POLICY BRIEF, JANUARY 2024

Data Privacy Protection by Consumer Laws in Pakistan

MUHAMMAD SHAHZEB USMAN

IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

NETT National Economic Think Tank

Chair, International Law

About the Author

Muhammad Shahzeb Usman completed his Bachelor of Laws (BA-LL.B.) from the Lahore University of Management Sciences (LUMS) in 2021. He graduated with the degree of Master of Laws (LL.M.) in 2022 from the University of Nottingham, United Kingdom where he studied as the Developing Solutions Scholar. In 2019, he completed the International Course on Global Refugee Crisis on Merit Scholarship at *Koc* University, Istanbul, Turkey. In 2018, he also completed an International Course on Politics in South – East Asia at UNMC, Kuala Lumpur, Malaysia. He is currently working as a Legal Researcher in the Department of International Law at the Islamabad Policy Research Institute (IPRI). His areas of interest include analysing the impact of International Financial Institutions (IFIs) from TWAIL perspective, International Human Rights Laws, Economic Rights, Labour Laws, Tax Laws, Competition Laws, and Refugee Laws.

About IPRI

The Islamabad Policy Research Institute (IPRI) is one of the oldest non-partisan think tanks on all facets of National Security, including international relations and international law, strategic studies, governance, public policy, and economic security in Pakistan. IPRI exemplifies two decades of rigorous and timely analysis of crucial strategic agendas and inter-governmental processes that influence national and regional policy community. Recognized for its objectivity and policy relevance, IPRI's publications offer current, up-to-date, and high-quality research in the form of authoritative journals, books, monographs, and policy briefs. The Institute's events vary from seminars on current international and national affairs to large-scale international conferences that attract renowned leaders, academics, and policymakers from all over the world. The Institute also house two specialized Chairs for International Law and Economic Security.

Table of Contents

Abstract

Many digital platforms exploit their consumers by using such deceitful tactics to extract data which they further use to assert market dominance. They use this dominance to extract mire data much more effectively and sub-consciously. Consumer protection and data protection laws are interlinked in the digital sphere as the price of digital consuming is itself data. As opposed to competition law, consumer data protection laws could be used to target any processor regardless of its magnitude.

Key Words: Data Protection, Consumer Protection, Pricing, ICCPR

Executive Summary

Issue

The start of 21st century brought an unprecedented proliferation of digital platforms. Initially, these platforms were welcomed as an efficient vehicle of access to global mass information. However, continued use of these platforms revealed that they have almost an invincible ability to invade human privacy. This brief shall attempt to divulge into the legal designs under which Pakistani consumer and data protection regulations should be crafted so that any invasion of privacy could be deterred. For this purpose, this brief shall initially establish that Pakistani State is bound to protect the right to privacy. The brief shall further explore the complex digital manipulations which could be employed to extract data. This elucidation shall pave way for the understanding of Pakistani legislations' inability to prevent frequent violations of the right to privacy. This brief shall end with proposing following solutions in light of international best practices.

Recommendations

- Creation of a separate legislation named as Consumers and Citizens Data Privacy Act
- Development of informational self – determination within that legislation
- Clear definitions of consumer and commercial practices within that legislation
- Development of specific criteria for the processing of data with timelines for data erasure

I) Introduction

Pakistan is a signatory of International Covenant of Civil and Political Rights (the "ICCPR") and also ratified it in 2017.[1] ICCPR states that no one shall be interfered in an arbitrary or unlawful manner in relation to her privacy.[2] United Nations elaborated ICCPR to impose a positive and negative duty on the states to preserve the right to privacy. Therefore, positive duty of the states requires them to make a legislative framework to protect privacy of citizens from private parties with full awareness of all the manifestation through which it could be breached. Similarly, the negative duty requires the states not to breach the right to privacy.[3]

Article 14 of Pakistani Constitution also states that dignity of man and privacy of home must be respected. Any breach of privacy, thus, can incidentally impair a person`s dignity. Therefore, Supreme Court of Pakistan has also observed privacy as one of the rights which the state must upheld.[4]

II) Non Existence of Zero Pricing

In order to understand the craft of the proposed solution in the end of brief, a perusal of the manipulative behaviour employed by the digital companies is necessary. Digital companies usually leave the user in a situation which is similar to choosing between 'the devil and the deep sea'. As a result, a majority of the users even if they understand the need to protect their privacy agree to the terms and conditions of various platforms. This manipulation occurs *inter alia* due to the fact that need of digital platforms like Facebook has almost become a necessity due to the 'network effects' and user must take it on their conditions or 'suffer'.

