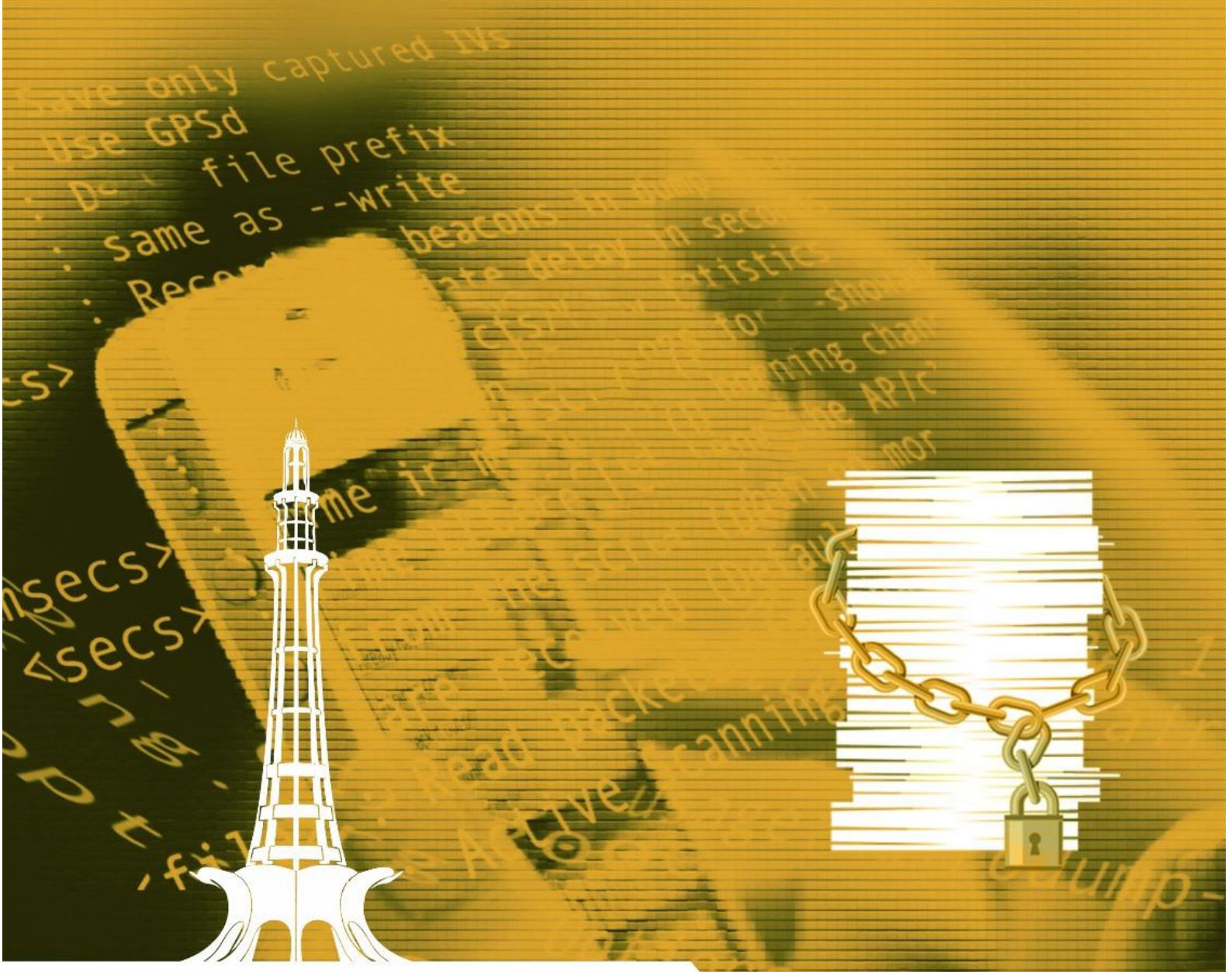
TELECOMS PRIVACY & DATA PROTECTION POLICIES IN PAKISTAN

A RESEARCH STUDY BY DIGITAL RIGHTS FOUNDATION



Digital Rights Foundation
"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

ABOUT

Digital Rights Foundation is a research based advocacy organization based in Pakistan focusing on ICTs to support human rights, democratic processes and better digital governance. DRF opposes any and all sorts of online censorship and violations of human rights both online and offline. We firmly believe that freedom of speech and open access to online content is critically important to the development of social and economic progress in Pakistan.

www.digitalrightsfoundation.pk

ACKNOWLEDGEMENTS

"Telecoms Privacy & Data Protection Policies in Pakistan" was researched, written, edited, and designed by Adnan Ahmad Chaudhri, Nighat Dad, Shmyla Khan, Luavut Zahid and Hija Kamran.

Many thanks to Ranking Digital Rights for inspiring this study. Please follow their valuable work, evaluating some of the world's most powerful internet and technology corporation, and investigating their commitment to their customers and users right to privacy and freedom of expression at:
https://rankingdigitalrights.org/

Many thanks to Privacy International for their support of Digital Rights Foundation's work, and for their untiring fight for privacy rights, on behalf of all citizens across the world. You can follow their work at:
https://www.privacyinternational.org.

TABLE OF CONTENTS

DigitalRightsFoundation

TELECOMS PRIVACY & DATA PROTECTION POLICIES IN PAKISTAN

INTRODUCTION

According to the Pakistan Telecommunication Authority, as of the end of September 2016 there are approximately 135 million cellular subscribers in Pakistan, and nearly 35 million 3G/4G subscribers, out of a total national population of nearly 194 million.[1] These subscriber bases are shared between a handful of foreign cellular telecommunications companies operating in Pakistan, of whom a number are in turn owned – either wholly or via shares – by foreign state-owned entities. Given the ownership structures and commercial nature of the operations of telecoms companies in Pakistan, it is essential that telecoms companies convey to their customers in clear and transparent terms just what will be done with their personal and traffic data. The passage of the Prevention of Electronic Crimes Act in August 2016 – which allows for retention of user data as authorities see fit, and sharing of data between the government of Pakistan and foreign agencies and states – and the absence of data and privacy protection legislation in Pakistan give the need for transparent privacy policies greater necessity.[2]

Subscribing to and setting up a broadband connection in Pakistan can be seen as quite costly for the majority of households in Pakistan, and also presupposes that there *is* available coverage across the country, owing to inconsistent telecommunications and overall infrastructure in Pakistan. With the formal introduction of internet-capable 3G and 4G networks in 2014, and low-cost smartphones – primarily running the Android operating system – made and sold by Chinese and Pakistani companies, however, *mobile* internet has been taken up by Pakistanis far more readily. Pakistan is a developing nation with a weak economy, with smartphone ownership at 11% as of early 2016.[3] In the context of the introduction of the 3G/4G

[1] "Telecom Indicators." Pakistan Telecommunication Authority, 18 Cot. 2016. Web 02. Dec. 2016. <http://www.pta.gov.pk/index?Itemid=599>

[2] Khan, Raza. "Cyber Crime Bill Passed by NA: 13 Reasons Pakistanis Should Be Worried." *Dawn.com*. Dawn News, 11 Aug. 2016. Web. 02 Dec. 2016. <http://www.dawn.com/news/1276662>

[3] Poushter, Jacob. "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies." *Pew Research Center's Global Attitudes Project*. N.p., 22 Feb. 2016. Web. 03 Dec. 2016. <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>

networks to Pakistan in 2014, however, this ownership percentage is impressive and is expected to increase further by the end of 2016.

