



DigitalRightsFoundation

Dissemination of Relief Packages and Welfare Activities during COVID-19

A research by Digital Rights Foundation



About

Digital Rights Foundation (DRF) is a Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation based in Pakistan working on digital freedoms since 2013. DRF envisions a place where all people, especially women and gender minorities, can exercise their right of expression without being threatened.

DRF believes that a free internet with access to information and impeccable privacy policies can create safe online spaces for not only women but the world at large.

Contact information:

info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

Acknowledgements

This report would not have been possible without the hard work of our research team comprising of ShehrBano Hassan and Zainab Durrani; and the revision and editing by the Head of Research and Policy, Shmyla Khan, the illustration by Mehak Tahir, the design work by Ahsan Zahid and Talha Umar and the support of Privacy International.

We are also grateful to all the individuals who agreed to address our queries and provided the valuable information that are a core element of this report.

Table Of Content

| | |
|--------------------------------------|----|
| Executive Summary | 01 |
| Main objectives | 02 |
| Key outcomes | 03 |
| Introduction | 04 |
| Methodology and Limitations | 06 |
| Literature Review | 07 |
| a. Personal data and data protection | |
| b. Data privacy and laws in Pakistan | |
| Findings and Discussion | 11 |
| a. Privacy policy: Telenor | |
| b. Privacy policy: EasyPaisa | |
| c. Zakat and Ushr Department | |
| Conclusion | 16 |
| Recommendations | 17 |
| Bibliography | 18 |

Executive Summary

This research was motivated by the desire to understand the ways in which, in light of COVID-19, relief dissemination efforts were conducted by telecommunication companies in collaboration with the Government of Pakistan. Moreover, it was aimed at understanding the role privacy plays in practice in such efforts, including perceptions of privacy as understood by telecommunication companies and the relevant department, as well as the privacy practices influenced by such ideas. As DRF has found in previous studies, telecommunication companies lack basic data protective mechanisms in Pakistan, made more concerning by the lack of awareness and understanding around privacy amongst the public. Coupled with weak legislative and institutional infrastructure of countries like Pakistan, it becomes particularly imperative to investigate whether appropriate checks and balances exist to ensure and protect the privacy of individuals. At the time of publishing this report, Pakistan does not have a specific data protection law, nor does it have any legislation allowing individuals the right to request data about themselves. The main governing legislation around crimes in the digital sphere is PECA (Prevention of Electronic Crimes Act 2016), which has come under severe criticism for its harsh penalties for speech acts and its potential for abuse and misuse. In fact, matters of data privacy and protection, particularly digital privacy, are relatively new areas of concern for the Pakistani government and society in general. This is further corroborated by the fact that health data privacy is a relatively under-studied subject in Pakistan, leading to a lack of implementation and understanding of its principles in practice. Considering this, the aim of this study is to unpack the ways in which privacy is understood and practiced in the health sector of Pakistan. In light of this, the aim of this study is to highlight the specific privacy perceptions and practices involved in COVID-relief funds dissemination and determine the effectiveness of privacy policies that dictate these projects. Moreover, we seek to identify the gaps in information and practice between the state, telecommunication companies, beneficiaries of relief funds and ordinary citizens of the state.

Objectives

- 01** Empower telecom customers by providing them with information and analysis on the extent to the privacy policies provided by cellular providers which are publicly available
- 02** Ensure that cellular telecoms users and relief beneficiaries in Pakistan are aware as to where their information goes and how that information is used
- 03** Assess the extent to which beneficiaries of COVID-relief have had their privacy protected and secured during the process of relief dissemination by telecommunication organizations

Key Outcomes

- 01** There are significant gaps in awareness and information regarding privacy within telecommunication companies and specific government departments
- 02** There is a lack of appropriate privacy policies and measures in place to protect citizen data, specifically vulnerable groups such as those receiving financial relief
- 03** Where privacy policies exist, they lack accessibility, robustness and implementation
- 04** The rapid digitalisation of finance and telecommunication technology has not strictly led to simultaneous consideration of privacy concerns, risks and harms in Punjab
- 05** Vulnerable groups' data is at risk of being exploited during relief dissemination and e-finance transactions, and their data being subjected to violations due to lack of privacy measures