Digital platforms also usually employ the use of heuristics and reinforce them with their ability to understand consumer`s biases as they extracted their data in past.

---

[1] Khan AN, "Privacy - A Missing Fundamental Right in Pakistan" *The News* (October 21, 2018) <https://www.thenews.com.pk/print/383470-privacy-a-missing-fundamental-right-in-pakistan> accessed November 10, 2020

[2] International Covenant of Civil and Politics Rights, Article 17.

[3] United Nations High Commissioner for Refugees, "CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation" (*Refworld* April 8, 1988) <https://www.refworld.org/docid/453883f922.html> accessed November 8, 2020

[4] *Khawaja Salman Rafique V* NAB [2020] SCP *130*

They can manipulate human psychology by pushing the consumer to the easier option of not reading terms and conditions while fully being aware of the consumer`s inability to understand implications of such terms and condition without legal counsel. This situation is further worsened by creating a 'cloudy situation' in which a user simply does not know the extent of the use and processing of their data.

Many digital platforms exploit their consumers by using such deceitful tactics to extract data which they further use to assert market dominance. They use this dominance to extract mire data much more effectively and sub-consciously. All of this happens without ever giving an explicit option to a consumer to give money instead of data. Thus, this chimera of 'zero pricing' which they present is generally false.[5]

III) The Consumer Protection and Date Protection Link

Consumer protection and data protection laws are interlinked in the digital sphere as the price of digital consuming is itself data. As opposed to competition law, consumer data protection laws could be used to target any processor regardless of its magnitude.

Similarly, breach of consumer and data laws is also comparatively easier to prove due to their individualistic nature as compared to proving abuse of market power in competition law. Thus, a 'continuing limiting deterrent' is created on companies. An example of this premise could be observed in Italy`s imposition of hefty fine under consumer protections laws on Facebook as Facebook *inter alia* falsely claimed that they provided zero pricing.[6] On the other hand, Germany was able to only investigate Facebook on collection of data from third party websites using Facebook Application Interface because it employed competition law for investigation.[7]

[5] Marco Botta KW, "The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey* - Marco Botta, Klaus Wiedemann, 2019" (*SAGE Journals* July 25, 2019) <https://journals.sagepub.com/doi/full/10.1177/0003603X19863590> accessed November 20, 2023

[6] Hern A, "Italian Regulator Fines Facebook £8.9m for Misleading Users" (*The Guardian* December 7, 2018) <https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users> accessed November 20, 2023

[7] Satariano A, "Facebook Loses Antitrust Decision in Germany Over Data Collection" (*The New York Times* June 23, 2020) <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html> accessed November 20, 2023

Moreover, it is also necessary to examine data and consumer protection laws jointly as data manipulation and leak happens both on the part of public companies, private companies and government agencies. Thus, a 'citizen' and a 'consumer' are both simultaneously or in any isolated way subject to violation from the right to privacy. An important illustration of a public entity's disregard to protect privacy can be observed when British GCHQ`s hacked Pakistan Internet Exchange in 2015.[8] Similarly, Careem`s data breach of 2018 reflects violation of consumer privacy on part of a private company as well.[9]

IV) Inadequacy in Consumer Protection Acts

For the purposes of this brief, the Punjab Consumer Protection Act 2005 (the "PCPA") shall be considered as a template for analysis. The first inadequacy in this legislation in relation to digital privacy is in relation to its ambit. PCPA does not include e-consumers in the definition of consumers and neither attempts to define them. The definition of consideration for buying services or a product is also left for judicial interpretation. This is important as digital platforms can be free. Therefore, data should also be a 'consideration'. [10] Definition of damage only includes economic loss but excludes any loss in terms of privacy through data.[11] Similarly, digital services are not included in services although definition of services do list engineering, medical and legal services.[12] PCPA also does not attempt to define digital platforms and fails to classify it within goods or services.[13]

Another avenue on which PCPA fails in regards to privacy is in its failure to include any injunction to protect unauthorized or malicious use of data from the company itself or third-party. It does provide provisions which forbid manufacturers from deviations in stated specifications; forbid them from using a model which could be substituted with another model that would have averted foreseeable damage and

[8] (2018) Report <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/DigitalRightsFoundation.pdf> accessed November 20, 2023
[9] Dawn.com, "Careem Users' Personal Data Compromised in Massive Data Breach" (*DAWN.COM* April 23, 2018) <https://www.dawn.com/news/1403401> accessed November 20, 2023
[10] Punjab Consumer Protection Act 2005 s 2(c)
[11] Punjab Consumer Protection Act 2005 s. 2(d)
[12] Punjab Consumer Protection Act 2005 s. 2(k)
[13] Punjab Consumer Protection Act 2005 s. 2(j); 2(k)

make manufacturers specifically use a warning when it should have been given.[14] However, a common element in these sections is an absence of any explicit use of digital platforms although the aforementioned sections have special relevancy to digital platforms as they are mostly in breach of these provisions. This inadequacy in PCPA is further intensified when PCPA restricts the criteria of 'defective products' to the violations of aforementioned stipulations. Thus, it provides an exhaustive list leaving no room for 'privacy breach as a design' to make a digital platform declared as defective.