The total cellular subscriber base in Pakistan is shared between six telecoms companies: Mobilink, founded in Pakistan but now owned by Russian-founded – and now headquartered in Amsterdam, The Netherlands - VimpleCom Ltd; Ufone, owned by Emirates Telecommunications Corporation (Etisalat) as of 2006; Zong, wholly owned and created by China Mobile; Telenor Pakistan, wholly owned by the Norwegian Telenor Group; Warid, founded in Pakistan and as of July 2016 has formally merged with Mobilink (for the purposes of the report, however, we are treating them as a separate entity); Special Communications Organisation (SCO), a government-owned entity that provides telecoms services to Gilgit Baltistan and Pakistan-administrated Kashmir (lack of sufficient coverage and data means that the SCO will not be covered in this version of the study).

Given that Pakistan does not have specific data protection legislation, this becomes a matter of concern: who has the right to access the personal data of Pakistani cellular users – including national identification numbers, biometric and geolocation metadata – and what happens to that data? Is the privacy of Pakistani citizens at risk from state and non-state actors? If so, what are these companies doing about it?

Visiting the websites of each of the companies listed, current and potential subscribers should be able to take a look at each company's privacy and data policies. Beyond the generic language, however, for the most part the privacy policies do not provide adequate details as to what takes place in the event of a government request of user data, or what happens if a customer's personal data has been stolen by hackers. Telenor Pakistan's parent company, Telenor Group, for example, 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. This contrasts with Telenor Pakistan, the local subsidy, whose own privacy policy as listed on their website is general and at times unclear.

Pakistan's lack of data protection legislation is a concern whether telecommunications companies are wholly-owned by domestic or foreign stakeholders. In either case, questions have to be asked: who has the right to access the personal data of Pakistani cellular users –

including national identification numbers, biometric and geolocation metadata – and what happens to that data? Is the privacy of Pakistani citizens at risk from state and non-state actors? If so, what are these companies doing about it? The privacy and data protection policies of these companies, furthermore, do not address the recent change in Pakistani law, with the passing of the Prevention of Electronic Crimes Act in August 2016, which has provisions that could have serious ramifications for telecoms in Pakistan, and the people that use them.

OBJECTIVES

Revelations by the American National Security Agency (NSA) whistleblower and former NSA contractor, Edward Snowden, have exposed the extent to which telecoms and social media platforms have been exploited by the NSA and other intelligence agencies to track and spy on millions of people around the world, including employees of the Qatar-based media organisation, Al Jazeera.

This whistleblowing has led to debates and action taken by activists and governments across the world, emboldening - and in some measure, frustrating - privacy and surveillance work everywhere. We have learned of the infiltration of Pakistan's Internet Exchange by the UK's GCHQ[4], for example, and the usage of the mobile phone records of 55 million Pakistanis by the NSA to track individuals in Pakistan and Afghanistan, without the consent or knowledge of said users, including Al Jazeera's Islamabad bureau chief.[5] In this global context, it is imperative that cellular companies operating in Pakistan be transparent as to how they protect their users' data, and how they formulate privacy policies.

Digital Rights Foundation is carrying out this research study in order to provide Pakistani cellular telecoms customers – current and prospective – information and analysis on the extent to the privacy policies provided by their chosen cellular providers which are available to the public protect their privacy – or otherwise – and the extent to which – and by/to whom – their information is shared. The lack of clear and effective data protection legislation in Pakistan, as well as the current legal uncertainty regarding the PECA, leave Pakistani cellular internet and phone users potentially at great risk. The aim of the study is to ensure that cellular telecoms users in Pakistan are aware as to where their information goes, how that information is used and how the users can take steps to push for greater responsibilities from their cellular providers.

[4] Fishman, Andrew, and Glenn Greenwald. "Spies Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law." *The Intercept*. N.p., 22 June 2015. Web. 03 Dec. 2016. <https://theintercept.com/2015/06/22/gchq-reverse-engineering-warrants/>

[5] Chaudhri, Adnan A. "Spectrum Eyes: The NSA & Pakistani Metadata." *Digital Rights Foundation*. N.p., 14 May 2015. Web. 03 Dec. 2016. <http://digitalrightsfoundation.pk/spectrum-eyes-the-nsa-pakistani-metadata/>

RESEARCH METHODOLOGY

The study comprised of a series of questions given to personnel at each telecom company responsible for the creation and development of each privacy policy. The questions were to be in two batches. The first batch of questions were emailed or personally given to said personnel, and covered the following areas, each of which was broken up into sub sections:

1. *Does the company have a privacy policy that can be easily accessed by customers and the public at large?*

2. *What safeguards are in place to protect customer/user data privacy and security?*

3. *What are the standard operating procedures (or SOPs) and framework concerning local and foreign government requests for customer/user data?*

4. *In the wake of the passing of the Prevention of Electronic Crimes Act – Pakistan's cyber-crime legislation - what are the ramifications, if any, for your company, in regards to current customer privacy, data protection and government request practices?*

Using the responses that we would receive, we would develop a series of follow-up questions, informing recipients that we would be doing so, to elaborate on the previous set of answers. The aim of this would be to gain a much more rounded picture of the state of the company's privacy policies and their approaches towards customer data protection.

Unfortunately, the intended follow-up questions never came to pass. Despite numerous attempts to either make initial or follow-up contact with the major cellular telecoms companies in Pakistan, we were left with a total lack of responses to the first set of questions – even in cases where companies we reached out to had initially agreed to get back to us with answers.

The lack of responses ensured that the structure of the study would change, and focus on an analysis of the privacy policies that were currently available, or otherwise, at the time of writing.

The aim in reaching out to the telecoms companies was to notify them of our intentions, and to include them in the process – not only to allow them to provide insight into how they came to develop their respective company's privacy policies, but to also highlight their commitment to protecting the data of their subscriber bases. The lack of responses, initial or follow-up, is of concern.

As the study shows, while there were some positive aspects to a few of the privacy policies that we examined, there were structural or formatting problems that appeared to indicate that attention was not, at least visibly, being given to their customer's data privacy. In one instance, for example, one company gave customers the option to report "a breach of privacy" via a "privacy breach form", ostensibly available on the same page. No link or sample of a "privacy breach form", however, could be found.

We also found cases where the parent company of the telecoms entity being studied would have clear and fairly well laid out privacy policies and safeguards in the event of requests by government or non-government entities - only for their Pakistani subsidiaries to display generic privacy policies, if at all.

CONSTITUTIONAL & LEGAL PROTECTION OF PRIVACY AND DATA IN PAKISTAN

Data protection is commonly defined as legislation designed to protect one's personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system."[6] Data protection legislation is necessary to protect against companies and government abuses and to empower individuals to control our data, including against unlawful surveillance by governments and sharing with third parties. Data protection legislation also requires companies to protect personal data against breaches (such data theft) and to provide individuals with means of redress against abuses.

What constitutes personal data or information? Personal information means any kind of information that can personally identify an individual or single them out as an individual. The obvious examples are somebody's name, address, national identification number, date of birth or a facial image. But it may also include traffic data and location data, such as that collected by mobile phone companies.

Governments and other entities may require or request access to personal data to customise or modify their services, either to better serve the public, or to increase profit margins. Should that personal data be leaked or otherwise illegally accessed, it can violate the rights of an individual, and/or put them in harm's way.

Strict data protection or privacy legislation works to, in theory, ensure that there are strong safeguards to ensure the effective storage of personal data, and ethical usage of said data in a manner. Strong data protection legislation that is proactively enforced also means that companies and corporations are not allowed to make use of your data without your consent or permission, including biometric data.