Introduction

Our previous research on issues and the telecoms sector led us to the practice of the government using mobile cash transfer platforms for relief and welfare cash disbursements in Pakistan. Given the prevalence of mobile banking channels, they are being used to disseminate relief funds and on the beneficiary end, to collect relief funds via the e-banking platform known as EasyPaisa (translation: EasyMoney). EP became the 'official' e-wallet partner for the Zakat and Ushr department from 2016 till 2020 after winning out a tender bid. This prompted the question of what data protection controls are in place vis-à-vis citizens' data as governmental welfare programs are being channelled through privately-owned platforms, leading to an immense amount of data exchange and transfer

Easy Paisa, a platform launched by Telenor Pakistan in 2009, is a service of Telenor Microfinance Bank which is jointly owned by Telenor Group, one of the world's largest telecommunications companies across the Nordics and Asia with 186 million customers. In Pakistan, it is an e-wallet relying on branchless banking to provide easy access to funds. Though initiated as a money transfer service, it has grown to include a wider range of financial transactions, including international transfers. Easypaisa currently has more than eight million active users per month and 170,000 registered agents across the country, with over 25 million registered wallets. In 2020 alone, over 800 million transactions were executed through the Easypaisa platform amounting to around Rs1.5 trillion.¹

In April 2020, in the peak of the COVID pandemic, several media outlets in Pakistan reported on an agreement between Telenor Microfinance Bank's EasyPaisa and the Government of Pakistan's Zakat and Ushr Department, for the dissemination of funds to locals who have been impacted by the Coronavirus (COVID-19) outbreak and resulting economic slowdown due to a nationwide lockdown.² It was reported that the companies would disburse Zakat (Islamic charity) funds worth PKR 1.5 billion (appr. \$9.2 million) to over 170,000 eligible residents who were struggling to meet basic personal needs during the COVID pandemic, particularly low-income segments of society and daily wage earners. Disbursement of the funds was allegedly spread over 10 days to ensure social distancing measures. Beneficiaries across 36 districts of Punjab were able to receive funds from over 70,000 Easypaisa retailers.³ The use of mobile-based accounts through the mobile cash transfer EasyPaisa platform by the government for relief and welfare cash disbursements prompts the question of what data protection controls are in place around the citizens' data that is being accessed by the government via a private telecom company's platform.

When asked about the partnership, Punjab Minister for Zakat and Ushr told various news outlets:

“We are happy to be partnering with Easypaisa, one of the most reliable money transfer and digital banking services in the country. We believe that their widespread network and technology will allow us to disburse these funds in a hassle-free and safe manner”⁴

The emphasis on the safety of the process, given the context and legal history of data protection in Pakistan, begs the question of whether the dissemination of COVID-relief funds were actually done in a safe manner, particularly with regards to the data privacy of those individuals involved. Furthermore, given that relief funds are exclusively given to low-income groups, particularly those below the poverty-line, any privacy violations in this context would disproportionately impact individuals and groups from lower socio-economic backgrounds. To probe into this further, we have conducted desk research and interviews with both parties involved in this partnership.

Methodology

Though originally intended as a primary field research study involving qualitative data collection through surveys and interviews with both telecommunication companies involved in COVID relief dissemination as well as beneficiaries of this relief, it quickly became clear that this would not be possible due to the escalating emergency and public health concerns around COVID-19. This was compounded by the additional problems of accessibility of beneficiaries whose data was not traceable without cooperation from telecom companies and specific government departments involved in the partnership with telecom companies.

Lack of transparency and openness meant that both private and government stakeholders were not receptive to efforts to establish contacts by the research team. Our initial approach was to contact relevant telecom companies, Jazz (JazzCash), Telenor (EasyPaisha) and Ufone (UPaisha) to gather information regarding their policies around data protection and privacy involving relief packages and welfare cash disbursements. In addition, interviews with government officials (NADRA,, Social Welfare Department, Poverty Alleviation and Social Safety Division) were planned to qualify the use and sharing of personal data (such as CNIC numbers, DOB, names and addresses). However, DRF previously engaged in studies involving these institutions and found limited responsiveness, as was the case this year.

The lack of responsiveness meant that the research pivoted to one that was primarily conducted through extensive desk research on the privacy policies of related telecommunication companies and their partner government departments involved in the COVID relief dissemination. This was supported by two brief interviews with representatives of each institution.