Furthermore, PCPA potentially legitimized a common defence for digital platforms as the legislation does not declare a product defective even if no warning is given provided a dangerous consequence is easily foreseeable.[15] This leaves room for digital platforms to argue that leaving digital footprint and company`s use of it is easily foreseeable and they are not required to provide warning. Similarly, PCPA further allows digital platforms to use a broad defence i.e. an 'alternative design which could have protected consumer privacy was not feasible and thus it was not used'.[16] This clause could allow digital platforms to again exploit 'zero pricing' as a justification for extracting data through different means.

Moreover, PCPA uses the word 'proximate damage' for imposing a liability for delivering defective services but fails to indicate that loss of privacy in itself and any incidental physical or emotional hurt must also be within its ambit.[17] Similarly, while listing a range of misleading representations and advertisements as unfair practices, PCPA fails to list statements such as 'a product or service is free' as unfair.[18] PCPA also does not explicitly declare any representation and advertisement as unfair which deliberately tries to use heuristics; exploit bounded rationality of humans or exploit any of their biases to extract consent for data processing. Declaring such representation as unfair is essential as it would cut the root which allows violation of consumer privacy.

[14] Punjab Consumer Protection Act 2005 s 4; s.5; s.6; s.7; s.8; s.9
[15] Punjab Consumer Protection Act 2005 s 7(1)(a)
[16] Punjab Consumer Protection Act 2005 s 9(1)(c)
[17] Punjab Consumer Protection Act 2005 s 13
[18] Punjab Consumer Protection Act 2005 S 21; S 22

V) Inadequacy in Electronic Crimes Act

Prevention of Electronic Crimes Act 2016 (the "PECA") further mandates mass retention of traffic data by service providers for a minimum of one year. This data can also be accessed by the Pakistan Telecommunication Authority ("PTA").[19] The practice of retention of data for a long period by service providers was noted in the UK High Court which declared this practice against the right to privacy.[20] PECA also allows an authorized officer to search or seize data and disclose data respectively for criminal investigation.[21] This is extremely vague as it is very difficult to decipher the criteria of a 'criminal conduct'.

Furthermore, the definition of 'act' has been defined under the statute as 'a series of action' without elaborating or qualifying this critical word.[22] Prevention of Online Harm Rules 2020 (the "POHR"), drafted under the auspices of PECA, go one step further in invading the privacy of the consumer as it allows an investigation agency to require from a social media company any information, content or data.[23] This is extremely troubling as this request from the social media company is not even dependent on any judicial process as opposed to PECA. In addition, POHR also require to provide information in "decrypted, readable and comprehensible format" which violates the privacy rights of citizens under international law.[24]

VI) Recommendations

1. In light of the aforementioned guidelines and under the guidance of best practices of EU General Data Protection Regulations 2018 and US Privacy Act

[19] Pakistan Electronic Crimes Act 2016 S 29
[20] Marlow J, "DRIPA Struck Down by High Court in Judicial Review Challenge" (*www.hoganlovells.com*July 24, 2015) <https://www.hoganlovells.com/en/blogs/focus-on-regulation/dripa-struck-down-by-high-court-in-judicial-review-challenge> accessed November 9, 2023
[21] Pakistan Electronic Crimes Act S 33; S 34; (2017) rep <https://privacyinternational.org/sites/default/files/2017-11/UPR28_Pakistan.pdf> accessed November 9, 2023
[22] Khan EA, "The Prevention of Electronic Crimes Act 2016: An Analysis" LUMS Law Journal Volume 5 <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis> accessed November 9, 2023
[23] Prevention of Online Harm Rules 2020 Rule 6
[24] David Kaye, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (*A.HRC.29.32_AEV.doc*May 22, 2015) <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/_layouts/15/WopiFrame.aspx?sourcedoc=%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession29%2FDocuments%2FA.HRC.29.32_AEV.doc> accessed November 10, 2020; 2017) ; Report <https://privacyinternational.org/sites/default/files/2017-11/UPR28_Pakistan.pdf> accessed November 9, 2023

of 1974, Pakistan needs to implement a Consumers` and Citizens` Data Privacy Act (the "CCDPA"). It shall define a commercial practice as unfair *inter alia* if it is against the requirements of professional diligence; materially distorts or is likely to materially distort the economic behaviour in relation to the average consumer and when it is simply misleading.[25] Furthermore, 'consumer' must be defined in negative terms but e-consumer should be mentioned specifically.[26] This shall include everyone as consumer who is a natural person and is acting outside of his commercial or professional activities.[27]