Proper data protection legislation is that which has been formulated by various stakeholders, including the government, rights organisations, constitutional and civil rights legal specialists and Informational Technology (IT) experts, to reflect a progressive and ethical balance between security and privacy.

---

6 "What Is Data Protection?" *Data Protection*, Privacy International, Web. 02 Dec. 2016 <www.privacyinternational.org/node/44.>

On paper, the Government of Pakistan – much like other governments across the world – respects the right of its citizens to privacy. The Constitution of the Republic of Pakistan declares privacy to be a fundamental right afforded to all citizens of Pakistan. Article 14 (1) of the Republic of Pakistan's Constitution affirms that the "dignity of man, and subject to law, the privacy of home, shall be inviolable." Article 8 of the constitution contains provisions that state, as in 8(2), "that the "State shall not make any law which takes away or abridges the rights so conferred and any law made in contravention of this clause shall, to the extent of such contravention, be void."[7]

This same document and article contain clauses, however, that provide exceptions to the police, armed forces "or of such other forces as are charged with the maintenance of public order, for the purpose of ensuring the proper discharge of their duties or the maintenance of discipline among them", to quote Article 8 (3).

Data protection is commonly defined as legislation designed to protect one's personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system.

Beyond the constitution, the Government of Pakistan has not enabled any legislation that directly recognises and provides strict data protection. The Electronic Transactions Ordinance 2002, designed to legally recognise "electronic forms" of documents, communications and transactions, does not provide protection for the misuse or theft of the data of citizens.[8] The only section that deals with data protection is Article 43 2 (1), which provides that "regulations may provide for" the "privacy and protection of data of subscribers" (1e). The Ordinance does not elaborate further and no regulations were promulgated to provide for this gap in the law.

This is not to say that attempts have not been made to remedy the situation. In 2005 the Pakistan Software Export Board drafted the Electronic Data Protection Act, designed to "provide for the processing of electronic data while respecting the rights, freedom and dignity of natural and legal persons, with special regard to their right to privacy, secrecy and personal

[7] "The Constitution of the Islamic Republic of Pakistan." *The Constitution of Pakistan*. N.p., n.d. Web. 02 Dec. 2016. <http://www.pakistani.org/pakistan/constitution/>.

[8] Electronic Transaction Ordinance 2002, Ministry of Law and Justice, Government of Pakistan n.d. Web. 02 Dec. 2016. <https://tinyurl.com/z28dlav>

identity".[9] Though the Act would have still permitted data collection by the state, it set forth provisions that called for transparency on the part of state actors, and recognition of consent on the part of parties from whom the data would be collected, as well as respect for rights, as mentioned above. There has been no update since 2005 on the proposed Electronic Data Protection Act, however, and as of the time of this report it has not been revisited by the Government of Pakistan.

On August 11, 2016, the Government of Pakistan passed the Prevention of Electronic Crimes Act (PECA), a controversial cybercrime law with broad reach. The PECA has come under fierce criticism by domestic and international rights organisations and bodies, not just for reportedly disproportionate penalties, but for overly broad language that runs the risk of ensnaring innocent internet and digital service users, depending on the interpretation of "authorised officers".[10] The PECA has also come under fire for including data retention provisions that make it mandatory for service providers to hold traffic data for a 90 day minimum or as "authorised officers" see fit. The PECA does not, however, explicitly list any provisions for data privacy or protection, outside of conditions that officers of the law must provide anyone "with a legal right to the data" a list of said data, and copies of said data, though this can be refused by an "investigating officer" if there are "reasonable grounds." Via this language, the PECA attempts to skirt around the lack of stringent data protection provisions or oversight within the overall legislation. Service providers cannot refuse to hand over data, for example, or else risk being penalised by the government, for instance. Further to this, Article 39 of the PECA, "International Cooperation", permits the government to share whatever data it gathers with foreign government agencies in the context of the powers of this Act, even without "prior request" by said foreign partners.[11]

This dovetails into our concerns with the cellular telecommunications companies currently operating within Pakistan, in part because of a lack of updates by said companies in the wake of the passage of PECA.

Digital Rights Foundation undertook this study to examine the privacy policies that are readily available to Pakistani cellular subscribers, the extent to which customers are made aware of

[9] Farooq, Mohammad. "Data Protection Act & Privacy: Pakistan Needs It Badly." *TechJuice*. N.p., 19 May 2015. Web. 02 Dec. 2016. <https://www.techjuice.pk/data-protection-act-privacy-a-pakistani-perspective/>.
[10] Khan, Raza. "Cyber Crime Bill Passed by NA: 13 Reasons Pakistanis Should Be Worried." *Dawn.com*. Dawn News, 11 Aug. 2016. Web. 02 Dec. 2016. <http://www.dawn.com/news/1276662>.
[11] "Prevention of Electronic Crimes Act 2016." National Assembly of Pakistan. Government of Pakistan, n.d. Web 02 Dec. 2016 <http://www.na.gov.pk/uploads/documents/1462252100_756.pdf>

their rights, and what will happen to their personal and traffic data, For the purpose of this study, scorecards were developed to gauge the levels of user friendliness, effectiveness and compliance with international standards that current privacy policies of telecoms companies in Pakistan meet, using metrics developed along the lines of Ranking Digital Rights own scoring system, which investigates the transparency and respect for human rights and user rights of major tech companies including Facebook and Google.[12] Parts of the index have been adjusted to take into account the specificities of telecom companies and their operations in Pakistan.

The index developed and used by Ranking Digital Rights has been used as an inspiration in this study in terms of scorecard development to populate the scorecards and see how the companies measure up. The RDR index provides a detailed breakdown of its indicators and the factors who consider when developing the rating: DRF has based its scorecards on the Privacy segment of the RDR indicators, given the other indicators would require affirmative disclosure by the telecoms companies in Pakistan - the latter being an action that all the companies we approached have been reluctant to do.

The major existing cellular telecommunications companies that currently operate in Pakistan have been put through the metrics.

While a number of the websites of the telecoms companies operating in Pakistan provided privacy policies on their websites, the research revealed some areas of concern: in many instances privacy policies were not easily accessible or quickly available via respective company websites, and had to be actively searched out; one privacy policy would go into detail, for instance, but provide links to downloadable forms that were not available; another company did not have any privacy policy available on the website of their company in Pakistan, but would have a clear policy outlined in other territories; the telecoms group that wholly-owned their Pakistani operations would have clear and well-thought pages pertaining to government and non-government requests, but would be very general when it came to the Pakistani operation; what privacy policies were available were in English, and not in Urdu or any other languages used in Pakistan, thereby ensuring that a segment of the population may not be fully aware of their rights regarding data privacy. Another problem that DRF faced was a lack of sufficient cooperation by some of the companies approached – ironically, for reasons of privacy.

[12] "2015 Ranking Digital Rights Corporate Accountability Index." Ranking Digital Rights. N.p., n.d. Web. 20 Dec. 2016. <https://rankingdigitalrights.org/index2015/>.

Data is currency. It is bought and sold by companies to advertisers and researchers, in order to best tailor their services to the same people whose data has been distributed. Data is also the currency used by state and non-state actors carry out mass surveillance, often without the knowledge and consent of the citizenry at large. In this context, this manner of study is essential to ensure that customers and citizens know how the companies they use treat their data, and treat their privacy, that a vital discussion can and will take place.