Literature review

a. Personal data and data protection

Data protection often refers to sets of regulations and frameworks used to secure the privacy, availability, and integrity of data subjects. Data protection laws seek to protect people's data by providing individuals with rights over their data, imposing rules on the way in which companies and governments collect, use, process, store and share data, and establishing regulators to enforce these regulations.⁵ A data protection strategy is essential for any organization that collects, handles, or stores sensitive data. This means companies must ensure they are protecting their clients' personal data from data theft, data breaches and non-consensual third party sharing. These abuses can have significant consequences for both clients and organizations, thus laws around data protection seek to either prevent such harms from taking place or ensure that clients have points of redress in case personal data is abused.

Personal data is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name, phone number, biometric data or could include other identifiers such as an IP address or a cookie identifier, among other factors.⁶ Personal data becomes particularly vulnerable when considering the ways in which it can be shared with third parties, including corporations and government agencies. Such entities may require personal data in order to cater their services to meet public demands better, including improving their services or increasing their profits. In cases where this data is inaccessible, the leaking of personal data or stealing and selling becomes a lucrative business. 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. It is here that data protection safeguards become essential.

Data protection is not a new phenomenon. First conceptualized in the 1960s and 70s in response to a growing concern over the use of databases,⁷ it has now evolved to fit the complexities of the 21st century and more so, the growing salience of digital communications during COVID-19. Technology is now deeply tied to business models in almost all sectors of society, with companies relying on analytics and data sharing in order to improve their services and Artificial Intelligence (AI) being used to predict consumer behavior. Beyond companies, 'Big Data' has taken over other spheres of society such as healthcare and politics. In 2019, it was revealed that Cambridge Analytica was illegally harvesting data from millions of people through Facebook for political advertising (Davies: 2018). According to Raso et

al. (2018: 4), privacy is the single most impacted right by current AI implementation. AI systems rely on the collection and storage of vast amounts of personal data in order to make their outputs as fair and equal as possible. This means it requires a large quantity of potentially sensitive and personal data from people.

In healthcare, sensitive genetic material is obtained in order to diagnose people by comparing their symptoms with the thousands of reports through ‘diagnostic decision support systems’ (Raso et al. 2018: 33). While the success of such software is high, the risk of violating human rights is also alarming. Breaches to the genetic testing databases can cause mass violations of privacy rights and endanger people by giving access to their unique DNA, which can be used to access further personal information. As of this week, a breach like this has been reported to have occurred at Veritas Genetics (Brown, 2019), one of the largest DNA testing firms. This only goes to prove that state laws have to place stricter regulations and restrictions to ensure that the right to privacy is not endangered further. As Privacy International articulates: “the spaces and environments we inhabit and pass through generate and collect data from human behavior. The devices we wear and carry with us, installed in our homes, our channels of communications, sensors in our transport and our streets all generate more and more data.”⁸ It is no surprise that this data is valued like currency in today’s age. As such, this data is continuously at risk of being abused in many ways.

It is imperative to have data protection frameworks in place to ensure adequate safety of personal data and accountability for those who violate personal data. Data protection, though codified into law in many countries, remains weak. Those that exist often have their boundaries and are not updated quick enough in relation to the fast pace of technological advancements. However, these frameworks do provide an important starting point to ensure that the fundamental safeguards are implemented nationally and globally.

b. Data Privacy and Laws in Pakistan

Article 14 (1) of the Constitution of Pakistan affirms the “dignity of man, and subject to law, the privacy of home, shall be inviolable.” Article 8 of the Constitution contains provisions that 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.”⁹ This effectively means that citizens in Pakistan have a right to their privacy. However, much like many security-centric regimes, Article 8 contains clauses providing exemptions 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”. This underscores the fact that fundamental rights such as privacy are not absolute and can be circumvented under some circumstances.

We do however, note that efforts have been made to solidify data privacy regulations in Pakistan. In 2002, the Electronic Transactions Ordinance was passed to legitimize electronic versions of documentation, communications and transactions, thereby recognizing such technological advancements. However, section 43 2 (1) is the only section to address data protection, providing that “regulations may provide for” the “privacy and protection of data of subscribers” (1e).¹⁰ Similarly, the 2005 Electronic Data Protection Act was drafted to process “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 identity.”¹¹ However, in spite of being proposed, it was never updated.