2. Pakistan also needs to develop the policy of 'informational self-determination' in CCDPA.[28] The policy shall require affirmative consent for the processing and submission of data from consumer or data subject. This consent shall be defined to be freely given in a specific, informed and unambiguous manner with full awareness of the fate of data and extent of its processing.[29] Moreover, this consent should be specified with a high standard when it is approving sensitive information such as medical records.[30] There must also be an option to withdraw consent at any time and altogether erasure of whole data in CCDPA.[31]
3. CCDPA can ensure privacy of consumers and citizens by adopting an exhaustive six lawful basis for processing of data in CCDPA which includes consent; contract; legal obligations; vital interests such as life and health; public tasks and legitimate interests of the company which must not override the interests of the Charter of Fundamental Rights.[32] Moreover, processing of personal data must also be required to be lawful, fair and transparent. These phrases should be interpreted in CCDPA to encompass the requirement of minimum time limitation for data storage; information related to data be accessible, easy and encompassing all facets; data minimization; data review; data erasure after 90 days except specific data which government request to

[25] EU Unfair Consumer Directive 2005 Article 5(2)
[26] "Consumer Protection in EU" (*europarl.europa* September 2015) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf> accessed November 10, 2023
[27] Kingisepp M, "The Notion of Consumer in EU Consumer Acquis and the Consumer Rights Directive-a Significant Change of Paradigm?" (*Juridica International*) <https://www.juridicainternational.eu/?id=14841> accessed November 10, 2023
[28] Schastlivtseva Pby Y, "Yuliia Schastlivtseva" (*Legal Dialogue* July 3, 2018) <https://legal-dialogue.org/informational-self-determination-of-europe-and-its-importance> accessed November 10, 2023

[29] EU General Data protection Regulation 2018 Art. 4(11)
[30] EU General Data protection Regulation 2018 Art. 9
[31] EU General Data protection Regulation 2018 Art. 7(3); Art.17
[32] EU General Data protection Regulation 2018 Article 6(1)

retain; data accessibility; data rectification and clear, specific purpose for collection and data accuracy.[33]

4. In order to protect data subjects as consumers or citizens, CCDPA must include all companies, institutions, and government agencies to be held liable if they process data on individuals residing in Pakistan.[34] Therefore, a narrowly tailored test of 'extremely relevant and necessary' must be present in CCDPA to access, seize or retain data.[35] Similarly, for government officials, the same test should be applied to access or seize data trumping all other tests. This test must be assessed by a court in a relevant situation before allowing any search or seizure. Moreover, all controllers or processors of data must implement encryption while choosing from a range of methods so as to give them space to respect the principle of 'privacy by design' and develop sound security features.[36] CCDPA must also fine per violation with apparent no cap so big companies which control numerous amounts of capital are deterred while also allowing a fine on non-compliance instead of data breach.[37]
5. Lastly, it must be noted that CCDPA does provide a broad mechanism which shall address most deficiencies mentioned in PCPA and PECA but it could be enacted *pari materia* to PCPA and PECA even if the pointed deficiencies are not removed. This shall further reinforce right to privacy providing the benefit of both legislations. However, there should be an overriding clause which prioritize CCDPA provisions in comparison to any other legislation.

[33] EU General Data protection Regulation 2018 Article 5; Recital 39, Article 16, Article 5(1)(c)

[34] Kawamoto D, "Will GDPR Rules Impact States and Localities?" (*Government Technology State & Local Articles - e. Republic*) <https://www.govtech.com/data/Will-GDPR-Rules-Impact-States-and-Localities.html> accessed November 10, 2023

[35] Green A, "Complete Guide to Privacy Laws in the US: Varonis" (*Inside Out Security* March 30, 2020) <https://www.varonis.com/blog/us-privacy-laws/> accessed November 10, 2023

[36] "Art. 25 GDPR – Data Protection by Design and by Default" (*General Data Protection Regulation (GDPR)*March 28, 2018) <https://gdpr-info.eu/art-25-gdpr/> accessed November 10, 2023

[37] Felding J, "Four Differences between the GDPR and the CCPA" (*Help Net Security* February 3, 2019) <https://www.helpnetsecurity.com/2019/02/04/gdpr-ccpa-differences/> accessed November 10, 2023