TELECOMMUNICATIONS COMPANY #1:

MOBILINK

(Pakistan Mobile Communications Limited)

Established: June 11th 1994 by Saif Group (Pakistan) and Motorola Inc (USA);
Global Systems for Mobile Communications (GSM) license obtained in 1992
Ownership:
Saif Group and Motorola Inc. until 2007;
Purchased by Orascom Telecom Holding (now Global Telecom Holding) (Egypt) in 2001;
Ownership by VimpleCom Limited (Russia) (Global Telecom Holding is a subsidiary of VimpleCom);
Private/Public Ownership: Mobilink is a public limited company, and a subsidiary of VimpleCom. VimpleCom is a private limited company, jointly owned by Altimo (Owned by the Alfa Group Consortium) and Telenor Group, at 47.85% and 42.95% respectively. The Telenor Group is a publicly owned company, with the Government of Norway owning 54%.
Subsidiaries/Brands: Jazz Prepaid Service, Jazba, Indigo Postpaid Service.
Personal Data Breaches: None reported as of November 30th, 2016
Privacy Policies: Three of Mobilink's company websites, www.mobilink.com.pk, www.mobilinkgsm.com, and www.jazz.com.pk/ list privacy policies, as of November 30th, 2016, accessible at the following URLs:

1. Customer Privacy Policy: https://www.mobilink.com.pk/help/customer-privacy-policy/
2. Mobilink, Privacy Policy: https://www.mobilink.com.pk/business/privacy-policy/
3. Jazz, Privacy Policy: https://www.jazz.com.pk/privacy-policy/

Of the three available privacy policies listed above, "Mobilink, Privacy Policy" goes into the most detail as to what data is requested by the company, with 2 and 3 being very general and brief, as well as being very similar in language and length to each other.

Protection of customer privacy "is a big deal" writes Mobilink, so they are "strict about how we handle your personal information." The policy is divided into seventeen numbered points, with many breaking down further for clarity and apparent transparency on the part of the company in regards as to what is done with customer data. This transparency, while laudable, also highlights the amount of information that is possibly gathered by telecommunications firms as

whole in Pakistan, and that which needs to be protected by stringent data protection legislation.

In addition to basic personal information – name, Computerised National Identity Card (CNIC) number, address, telephone number, email address, profession or occupation (listed as "Common Data" in 3.1) – the policy goes further. "Usage", "Traffic" and "Location data" are also collected by Mobilink – however, the terms "Usage" and "Traffic Data" have not been given any definitions within the policy, and are simply written as is. The policy, on the other hand, goes into detail about Location Data– something echoed by Sections 9 onwards.

For example, within Section 3, "the websites you visit and the online searches you perform" (3.2.2), and "the date, time and length of the calls and messages you send or receive through our network, and your general location at the time these calls and messages take place" (3.3.2) are listed, among others.

Section 4 of the privacy policy is where Mobilink explains why it collects customer data. In addition to requiring the data to carry out "market analysis and research", being able to contact users regarding services, and "identifying your location so we can send you emergency alerts", section 4.1.9 lists this: "Conducting internal investigations in relation to crime and fraud prevention, detection, recovery or prosecution." Rather than elaborating, however, Section 4 continues onto the promotional and marketing aspect of data collection. One positive aspect of the policy is the option to "opt out" of the data processing under section 5. The process of opting out, however, does not clarify what exactly one is opting out of, and what data processing remains as part of the basic and unavoidable data processing conducted by Mobilink.

Section 9 deals with data retention – which, in the wake of the passage of the Prevention of Electronic Crimes Act, is of concern. According to the policy, customer data – specifically "traffic and billing can and will be held for the following reasons:

"9.1. Data for scrutiny by the Pakistan Telecommunication Authority and Law Enforcing
9.2. Data for billing purposes; No retention period has been specified for the billing data in our Agencies.

9.1.1. As per our licensing clause 6.8 we are required to maintain call records including called and calling numbers, date, duration, time, IMEI and location details with regard to the

communications made on our Telecommunication System for a period of one year for scrutiny by or as directed by the Pakistan Telecommunication Authority.
9.1.2. In addition, we are also required to record/store data session logs/info along with IP address for one year for scrutiny by or as directed by the Pakistan Telecommunication Authority.

Mobilink Customer's Privacy Policy
9.2.1. Billing data for the postpaid subscribers is maintained for a period of six months.
9.2.2. Billing data for the prepaid subscribers is maintained for a period of sixty days."

The Prevention of Electronic Crimes Act, as indicated in the introduction, directs service providers to retain data for a period of at least one year - "or as directed" by the PTA. The lack of references to the PECA indicates that thus far Mobilink and its parent company have yet to update or revisit its internal data retention policies, as indicated above.

Section 11, "Who can we provide your personal data to?" indicates in 11.4 that "For the prevention or detection of crime or the apprehension or prosecution of offenders, the information is disclosed in confidence to that Operator; or as may otherwise be authorized by or under any law of Pakistan."

11.4, though appearing to be vaguely similar to 9.1, does not clarify which investigative body or department the data can or will be passed on to. Further to this, the authorisation "by or under any law of Pakistan" is overly broad, with the possible risk of customers being charged with the violation of any of the provisions of PECA without their knowledge or intent.

Unlike the PECA, however, section 10 of this Mobilink privacy policy, "Customer's Right", clarifies that customers have the right to request information pertaining to their personal data and "related processing activity"; "data update, deletion and ownership"; and the "protection policy adopted." While section 10 of the policy allows for customers to request information about the personal data processed by the company (a usual requirement under data protection standards), the policy does not however mention that under the PECA operators or service providers can be placed under a gagging order not to reveal if personal data have been requested by the investigative authorities or other forms of surveillance have been applied to their communications.

Mobilink, according to the policy, also collects cookies, including "persistent cookies" and the possible logging of IP addresses (section 12), for marketing, analytical and research purposes.

According to section 13, the company takes “all reasonable steps to securely store your personal information so it’s protected from unauthorized use, access, modification or disclosure.

This includes both physical and electronic security measures.” In the case of a stolen phone, the company has listed several phone numbers, email addresses to contact in the event of a theft, as well as the means of blocking said phone(s).

The policy also permits customers to report “a breach of privacy” via a “privacy breach form” - which does not appear to be on the webpage, and which will result in a member of Mobilink staff contacting the customer within ten business days.

Score: Good, with Room for Improvement.

Mobilink’s privacy policy is easily available and accessible, and can be easily understood. It is only available in English, however, and not in Urdu or any other languages of Pakistan. Formatting and grammatical errors, however, indicate that it is not regularly updated or monitored by Mobilink, which raises some concern.

The privacy policy listed what data is collected by the company, and how users can opt out of certain collection mechanisms. This could still be improved, however, as the language remains vague.

Recommendations:

Mobilink’s privacy policy page suffers from grammatical and formatting errors, and has clearly not been updated or reviewed on a regularly basis. Although opt-out and privacy breach report mechanisms have been identified and offered to customers, the “privacy breach” form that the page offers are not available. Mobilink must ensure that these are made available, and that amendments are made to the company’s privacy policy pages.

The privacy policy must be available in English and Urdu, as must any reporting mechanisms as discussed above.