In 2016 came the largest development in the arena of digital laws in Pakistan. The Government of Pakistan passed the Prevention of Electronic Crimes Act (PECA). The cybercrime law is broad and has faced significant criticism from the international community for its vague language that can be weaponized against human rights defenders online and innocent netizens.¹² The PECA has also been criticised for establishing provisions that mandate service providers and “authorised officers” hold traffic data for one year minimum. This effort to protect data is at best weak and at worst, dangerous. Much of this language is left to individual discretion and as evidence suggests, is used in ways that vary from mildly abusive to potentially life threatening to citizens. This oversight means that telecom service providers risk being penalised by the government for refusing to hand over data to them. This government interference is only substantiated further by Article 39, which allows governments to share data with other foreign international partners.¹³

At present, Pakistan has no specific law relating to data protection. However, in 2018, the Ministry of Information Technology and Telecommunication drafted the Pakistan Personal Data Protection Bill, with further revisions in 2020 and 2021. This bill is the most extensive piece of legislation, naming and establishing data privacy and security as a key concern in Pakistan. For instance, the bill explicitly recognises and provides for separate treatment of ‘sensitive personal data’ and ‘critical personal data’. ‘Biometric data’ is included within the definition of

'sensitive personal data'. With regards to data security, it specifies that data controllers must take "practical steps to protect personal data" when collecting or processing personal data including, among other factors, taking into consideration the nature of the personal data and the harm that would result from loss, misuse, modification, or unauthorized or accidental access, disclosure, alteration or destruction.¹⁴ Similarly, it states that data controllers may not disclose personal data without the consent of the data subject (1) for any purpose other than the purpose for which the personal data was disclosed at the time of collection or a purpose directly related to that purpose, or (2) to any third party not within the class of third parties provided within its notice. Though seeming extensive on paper, the bill contains vague language and open-to-interpretation time frames as its predecessors. Though it is yet to be accepted into law, there are already skepticisms regarding its effectiveness in tackling data privacy issues in Pakistan.

Findings

a. Privacy policies: Telenor

In 2017, Digital Rights Foundation conducted an assessment on the privacy policies of the main telecommunication platforms in Pakistan. The study found that privacy policies across the board were inconsistent, lacked adequate oversight and updates and were not readily available to the public. In particular, none of the telecommunication companies, including Mobilink, Telenor, Ufone, Warid or Zong had shown any consideration of the requirements of PECA and had not met privacy and customers' data protection standards.¹⁵ As EasyPaisha is a subsidiary initiative of Telenor, its privacy policy is of particular salience here.

Telenor Pakistan's privacy policy covers the form of data that is collected by the company, which includes data being used for marketing and research purposes, as well as to "provide a service to meet your needs." For instance, in its "Privacy Commitments" section, vague language is used stating "we will only process your personal information for legitimate purposes, and only for as long as it is necessary to achieve those purposes". There is no clear indication of what a "legitimate purpose" is nor is a concrete timeframe provided. Similarly:

*"Telenor Pakistan is legally bound to cooperate with and implement lawful directives/Authority Requests including such requests from Pakistan Telecommunication Authority, designated law enforcement agencies and other governmental functionaries as part of its license obligations as and when required."*¹⁶

This broad ranging clause does not specify the extent of third party sharing involved, nor the types of data that may be shared upon request. Moreover, as the assessment in 2017 showed, Telenor still does not specify whether the relevant policies for data sharing are for cellular use or website usage. The website states that it was updated in November 2021 though any major changes are not apparent immediately. In DRF's 2017 research report, Telenor Pakistan was given a verdict of "Concerning" and there is not enough evidence to upgrade that verdict. Attempts to get comments from Telenor and EasyPaisha in 2020 and 2021 were unsuccessful due to unresponsiveness from their representatives.

Representatives were contacted via email, with initial interest expressed from them. However, upon further probing, in the course of which a brief interview

was requested by the company requested by the company to clarify our request and ask additional questions, researchers were met with the same unresponsiveness. Despite initially agreeing to fulfill our request (including the disclosure of their internal policy around customers data retention), at the time of publishing this report, no further communication has come forward from Easy Paisa's end.

b. Privacy policy: Easy Paisa

Compared to its host organisation, EasyPaisa and Telenor Microfinance Bank have a much more transparent and extensive privacy policy in place. It emphasises the importance of individual user's right to privacy as well as the organisational commitment to "safeguarding the privacy of all customers"¹⁷. It makes note of specific laws, namely the Banking Companies Ordinance 1962 and the Microfinance Institutions Ordinance 2001 and is extensive in specifying the types of information it collects as well as the uses of said information. Finally, EasyPaisa's privacy policy explicitly highlights the types of technologies used to secure users' data, including passwords, encryption and physical security. However, the privacy policy was not easily accessible, with no visible links to it anywhere on their website. It was only through actively searching for it online that we were able to eventually locate it. For the average user, the presence of a privacy policy is not the only priority. Even when such policies exist, the lack of accessibility means users are still not aware of their rights.

