-case
43. The Nation. (2017). Pakistani right cries 'blasphemy' to muzzle progressives. http://nation.com.pk/national/17-Jan-2017/pakistani-right-cries-blasphemy-to-muzzle-progressives
44. Independent. (2012). Pakistan blasphemy laws increasingly misused to

settle petty disputes against Christians. https://www.independent.co.uk/news/world/asia/pakistan-blasphemy-laws-increasingly-misused-to-settle-petty-disputes-against-christians-a6768546.html
45. The Washington Post. (2012). In Pakistan, vigilante attacks on the rise against accused blasphemers. https://www.washingtonpost.com/world/asia_pacific/in-pakistan-vigilante-attacks-on-the-rise-against-accused-blasphemers/2012/07/13/gJQAloi7hW_story.html?utm_term=.5cfe25caaf4e
46. International Human Rights Clinic, Harvard Law School. (2015). Securing Safe Spaces
47. Online: Encryption, online anonymity, and human rights. http://hrp.law.harvard.edu/wp-content/uploads/2015/06/Securing-Safe-Spaces-Online-2.pdf
48. Pakistan Telecommunication Authority. (2010). Directive No.17-1/2010/Enf/PTA(VPN) Ref: PTA's Monitoring and Reconciliation of Telephony Traffic Regulations, 2010
49. Peter Jacob & Sunil Malik [Personal Interview]. (Feb 2017). Center for Social Justice (CSJ). Lahore
50. Hassan Karrar, Dr. [Personal Interview]. (Feb 2017). Lahore University of Management Sciences (LUMS)
51. Rabia Mehmood [Personal Interview]. (Mar 2017). Lahore
52. Peter Jacob & Sunil Malik [Personal Interview]. (Feb 2017). Center for Social Justice (CSJ). Lahore
53. Salman Haider. (2017).Front Line Defenders. https://www.frontlinedefenders.org/en/profile/salman-haider
54. Waqas Goraya. (2017). Front Line Defenders. https://www.frontlinedefenders.org/en/profile/waqas-goraya
55. Asim Saeed. (2017). Front Line Defenders. https://www.frontlinedefenders.org/en/profile/asim-saeed
56. Ahmed Raza Naseer. (2017). Front Line Defenders. https://www.frontlinedefenders.org/en/profile/ahmed-razanaseer
57. Samar Abbas. (2017). Front Line Defenders. https://www.frontlinedefenders.org/en/profile/samar-abbas
58. Disappearance of activists echoes in parliament. http://www.dawn.com/news/1307532/disappearance-of-activistsechoes-in-parliament
59. BBC. (2017). Pakistan activist Waqas Goraya: The State tortured me. http://www.bbc.com/news/world-asia-
60. 39219307
61. Peter Jacob & Sunil Malik [Personal Interview]
62. Bytes for All GenderTech & Privacy Event. (Feb 17, 2016). Feedback from Expert Focus Groups.
63. Bytes for All GenderTech & Privacy Event
64. GenderIT.org. (2016). Invasion of Privacy and the Murder of Qandeel Baloch. http://www.genderit.org/es/node/4756
65. The Express Tribune. (2013). Chilas town: Saving 'honour' or family riches.

https://tribune.com.pk/story/576737/chilas-town-saving-honour-or-family-riches/
66. The Express Tribune. (2016). Kohistan 'honour' killing: Four years on, no justice in sight. https://tribune.com.pk/story/1034553/kohistan-honour-killing-four-years-on-no-justice-in-sight/
67. Bytes for All, Pakistan. (2014). Case Studies - Technology Driven Violence Against Women. http://content.bytesforall.pk/CaseStudies-Technology-DrivenViolenceAgainstWomen
68. BBC News. (2015). Pakistan child sex abuse: Seven arrested in Punjab. http://www.bbc.com/news/world-asia-33843765
69. Daily Pakistan. (2016). Another organized child abuse ring discovered in Pakistan, hundreds of photos and videos recovered. https://en.dailypakistan.com.pk/headline/organized-child-abuse-jolts-khyber-pakhtunkhwa/
70. Bytes for All, Pakistan. (2014). Case Studies - Technology Driven Violence Against Women. http://content.bytesforall.pk/CaseStudies-Technology-DrivenViolenceAgainstWomen
71. Dawn. (2013). First child convicted in KP of pornography. https://www.dawn.com/news/1031509
72. UN OHCHR. http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=131&Lang=EN
73. The New York Times. (2014). Pakistani Says He Killed 3, Using Gay Site to Lure Them. https://www.nytimes.com/2014/04/29/world/asia/pakistani-man-confesses-to-using-gay-sites-to-lure-victims.html?_r=0
74. Chay Magazine. (2015). Lahori Grindr Boys Exposed. http://www.chaymagazine.org/2015/11/20/lahori-grindr-boys-exposed/

Neengar Society