TELECOMMUNICATIONS COMPANY #2:

TELENOR PAKISTAN

Established: Commercial services launched on March 15th 2005, GMS license obtained on May 26th 2004.
Ownership: Telenor Group (Norway)
Private/Public Ownership: Telenor Pakistan is a wholly-owned subsidiary of the Telenor Group, a Norwegian public company of which the Government of Norway owns 54%.
Subsidiaries/Brands: Tameer Micro Finance is a wholly owned subsidiary of the Telenor Group as of March 2016; Easypaisa; Djuice; Talkshawk; Postpaid
Personal Data Breaches: None reported as of November 30th, 2016.
Privacy Policies: As of November 30th, 2016, Telenor Pakistan's privacy policy is accessible at https://www.telenor.com.pk/privacy-policy and Telenor Group's Policies are available at: https://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/

Telenor Pakistan's privacy policy covers the form of data that is collected by the company, and echoes that of Mobilink, in regards to data being used for marketing and research purposes, as well as to "provide a service to meet your needs."

Where this privacy policy differs from that of Mobilink's is that the company may disclose "your Personal Data acting in good faith if it believes such action is necessary: to conform with a legal requirement or comply with the legal process, protect and defend the rights or property of Telenor.com.pk enforce this Online Agreement, or act to protect the interests of its users." The policy does not go into detail as to which law or laws it will disclose said data under, nor which investigating body, much like Mobilink.

Although Telenor Pakistan's privacy policy does indicate what personal data is collected by the company, the context in which it may be disclosed, and provides contact information regarding privacy concerns, the policy appears to fall short on specifics. This is in glaring contrast to the privacy policy available on the Telenor Group website which can be found at http://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/.
Unlike the Pakistani subsidiary, the Telenor Group website goes into detail and divides the different aspects of the Group's stances on privacy and data protection in different sections and webpages:

1. "Our Privacy Position"
2. "Understanding Our Privacy Position"
3. "Handling Request Authorities"

4. “How We Work with Privacy”
5. “Frequently Asked Questions”
6. “Privacy Statement”
7. “Privacy Contact”

As Telenor Pakistan is wholly-owned by the Telenor Group, it would be logical from an organisational and legal perspective that the former’s privacy policies would reflect that of the latter. It is only when we come to “Frequently Asked Questions” on the Telenor Group website that visitors to the website are informed that “Telenor’s position on Privacy applies to all our operations across our 13 markets.” Interestingly, it is also in “Frequently Asked Questions”[13] that we learn that Telenor “supports and endorses “Privacy by Design” (PbD)”, though it is not elaborated on within the website itself.

While the extent to which Telenor Group’s privacy policy as laid out is encouraging, that the Pakistani subsidiary does not carry the same information – or a modified version factoring in local legislation – is of concern.

“Handling Access Requests from Authorities”[14] reflects a holistic approach that Telenor Group has been publicly advocating and broadcasting. As the section begins, “law enforcement agencies (LEAs) and other authorities have the legal power to access the personal data we possess or information from our networks.” Where the section deviates however, is its laying out of the company’s overall stance, the balance that it must maintain between security and freedom. There is reference made to the validity of “access to historical data and lawful interception”, and Telenor’s recognition of its importance. But the company then writes that at “the same time, we recognize that there may be circumstances in which otherwise legitimate rights to access may be misused by authorities.” The section also states that “When a conflict regarding access to information arises, Telenor does its best to apply the higher standard, as outlined in the U.N. Guiding Principles for Business and Human Rights.” The page also lists reports that cover authority requests made by territory, including Pakistan.

By inference, the policies of Telenor Group are to be implemented by Telenor Pakistan, in theory - “inference” is used here, as the Telenor Pakistan website does not go into the detail that the parent company’s website does. But if so, it offers a valuable insight into the conflict

[13] "Frequently Asked Questions" *Privacy and Data Protections.* Telenor Group, n.d. Web. 02 Dec. 2016. <http://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/frequently-asked-questions/>.

[14] "Handling Access Requests from Authorities." Telenor Group. N.p., n.d. Web. 03 Dec. 2016. <https://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/handling-access-requests-from-authorities/>

and balance between cellular telecommunication markets, the rights of their customers, and government calls for data. We are focusing on “Handling Access Requests from Authorities” in particular as the section also details the company’s approach to data requests, and transparency in the form of engaging “with a range of stakeholders”.

While the extent to which Telenor Group’s privacy policy as laid out is encouraging, that the Pakistani subsidiary does not carry the same information – or a modified version factoring in local legislation – is of concern. Though the FAQ section does state that the privacy policies of Telenor Group “applies to all our operations”, there does not appear to be any mention or reference to specific Pakistani legislation: to find any reference, one must access the Authority Access Reports on the Telenor Group website, where the Pakistani laws referred to are The Pakistan Telecommunications (Re-Organisation) Act 1996[15], which “gives the Federal Government of Pakistan powers to authorise any person to intercept communications for national security reasons or for the investigation of any crime” and the Investigation for Fair Trial Act 2013, which highlights the necessity of the “Court’s approval for interception and acquisition of communications data relating to such terrorism-related offences.”

The Telenor Group’s privacy policies indicate transparency not just in what is done with personal data, or what is given to the authorities, but the protocols by which the company works to ensure that the data and rights of their customers are protected as much as is possible in the context of local laws and international rights guidelines. That the Group has a Privacy Officer – as do local subsidiaries of Telenor – and calls for active training of personnel in privacy and data sensitivity indicates that there is an identifiable culture of privacy protection. Telenor Pakistan’s privacy policy as outlined on their website does not go into detail, and does not provide clarity as to its limits or reach. Again, given the passage of the Prevention of Electronic Crimes Act, clarity and detail pertaining to what happens to the data of Pakistani Telenor customers is essential, and must be addressed by the company.

Survey responses: As with Mobilink, Digital Rights Foundation reached out to Telenor Pakistan. Although we were put into contact with Telenor Pakistan personnel, and distributed the questionnaire, we did not hear back from the relevant department, even though we were informed that we would receive responses to the questionnaire, despite numerous attempts. What Digital Rights Foundation staff members were told, furthermore, is that in order to

[15] "Pakistan Telecommunication (Re-Organization) Act, 1996 (with 2006 Amendments)." *Pakistan Telecommunication Authority*. N.p., 12 Oct. 2015. Web. 03 Dec. 2016. <http://www.pta.gov.pk/index.php?Itemid=616>.

continue further in this vein, Non-Disclosure Agreements (NDAs) would need to be signed. Digital Rights Foundation has not done so, as it would go against the nature of the study.

Score: Concerning.

The Telenor Group's website contains privacy policies and government request information that is well thought out and comprehensively broken down for customers. Telenor Pakistan's website, however, does not have a clear privacy policy present. It is unclear as to whether there is any clarification made between the Telenor Pakistan website, or Telenor cellular services. Telenor Pakistan does say that customer data may be shared with third parties, and that customers can request copies of their data, but again this is not made clear whether this is specifically for the website or cellular services.

Telenor Pakistan has been given a score of "Concerning" in particular in the context of the aforementioned comprehensive privacy policy and data privacy information that is provided by the Telenor Group.

Recommendations:

As mentioned above, the score that Telenor Pakistan has been given in the context of the transparency and detail of the privacy and third-party data request policies of its parent company, the Telenor Group.

Telenor Pakistan and its parent company must work to ensure that its own privacy policies regarding Telenor.com.pk and the cellular data of its customers in Pakistan are clearly marked out and made separate. A privacy policy must be made publicly available that reflects the clarity, detail and procedures that the Telenor Group website has provided as a model to follow. In doing so, it must also ensure that it is readily available in English and Urdu, as must the Customer's Charter.

Further to this, there must be regular update and review taken of said privacy policy, to ensure that all information is correct, and that the website pages themselves do not suffer from linkage or formatting errors. Telenor must also provide a downloadable complaint form in the event of customer concerns pertaining to possible privacy breaches. The Telenor Group must work to ensure that its subsidiaries in Pakistan and other territories are consistent in regards to Telenor's respect for privacy and security of its customers' data.