Furthermore, the extensive nature of the information collected and its uses was alarming. Though they declared all forms of information, much of the information specified seemed extensive, particularly for a branchless banking experience. For instance, apart from CNIC, complete family information and email addresses, they also specify transactional information, computer browsing information, IP addresses as well as information about buying patterns and behaviours. This seems in direct conflict with the data minimization principle; which states that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. Though usually much of this information is collected for third party sharing, EasyPaisa states that it doesn't share with any third parties. This is particularly concerning because much of the consent being taken from users seems to be implicit. For instance, the privacy policy states:

“If you choose to provide us with personal information, you consent to the transfer and storage of that information on our servers located anywhere under the custody of Telenor Microfinance Bank or its authorized partners, vendor, supplier, service provider.”¹⁸

At other points, stipulations use vague language that is subject to interpretation. For example, though specifying in earlier sections that third party sharing will not occur, the privacy policy later states that they “may disclose personal information to respond to legal requirements, enforce our policies, respond to claims that a listing or other content violates the rights of others, or protect anyone’s rights, property, or safety.”¹⁹ Here, it is up to the organisation to determine what sharing falls under the enforcement of their policies and whether users consent to this sharing explicitly or implicitly. Another section states that the company “may combine your information with information we collect from other companies and use it to improve and personalize our services, content and advertising and to better understand your interests.”²⁰ Yet again, it is unclear what information is being taken and in what ways it will be combined with information from other companies. The implicit nature of the consent obtained is further reinforced with the clause stating that EasyPaisa may share information with “relevant third parties whom you consented service providers, dealers, agents or any other associate company for reasonable commercial purposes.”²¹

Finally, there is no set clause for special circumstances involving elevated use of electronic banking, such as COVID-19, which may potentially involve additional use of and reliance on information. Additionally, in particular interest to our investigation, there are no clauses indicating the collection, storage, use and sharing of data when the company goes into long-term partnerships with government departments, which is the case with its long standing partnership with the Government of Pakistan’s Zakat and Ushr department. Though a section in the privacy policy refers to the sharing of information when required for a verified investigation, there are no further details about additional partnerships and agreements between organisations.

Efforts to retrieve a clarification from EasyPaisa have been unsuccessful so far. At the time of writing this report, we are waiting for responses from their representatives.

c. Zakat and Ushr Department

The Zakat and Ushr department is part of a set of departments aimed at promoting and disbursing social welfare. Other departments within this division include Special Education & Women Empowerment Departments. The department is aimed at contributing towards poverty reduction through investing in the poor for their subsistence and rehabilitation.²² The Zakat & Ushr Department Punjab serves as Secretariat and administers the affairs relating to Zakat & Ushr in Punjab.²³ The Secretary of Zakat & Ushr who is the in-charge of the department, performs the functions of Chief Administrator Zakat in the province. Programs of the Zakat and Ushr programs include the Guzara Allowance scheme and Educational stipends for students.²⁴

There is no greater proof of the lack of awareness and transparency around data privacy than the fact that Government Ministries and departments in Pakistan do not have a privacy policy, a practice which is particularly important in the absence of a data protection law in the country. In order to explore the privacy perceptions and practices taken up by the department, we interviewed two personnel at the Zakat and Ushr department in Lahore by contacting them via direct telephone calls on the number available on the Zakat and Ushr Department's website. Though brief, responses suggested that there was no specific privacy policy to which personnel or beneficiaries of relief could be directed. Beneficiaries of COVID-relief were selected from the existing databases involving the dispersion of Zakat funds since 2016. Approximately 9000-12000 Pakistani rupees were given each to an individual representing one family, across 36 districts in the Punjab province. Information collected from beneficiaries included names, contact details, CNIC numbers, their local committee code, their local chairman's phone number, local clerk's number as well as the istehqaq number - a number issued upon receipt of relief funds - for every beneficiary. When probed about the chain of custody of data, department personnel described a long line of responsibility starting from the local Zakat committee (composed of 10 individuals elected by members of the community), district committee, to field officers working on the dispersal of funds. There was no specification about how many people in total have access to the information of beneficiaries. However, we can determine that the databases from which their details are taken are also not dictated by any privacy policies and are accessible to the Zakat dispersal team. Moreover, there was no specification on whether the data is reserved for provincial departmental sharing or whether data is accessible on multiple levels of government, from district, provincial and federal.