TELECOMMUNICATIONS COMPANY #3:

UFONE

(Pak Telecom Mobile Limited)

Established: January 29th 2001

Ownership: Etisalat (Emirates Telecommunications Corporation) as of 2006

Private/Public Ownership: Ufone is a wholly-owned subsidiary of the Pakistan Telecommunication Company Limited (PTCL), which was purchased by the Etisalat Group in 2005. Etisalat is in turned 60% owned by the Emirates Investment Authority as of September 2015, with 40% being free floated.

Subsidiaries/Brands: Prepaid; Postpay; Value Added Services; Upaisa

Personal Data Breaches: None reported as of November 30th, 2016

Privacy Policies: As of November 30th, 2016, Ufone's privacy policy is accessible at https://www.ufone.com/self-care/privacy-policy/

Ufone's privacy policy covers the same ground as Mobilink and Telenor, in that it provides a guide as to what personal data is to be used and why by Ufone, as well as what is to be shared with third parties. In regards to government requests Ufone states that it "may disclose your personal information to your authorized (sic) representatives" which include "Government, regulatory authorities and other organizations, as required or authorized by law." In addition to this,

"Ufone may also disclose your personal information acting in good faith if it believes such action is necessary to conform to a legal requirement or comply with the legal process, protect and defend the rights or property of Ufone and the interests of its other users."

As with Mobilink, usage of "good faith" appears to rely on parties requesting personal data to have legal and ethical intentions. What is troubling is that outside of the extensive marketing and promotional reasons that Ufone lists for utilising personal data, the two sections quoted above appear to be the entirety of the extent to which Ufone addresses actual data protection and requests by authorities.

Ufone has already run into controversy, when reports emerged in 2015 of Ufone inserting so called "pop under" adverts into websites visited by users of its 3G data services.[16] Its parent company, Etisalat, furthermore, received Ranking Digital Rights lowest score for 2015 of 14%. According to the organisation, Etisalat's "performance showed gaps across all indicators, notably with respect to how it manages user information, how it processes requests from external parties, and how it secures its information."[17]

Survey responses: Digital Rights Foundation reached out to Ufone. Unlike Mobilink and Telenor – who did not return the questionnaires we had sent them, but nonetheless communicated with us – Ufone refused to meet with Digital Rights Foundation personnel, or respond positively to emails or phone requests.

Score: Needs Improvement.

Ufone does provide a guide that indicates what personal data will be used and why by Ufone, as well as what is to be shared with third parties. It also states that it "may disclose your personal information to your authorized (sic) representatives" which include "Government, regulatory authorities and other organizations, as required or authorized by law" as well as "acting in good faith".

The language used by Ufone is nonetheless general, and does not allay any possible concerns that customers may have. Ufone needs to provide more detailed information, include breakdowns.

As with Mobilink and Telenor Pakistan, there is no indication of the availability of the privacy policy in Urdu or other regional languages of Pakistan.

Recommendations:

Ufone scored slightly higher than Telenor Pakistan, primarily for outlining what data is used by Ufone and what may be shared with third parties. The language and information available in the privacy policy is very general, however, and sorely lacking in detail. When Ufone say that they may modify the privacy policy "in responses to changes in privacy legislation", for

[16] Anwer, Rizwan. "Adware Alert: Ufone 3G Is Insecure, Displays Pop-under Ads While Surfing Websites." *TechJuice*. N.p., 04 June 2015. Web. 03 Dec. 2016. <https://www.techjuice.pk/adware-alert-ufone-3g-is-insecure-displays-pop-up-ads-while-surfing-websites/>.
[17] "2015 Indicators - Etisalat Group." *Ranking Digital Rights*. N.p., n.d. Web. 02 Dec. 2016. <https://rankingdigitalrights.org/index2015/companies/etisalat/>.

instance, they do not cite the legislation in question, leaving customers uncertain. This is unacceptable, and Ufone must revisit their privacy policy to more effectively reflect ongoing privacy concerns held by customers and potential customers.

Ufone must also provide reporting mechanisms in the event of a possible breach of customer data privacy, via downloadable privacy breach application forms. It must also work to ensure that the privacy policy is available in English and Urdu

TELECOMMUNICATIONS COMPANY #4:

WARID

(Warid Telecom)

Established: April 24th 2004, with commercial operations beginning May 23rd 2005
Ownership: VimpleCom Ltd, through the June 2016 merger of Mobilink and Warid
Private/Public Ownership: Warid, through the aforementioned merger with Mobilink, is subsidiary of the VimpleCom, and thus privately owned, however the Telenor Group does have a 42.95% share in the company.
Subsidiaries/Brands: Postpaid; Prepaid; Mobile Paisa; Glow.
Personal Data Breaches: None reported as of November 30th, 2016
Privacy Policies: As of November 30th, 2016, Warid's privacy policy is accessible at http://www.waridtel.com/privacy-policy

Warid's privacy policy indicates that they aim to collect "and use your personal information only with your knowledge and consent and typically when you order and subsequently use products and services, make customer enquiries, register for information or other services, request product information, submit a job application or when you respond to communications from us (such as questionnaires or surveys)." As with other privacy policies we have observed, the policy outlines the promotional, marketing and research usage of personal data.

In regards to disclosure or sharing of data, there is a point of interest that arises, especially relevant in the wake of the Mobilink-Warid merger:

"(ii) in the event that we undergo re-organization or are sold to a third party, in which case you agree that any personal information we hold about you may be transferred to that re-organized entity or third party for the purposes and subject to the terms of this Privacy Policy Statement. For the purposes of this Privacy Policy Statement, 'Warid Affiliates' or 'Warid Associates' means any company or other entity which directly or indirectly controls Warid, or is directly or indirectly controlled by any entity that controls Warid, or is directly or indirectly controlled by Warid."

What can be taken away from this is that personal data can be transferred without consent of the customer, albeit admittedly in exceptional circumstances. It also does not say if the data would continue to be protected or if the privacy policy were to change, given the Mobilink-

Warid merger. Though the merger was officially completed on July 1st 2016,[18] discussions held between Digital Rights Foundation personnel and a regional manager with one of Warid's Lahore offices indicate the full absorption of Warid's personnel and framework into Mobilink would be gradual.

As with Mobilink's privacy policy, Warid provides general information and definitions pertaining to cookies, and the purpose for which they are used. In regards to the protection of data:

"Warid is constantly reviewing and enhancing its technical, physical and managerial procedures and rules to protect your personal data from unauthorized access, accidental loss and/or destruction. We use industry standard secure sockets layer (SSL) technology, for example, to encrypt sensitive information such as your credit card and other financial information."

A final aspect to the privacy policy is a section entitled "Monitoring and/or recording of your communications". Whether this relates to communications with Warid itself or others has not been made clear, as seen by the section in its entirety:

"Monitoring or recording of your calls, emails, text messages and other communications may take place in accordance with the laws of Pakistan, and in particular for national security purposes or business purposes, such as for quality control and training, to ensure effective systems operation and in order to prevent or detect crime."

Survey responses: As with Mobilink and Telenor, interactions with Warid personnel were positive, but Digital Rights Foundation received no updates regarding the survey questionnaire at the time of writing.

Score: Good, with Room for Improvement.

Warid is a peculiar case, as it completed its merger with Mobilink in this year. For the purposes of the report, however, we have treated it as its own entity.

[18] "VimpelCom and Dhabi Group Announce Completion of Mobilink and Warid Transaction." *Warid Telecom*. N.p., n.d. Web. 03 Dec. 2016. <http://www.waridtel.com/media-center/press-release/archive/381>

As with Mobilink, Warid's privacy policy has been written clearly, explaining concepts such as cookies, and pointing out that in the event of a transfer or purchase of Warid, customer data may be transferred to other parties. By the same token, however, the privacy policy infers that it is possible that, although in very exceptional circumstances, customer data may be shared without the prior knowledge or consent of customers. It also remains to be seen what happens to Warid's privacy policies and mechanisms after the merger.

Warid has not included any other language options for the privacy policy. As with Mobilink, Telenor Pakistan et al, the privacy policy is only available in English, and not in any other regional languages.

Recommendations:

2016 has seen the merging of Warid with Mobilink, another major presence in Pakistan's cellular telecommunications market, and also reviewed above. Given the merger, it is unclear whether the internal privacy policies of Warid will remain their own, or if they will be overwritten by Mobilink. In each case, the recommendations that have been written regarding to Mobilink apply to Warid.

TELECOMMUNICATIONS COMPANY #5:

ZONG

(China Mobile Pakistan)

Established: 1990 as Paktel

Ownership: China Mobile, as of April 1 2008

Private/Public Ownership: Zong is wholly-owned by China Mobile Pakistan. CMP is in turn wholly-owned by China Mobile, which is owned by the State Council of the People's Republic of China.

Subsidiaries/Brands: Zong4G; Timpey; Zong Circle.

Personal Data Breaches: None reported as of November 30th 2016.

Privacy Policies: Unlike the previous cellular telecommunications providers, Zong's website (https://www.zong.com.pk/) does not appear to contain a privacy policy that can be accessed by the public. The nearest that the website comes is in their Code of Commercial Practice (https://www.zong.com.pk/about-zong/code-of-commercial-practice/), where the following are in regards to customer confidentiality:

"CMPak will make every commercially reasonable effort to protect our customers' privacy. In addition to this, we have a secure network for the confidentiality of their information (noting, however, that no system is 100% secure against deliberate and targeted security breaches). Also our customers' personal information will be safe with us and will be guarded as per laws of Pakistan.

Disclosure of customer's data has to be made where the designated government bodies i.e. F.I.A, IB, ISI, etc require subscriber data from time to time, or where investigation in reported illegal activities necessitates such disclosure."

The website also lists the applicable laws and statutes and gives precedence to Pakistani law when it states that "M/S CMPak Ltd. shall be governed by, and these terms and conditions shall be construed in accordance with, the laws of Pakistan without giving effect to the conflicts of law principles thereof." The website lists the governing laws that it binds itself to: "Pakistan Telecommunication (Re-organization) Act, 1996 (as amended); Pakistan Telecommunication Rules, 2000 and any other Rules issued by The Government of Pakistan from time to time; Pakistan Telecommunication Authority (Functions and Powers) Regulations, 2006 and any other; PTA Regulations issued from time to time, including but not limited to the Class

Licensing; and Registration Regulations, 2007 and the Telecommunication Consumers Protection Regulations 2009; Terms and conditions of the license issued to M/S CMPak Ltd. by PTA". This list itself is incomplete, as there are many other applicable laws.

Beyond this, however, Zong or China Mobile Pakistan's website is severely lacking in adequate explanations of the group's privacy policy. Further to this, the aforementioned paragraphs are not easily found, thus indicating a lack of proper user-friendly design. The state of Zong's privacy policies – or the lack thereof – is made even more glaringly visible when compared to China Mobile Hong Kong's own website[19]. The privacy policy displayed here covers the usage of personal data, transfer/disclosure and official requests of said data, as well as contact information for customers, with details and structure akin to Mobilink.

China Mobile Hong Kong, which is also a wholly-owned subsidiary of China Mobile Limited, asserts that they work to make sure that:

"Your personal data will be protected against unauthorized or accidental access, processing, erasure or other use. We maintain this commitment to data security by implementing appropriate physical, electronic and managerial measures to safeguard and secure your personal data. Personal data will only be retained for as long as is necessary to fulfill the original or directly related purposes for which it was collected, unless the personal data is also retained to satisfy any applicable statutory or contractual obligations."

What remains unclear is why Zong or China Mobile Pakistan have been unable to provide an easily accessible privacy policy for Pakistan.

According to the Pakistan Telecommunications Authority, as of the end of September 2016 China Mobile Pakistan's subscriber base was 26,156,593, placing it third after Telenor Pakistan (38,284,827) and Mobilink (40,604,402). In light of this and the controversial Prevention of Electronic Crimes Act, not having a privacy policy for Pakistani customers can place them in danger, and highlights an apparent lack of concern for the data protection and privacy in Pakistan. As a company wholly owned by a government that has been accused of cracking down on free speech and privacy in China and Hong Kong (Freedom House's 2016

[19] "Privacy Policy Statement."China Mobile Hong Kong Company Limited, n.d. Web. 03 Dec. 2016. <https://www.hk.chinamobile.com/en/corporate_information/Customer_Service/contract_terms_conditions/customer-support-privacy.html>.

Freedom in the World report has ranked China and Hong Kong as "Not Free"[20] and "Partly Free"[21], respectively), a lack of mention as to what happens to the personal data of Pakistani customers – who protects the data, and who the data is shared with is one that should be of concern to Pakistani citizens.

Survey responses: Absolutely no response or cooperation from China Mobile Pakistan personnel.

Score: Concerning.

Zong's website did not have a clearly defined or easy to find privacy policy at all. As indicated above, the document that comes closest to a privacy policy is in the company's Code of Commercial Conduct section, which listed the laws of Pakistan that Zong and China Mobile Pakistan must adhere to. This section also indicated that it would attempt to protect customer data as much as possible from unauthorized usage by others, but that it would also comply with government requests where possible. The sections that referred to these areas, however, were not easily found, which indicates a lack of user-friendly design.

As with Telenor, the availability of clearly laid-out and readily available privacy policies for websites in other territories where Zong's parent company operates makes the absence of Pakistan-specific privacy policies that much more glaring and a matter of concern.

As with the other major telecommunication operators in Pakistan, Zong does not provide any policies pertaining to privacy in Urdu or other regional languages.

Recommendations:

Each of the companies reviewed thus far have provided – to varying degrees - consistent privacy policies that have been gathered or compiled in one location or webpage. Zong, however, has not. A consistent and publicly available privacy policy does not appear to be present on Zong's website. A lack of communication with the company's head office in Islamabad, Pakistan did not help us to gain any further data that would have been constructive.

[20] "Freedom House: Freedom in the World 2016 - China." *Freedom House*. N.p., 2016. Web. 1 Dec. 2016. <https://freedomhouse.org/report/freedom-world/2016/china>.
[21] "Freedom House: Freedom in the World 2016 - Hong Kong." *Freedom House*. N.p., 2016. Web. 1 Dec. 2016. <https://freedomhouse.org/report/freedom-world/2016/hong-kong>.

What is required on the part of Zong, in order to gain customer trust, is a comprehensive revisiting of their attitude towards customer data privacy and security. Looking at other territories – Hong Kong was included in this study as a comparison – it is possible for Zong to do so. China Mobile must work to ensure that its Pakistani subsidiary, Zong, provides a clearly thought-out, transparent privacy policy that provides consistent clarity of language and detail, as well as the clearly indicated ability of customers to be able to report possible data privacy breaches. As with the other companies in this study, it must also work to ensure that the privacy policy and privacy breach report mechanisms are available in English and Urdu.