With regards to external sharing, personnel did not elaborate on how lists of beneficiaries and their details were shared with telenor and how that data transfer occurs. It is assumed that once data is transferred to the Telenor system, their privacy policy covers it. However, there was no confirmation of this either.

When asked about the storage of data, department personnel stated that data was stored both digitally and physically in the office, but kept securely. They did not elaborate on the ways in which the security was ensured. Moreover, there was no limit to how long data of beneficiaries would be stored. However, they did allude to an ongoing partnership with the Punjab Information Technology Board (PITB) to create a cross-departmental and cross-organisational database. Though this has not yet come to fruition, it is worth noting that this would have severe consequences for privacy practices, particularly with regards to data access and sharing.

Conclusion

This initial and brief investigation finds the vulnerable nature of privacy of Pakistani citizens, marked by fragile privacy practices and lack of clarity and transparency in privacy policies of all parties involved in the COVID-19 relief funds dissemination. Telenor's privacy policy remains concerning. EasyPaisa's privacy policy, though slightly more extensive, is brief and vaguely worded, leaving much to interpretation and contradicting its third-party sharing stance at several points. Furthermore, the consent of users is often implied rather than explicitly stated. Similarly, the Zakat and Ushr departments remain weak in the area of data privacy, with more of a focus on efficiency than safety and security of those involved. Without the appropriate emphasis on privacy and data protection, already vulnerable data of vulnerable users is at constant risk of abuse. Telecommunication companies, the government and civil society organisations must work together to ensure better privacy policies, legal frameworks to protect data and strict accountability for those who abuse and violate personal data.

Recommendations

The presence of a robust and extensive privacy policy is necessary for all telecommunication companies and departments dealing with sensitive data of citizens. These privacy policies must acknowledge the implications of data harms and the consequences of the abuse of such violations. Beyond privacy policies, accountability and transparency mechanisms must be developed to ensure that data breaches are appropriately handled and proactively deterred. Moreover, the accessibility of such privacy policies is as important as their very existence. Therefore, institutions must ensure they place an active role in ensuring that individuals are aware of the existence of the privacy policies that apply to them and their rights within them. This should be done by establishing a strong chain of communication between each sector or department, down to the customer or beneficiaries. Moreover, communication must be maintained between governing bodies such as the Government of Pakistan and Telenor Group and their subsidiaries. Moreover, the state must take steps to engage in raising awareness and dispelling misconceptions around privacy amongst citizens so that they remain protected and secure in an ever digitalising world.

Bibliography

1. <https://www.dawn.com/news/1640132/easypaisa-aims-to-increase-number-of-active-users>
2. <https://www.crowdfundinsider.com/2020/04/160384-covid-19-relief-pakistans-digital-payments-firm-easypaisa-to-help-government-organizations-distribute-funds-following-coronavirus-outbreak/>
3. <https://nation.com.pk/08-Apr-2020/easypaisa-collaborates-with-zakat-and-usshr-department-to-disburse-rs1-5b>
4. <https://nation.com.pk/08-Apr-2020/easypaisa-collaborates-with-zakat-and-usshr-department-to-disburse-rs1-5b>
5. <https://privacyinternational.org/learn/data-protection>
6. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>
7. Atten, Michel, et Elizabeth Libbrecht. "What Databases Do to Privacy. The Emergence of a Public Issue in 1960s America", *Réseaux*, vol. 178-179, no. 2-3, 2013, pp. 21-53.
8. <https://privacyinternational.org/learn/data-protection>
9. 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/>>.
10. *ibid*
11. <https://www.unescap.org/sites/default/files/Electronic%20Data%20Protection%20and%20Safety%20Act%202005.pdf>
12. <https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane>

13. 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>
14. <https://www.huntonprivacyblog.com/2020/05/14/pakistan-introduces-new-draft-of-personal-data-protection-bill/>
15. <https://www.dawn.com/news/1305503>
16. <https://www.telenor.com.pk/privacy-notice/>
17. <https://easypaisa.com.pk/privacy-policy/#:~:text=We%20don't%20sell%20or,to%20better%20understand%20your%20interests.>
18. Ibid
19. Ibid
20. Ibid
21. Ibid
22. https://zakat.punjab.gov.pk/about_us
23. Ibid
24. <https://zakat.punjab.gov.pk/programs>



DigitalRightsFoundation