CONCLUSION:

The aim of this study was to examine the privacy policies of the major telecommunications providers in Pakistan, and the treatment of their customer's personal data. What Digital Rights Foundation found was inconsistency in regards to the public availability of said privacy policies, as well as an apparently lack of proper updates and oversight. None of the privacy policies that were available indicated an awareness of the passage of the 2016 Prevention of Electronic Crimes Act. Where provisions in the policies indicated that customers could contact the companies concerning possible privacy breaches, there were again inconsistencies, with Mobilink, for example, being unable to provide a privacy breach form on its website, despite stating so only a few paragraphs earlier.

In the introduction, we wrote of the rise in mobile phone and smartphone usage in Pakistan. Over 35 million 3G/4G subscribers in Pakistan have placed their personal and traffic data in the hands of a handful of telecommunication companies. It is important that these companies provide privacy policies that are in-depth, and provide clear and extensive breakdowns of what happens to their data, and with whom it is shared, whether by government or third-party entities.

English is a lingua franca in Pakistan, but it is still not widely spoken within the country. Mobilink, Telenor Pakistan and other telecommunications companies that operate in Pakistan must work to ensure that once they have developed well-thought out and in-depth privacy policies, that these same policies are made readily and widely available to citizens that may not speak English, but that speak Urdu, Punjabi, as well as other regional languages that are widely spoken in Pakistan.

As Digital Rights Foundations and other non-governmental organisations in Pakistan have written about at great length, Pakistan does not have explicit data protection legislation – something that Digital Rights Foundation and others have advocated for and continue to advocate for. In the absence of strong data protection legislation, telecommunication providers must pursue strong privacy policies and mechanisms that indicate to their customers that their data is protected.

TELECOMS PRIVACY & DATA PROTECTION POLICIES IN PAKISTAN

SCORE CARD

AVAILABILITY & ACCESSIBILITY OF PRIVACY POLICIES

Mixed | No | Mixed | Mixed | No

COLLECTION OF USER INFORMATION

Yes | No | Mixed | Mixed | No

NOTIFICATION & CHARGES

No | No | No | No | No

SHARING OF USER INFORMATION

Mixed | No | No | Mixed | No

YES meets all the criteria

NO meets none of the criteria

MIXED meets some of the criteria

MOBILINK

TELENOR

UFONE

WARID

ZONG

DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

USER CONTROL OVER INFORMATION SHARING & COLLECTION

Mixed | No | No | Mixed | No

USERS' ACCESS TO THEIR OWN INFORMATION

Mixed | No | No | No | No

RETENTION OF USER INFORMATION

Mixed | No | Mixed | Mixed | No

PROCESS FOR RESPONDING TO 3RD PARTY REQUESTS FOR USER INFORMATION

No | No | No | Mixed | No

USER NOTIFICATION ABOUT 3RD PARTY REQUESTS FOR INFORMATION

No | No | No | No | No

YES meets all the criteria

NO meets none of the criteria

MIXED meets some of the criteria

MOBILINK

TELENOR

UFONE

WARID

ZONG

DATA ABOUT 3RD PARTY FOR USER INFORMATION

No | No | No | No | No

SECURITY STANDARDS

No | No | Mixed | Mixed | No

INFORM & EDUCATE USERS ABOUT POTENTIAL THREATS

No | No | Mixed | Mixed | No

DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

SUMMARY

MOBILINK

Good, with room for improvement

TELENOR

Concerning

UFONE

Needs improvement

WARID

Good, with room for improvement

ZONG

Concerning

DigitalRightsFoundation
"KNOW YOUR RIGHTS"
www.digitalrightsfoundation.pk

APPENDIX

DigitalRightsFoundation
"KNOW YOUR RIGHT

- AVAILABILITY OF THE POLICY
  - ↳ Freely available
  - ↳ Language
  - ↳ Understandability
- NOTIFICATION AND CHANGES
  - ↳ Method of direct notification
  - ↳ Timeframe of notification
  - ↳ Public archive of change
- COLLECTION OF USER INFORMATION
  - ↳ Data minimization
  - ↳ Discloses what information is collected
  - ↳ Discloses how said information is collected
  - ↳ Discloses why said information is collected
- SHARING OF USER INFORMATION
  - ↳ Discloses what information it shares
  - ↳ Discloses why said information is shared
  - ↳ Discloses descriptions of 3rd parties info may be shared with
  - ↳ Discloses names of 3rd parties and what information is shared with said parties
  - ↳ Clearly discloses policies regarding multiple sources
- USER CONTROL OVER INFORMATION SHARING & COLLECTION
  - ↳ Provides users with options to control collection of info
  - ↳ Provides users with options over company's sharing of info

USERS ACCESS TO THEIR OWN INFO

- ➔ Allows users to view their data
- ➔ Are users allowed to receive a copy of their data
- ➔ Can data be downloaded in an structured format?
- ➔ Data including all public facing & private information that the company holds about a user

APPENDIX

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

- RETENTION OF USER INFORMATION
  - ↳ Discloses that it retains user information not actively submitted by the user in anonymised form
  - ↳ Discloses the types of user info it retains
  - ↳ Discloses how long it retains user info
  - ↳ Discloses that it deletes all user info after they terminate accounts
- PROCESS FOR RESPONDING TO 3RD PARTY REQUESTS FOR USER INFORMATION
  - ↳ Process for receiving & responding to non-judicial govt. requests
  - ↳ Explains its process for responding to court orders
  - ↳ Explains its process for responding to requests by pvt parties
  - ↳ Process for responding to requests from foreign govt.
  - ↳ Includes the legal basis of complying
  - ↳ Commits to carry out the due diligence on requests before responding
  - ↳ Commits to push back on unlawful requests
  - ↳ Provides guidance or examples on policy implementations
- USER NOTIFICATION ABOUT 3RD PARTY REQUESTS FOR INFORMATION
  - ↳ Commits to notify users when govt requests their user data
  - ↳ Commits to notify users when non-govt entities request user data
  - ↳ Discloses situations when it may not notify users
- INFORM & EDUCATE USERS ABOUT POTENTIAL THREATS
  - ↳ Commits to inform users about unusual account activity, most recent account activity, & possible unauthorised access
  - ↳ Publishes practical materials that educate users on how to protect themselves from cyber threats

APPENDIX

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

- DATA ABOUT 3RD PARTY REQUESTS FOR USER INFORMATION
  - ↳ Company breaks down the number of user data & real-time communications access demands it receives by country
  - ↳ Company lists the number of accounts affected
  - ↳ Lists whether a demand sought communications content or non-content
  - ↳ Identifies specific legal authority or type of legal process through which law enforcement and national security agencies demand access
  - ↳ Includes court requests for user data
  - ↳ Includes other non-govt requests
  - ↳ Includes number of requests it complied with, broken down by category of demand
  - ↳ Lists the type of govt requests it's prohibited by law from disclosing
  - ↳ Reports this data at least once a year
  - ↳ Data reported by the company can be exported as a structured data file

- SECURITY STANDARDS
  - ↳ Commits to keep up-to-date with the latest security standards & publishes evidence that it does so
  - ↳ Commits to address security vulnerabilitieswhen they are discovered & publishes info on how it does so
  - ↳ Discloses that it has systems in place to limit & monitor employee access to user information
  - ↳ Discloses the transmission of user communication is encrypted by default
  - ↳ Discloses that it deploys advanced authentication methods to prevent fraudulent access

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk