Response dated 31 January 2021 to the Report by the Committee of Experts on Non-Personal Data Governance Framework released by the Ministry of Electronics and Information Technology in December 2020

Dvara Research[1] is an independent Indian not-for-profit research institution guided by our mission of ensuring that every individual and every enterprise has complete access to financial services. Our work seeks to address challenges for policy and regulation in India given the waves of digital innovation sweeping financial services, focussing on the impact on lower income individuals in the country. The regulation and protection of data has been a core area of our recent research.

In this document we present our response to the revised Report by the Committee of Experts on Non-Personal Data Governance Framework (the **Framework**) released by the Ministry of Electronics and Information Technology (MeitY) in December 2020. Our analyses suggest that the Framework is built with a disproportionate emphasis on the economic value to be realised by the sharing of Non-personal Data (NPD) and a narrow appreciation of the social and welfare-based merits and demerits of sharing privately held NPD. This emphasis on narrowly defined economic benefits risks creating an ecosystem that is not able to fully tap into the social benefits of sharing NPD, and has weak safeguards for consumer protection. Consequently, our response is organised into three sections:

1. **Section I** provides an analysis of the goals of the Framework, as set out in section 3.5, and offers recommendations for creating more equitable, inclusive, and ethical overarching principles for data sharing,
2. **Section II** examines the design of the institutions proposed to enable the sharing of NPD and offers recommendations for strengthening their institutional design,
3. **Section III** highlights the gaps in consumer protection and offers recommendations for addressing them.

This response continues our engagement with the public consultation process with the Framework.[2] We are concerned that, contrary to its objectives, the Framework would be unable to create benefits and ensure safety for communities, and may be inadequate to democratise the rights over NPD.

We welcome the opportunity to assist the Committee in developing the Framework further by responding to questions and comments, or by offering research assistance on the topic.

[1] Dvara Research has made several contributions to the Indian financial system and participated in engagements with many key regulators and the Government of India. Through our recent work we have extended research inputs to bodies including the Committee of Experts on Data Protection under the Chairmanship of Justice B.N. Srikrishna, the Ministry of Electronics & Information Technology (MeitY) and the RBI's Committee on Deepening of Digital Payments. Our primary research on Indians' data sharing attitudes was cited in the 2017 White Paper of the Expert Committee on Data Protection under the Chairmanship of Justice B.N. Srikrishna. Our regulatory proposals on enforcement and the design of the Data Protection Authority (DPA) were specifically acknowledged and relied upon in the Final Report of the Committee dated 27 July 2018.

[2] Our response to the Report of the Committee of Experts on Non-Personal Data Governance Framework released by MeitY in July 2020 can be accessed here.

Table of Contents

Section I: Analysis of the Goals of the Framework

Section 3.5 of the Framework presents two sets of goals that are sought to be achieved by the proposed regulation/ legislative policy (pp. 5-6). The first set of goals focuses on creating an enforcing framework that establishes the rights of communities over NPD, and protecting them from harms arising from the re-identification and misuse of NPD. The second set of goals are intended to unlock economic value from NPD for the benefit of Indians and create a data sharing framework that enjoys regulatory certainty.

An analysis of literature on the socio-economic implications of sharing privately held NPD and the objectives of other comparable frameworks suggests that **the rationale for some of these goals are unclear. They do not take into consideration the complete economic and social merits and demerits of sharing privately held NPD.**

i. ***The rationale for sharing privately held NPD widely is unclear:*** Section 3.5(ii) sets out the goal of creating a data sharing framework. However, the Report does not outline principles that justify widely sharing privately held NPD for the purposes of public interest.

In the field of data governance, there are well-established principles for opening publicly collected NPD for the benefit of all. As set out in the Data Sharing Principles for Developing Countries publicly collected NPD is highly non-excludable (CODATA-PASTD, 2015; The Nairobi Data Sharing Principles). Since all tax-payers contribute to the collection of that data, it is impossible to exclude anyone from it. This high degree of non-excludability, coupled with data's inherent non-rivalrous nature, justifies widely sharing publicly collected NPD. This is also the rationale behind the National Data Sharing and Accessibility Policy (NDSAP), which is designed to make non-sensitive data available for legitimate and registered use, *"given the deployment of substantial level of investment of public funds in collection of data and the untapped potentials of benefits to society..."* (Ministry of Science and Technology, 2012). However, it is unclear if a similar rationale exists for sharing privately held NPD - considering they are collected as part of private activities and are excludable.

ii. ***The goals do not account for the welfare costs of sharing privately held NPD:*** Section 3.5 (ii) pursues the goal of "*unlocking economic benefit from non-personal data for India and its people*". However, neither this specific goal nor the Framework in general considers the potential welfare loss of widely sharing privately held NPD.

Though data-sharing is generally welfare enhancing, it also raises certain concerns. These include concerns regarding privacy, collusion among providers due to the exposure of strategically important information about the market, and the imposition of other costs on the economy such as disincentivising collection of data altogether (Graef, Tombal, & Streel, 2019).

The European Union, for instance issued "*Horizontal Agreements Guidelines*" which examine whether there are any negative implications to the sharing of information among competitors (European Commission, 2011). Factors that can cause the exchange of information among competitors to restrict competition include *"the strategic nature of the information, the market coverage of the firms involved […], the age of the data, the frequency of the information exchange, the public or non-public nature of the information… etc."* (Graef, Tombal, & Streel, 2019).

Recently, the case of Insurance Ireland brought out the potential welfare losses that can accrue due to data pooling among competitors. Insurance Ireland is an association of motor insurance providers in Ireland that administers a database where member companies contribute insurance claims data on an ongoing basis. The objective of the system is "*to facilitate the detection of potentially fraudulent behaviour by insurance claimants and to ensure the accuracy of information provided by potential customers to insurance companies and/or their agents*" (European Commission, 2019). The European Commission is currently reviewing if the creation of this database and its controlled access impose a competitive disadvantage to non-member insurance providers, and restrict the choices of insurance products available to Irish drivers. While reviewing this case, the European Commission has also raised a more fundamental question on whether "***Data pooling reveals the market strategies of players and adversely affects competition in the market***" (European Commission, 2019)**.**

The Framework does restrict the sharing of trade secrets or intellectual property of businesses. However, it does not consider if the sharing of NPD could result in the strategies of competitors being revealed, or if it will help companies collude amongst themselves, to the detriment of the consumer. Without accounting for these welfare losses or placing reasonable fetters to prevent them from occurring, the Framework seems to take an incomplete view of the economic benefits of sharing privately held NPD.

iii. ***The Framework places a disproportionate emphasis on unlocking economic benefits:*** The Framework seems to consider realising economic gains from NPD as its chief objective. However, there is growing appreciation that the collection, sharing and use of NPD in public interest must give due consideration to ethical concerns, human rights and implications on minority groups (European Commission, 2020).

The case of one of the largest networks for the sharing of citizens' data — the Eurocities — may provide an example of the goals that can be set when data is shared for public interest. The Eurocities is a network of 190 cities in 39 countries which uses citizens' data to improve the condition of European cities (EuroCities, n.a.). It sets out six goals for itself, which include the two distinct goals of ***creating inclusive cities*** and ***creating prosperous cities***. In addition to identifying inclusion as a goal for its work, the network is also sensitive to the disparate impact that data collection and analyses can have on different groups. Therefore, it also identifies the ***principle of ethical and social responsibility***, where it recognises that "*collecting and combining data may result in unforeseen insights on society or individuals".* As such**,** it requires entities that are involved in the collection of data to adjust their practices so as to *"prevent all forms of discrimination based on, for example, gender, age, socio-economic status, ideology, race or religious beliefs"* (Mejia, 2019).

In comparison, the Framework's conceptualisation of the goal of unlocking economic value appears very narrow. Under the proposed Framework, Data Requesters would approach Data Trustees requesting access to HVDs that they can use to create benefits. The underlying assumption for this Framework appears to be that Data Requesters and Data Trustees would mutually benefit from the value of an HVD. However, this assumption is questionable considering how data only has perceived value. Data only has value that is perceived by entities who would find the data useful (Agarwal, 2020). Data which is not deemed useful by entities is unlikely to have any value by itself (Benjamin, Bhuvaneswari, & Rajan, 2007; Economic Commission for Latin America and the Caribbean, 2013; OECD, 2018; Wright, Prakash, Abraham, & Shah, n.a.). Under the Framework, it is likely that Data Requesters would approach only those Data Trustees with HVDs that they perceive to be valuable. As a result, communities whose data has no perceived value are unlikely to benefit from the Framework. For instance, low-technology communities that produce low amounts of data or low-value data could find themselves outside the scope of Data Requesters who find their data to be of little value. Communities that currently generate more data are therefore likely to benefit the most, widening the digital divide further (Agarwal, 2020; UNCTAD, 2019).

More broadly, social perceptions and structural discrimination faced by various communities could also ostracise these communities from drawing equal benefits from this Framework (Competition Commission of India, 2020; World Economic Forum, 2019). For instance, although women might generate high amounts of NPD in a city, the women community might receive fewer benefits unless products and services are specifically crafted with a gendered lens. Therefore, the focus on unlocking economic value may lead to unequitable outcomes and reinforce existing socioeconomic inequalities.

It may be worthwhile to reiterate this goal and focus on unlocking economic benefits with a view to being more inclusive. Similar criteria also exist with respect to other digital applications, which can be used as a guideline. For instance, the United Nations has issued the FATEN Principles for Artificial Intelligence. These principles stress on the objectives of Fairness, preserving Autonomy and Accountability, Trust and Transparency, Equality and beneficence and Non-maleficence in the use of AI (United Nations Sustainable Development Group, 2017).

Recommendations for principles using privately held NPD for public interest uses

The European Union’s High-Level Expert Group on Business-to-Government (B2G) Data Sharing recommends drawing inspiration from certain principles when devising an ethical framework for B2G data sharing (European Commission, 2020). These principles are set out in Box 1.

Box 1:Proposals for ethical principles for B2G data sharing frameworks, High-Level Expert Group on B2G Data Sharing, EU.

FATEN: Ethical principles

Fairness: B2G data-sharing frameworks might need to address potential biases in the data or provide information about such biases to the public-sector bodies. Given that B2G data sharing impacts several areas such as health, climate change or transport, a constructive exchange of resources and knowledge between the private, public and social sectors should be encouraged.

Accountability and autonomy: There should be clear accountability regarding the consequences of decisions taken and actions implemented because of B2G data-sharing. Human autonomy should never be violated through the use of data.

Trust and transparency: Generally, trust emerges when three conditions are met: (1) competence regarding the specific task that the trust will be placed onto; (2) reliability, that is, sustained competence over time; and (3) honesty and transparency.

Equality and beneficence: Any B2G data-sharing project should aim to have a positive impact on society, with sustainability, diversity and veracity. B2G data-sharing should contribute to increasing equality by enabling more stakeholders to benefit from the existence of data.

Non-maleficence: B2G data-sharing initiatives need to minimise their potential maleficence or potential negative consequences ensuring the security, reliability, robustness of the data and the processes that analyse it. It should also apply a principle of prudence and always preserve privacy.

Section II: Analysis of the design of the proposed entities

The sharing of NPD under the Framework broadly involves five key entities: (i) The Data Custodian (ii) the Data Trustee (iii) the Community (iv) the Data Requester and the (v) Non-Personal Data Authority (NPDA). Data Trustees have the power to create bespoke HVDs which contain NPD belonging to one or many communities. Data Trustees create these HVDs by collecting data from Data Custodians, which in turn collect the data from data principals based on their consent. The NPDA can mandate data sharing between the Data Custodian and the Data Trustee except on certain grounds mentioned in the Report. Further, the Framework allows for Data Requesters to approach Data Trustees for seeking access to HVDs. Data Trustees are free to deny access of HVDs to Data Requesters (Ministry of Electronics and Information Technology, 2020).

Our analysis of the Framework suggests that **the proposed institutional design of these entities is weak, and riddled with several and severe misalignment of interests that can weaken the proposed community rights and the desired economic benefits**. We discuss the deficiencies in each of these proposed entities below.

1. The current conceptualisation of "Community" is not inclusive, creates challenges for collective decision making and threatens the existence of community rights.

The Framework defines "Community" as:

> "*…Any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community*." (p. 16).

This definition of community requires that members of a community share some pre-defined socially constructed, physical and/or behavioural characteristics (Kammourieh, et al., 2017). Further, it assumes that the members of such groups are self-aware and proclaim the existence of and belongingness to such groups (Dvara Research, 2020; Mittelstadt, 2016). Mittelstad (2016) identifies three types of groups based on membership:

i. ***Collectives:*** This refers to groups formed by individuals based on common background, interests, traits, and/or purposes, such as labour unions and trade unions.

ii. ***Ascriptive groups:*** This refers to groups formed by individuals that share some inherent or incidentally developed characteristics, such as ethnic and racial groups.

iii. ***Ad-hoc groups:*** This refers to groups whose membership is based on perceived, and sometimes new and imperceptible links between members, often for a limited purpose or time. These include market segments and profiling groups (Dvara Research, 2020).

The current formulation of community in the Framework leaves Ad-hoc groups out of the scope of community rights. This is especially worrying considering that a sizeable proportion of use cases on the Internet affect such Ad-hoc communities. In 2014, the White House Published a report on Data Brokers. That Report produced evidence that data brokers create highly nuanced profiles of individuals on the web such as *single mothers that speak Spanish* (Federal Trade Commission, 2014). These profiles, in one use case were sold to a predatory lender who utilised these insights to make predatory loans. While it is clear that there was a community of single mothers that was affected by these unethical lending practices, it is also amply clear that individual members of this community (i) do not know such a community exists (ii) do not know they belong to a community such as this, and (iii) cannot identify other members of the community. Therefore, it is unreasonable to expect this group to coordinate amongst themselves and exercise their collective rights to protect themselves from harm. Therefore, this Framework does not provide for a method for virtual communities to be recognised or exercise their rights and does not appear to be inclusive.

2. The Data Trustee model risks being unrepresentative and prone to abuse due to lack of misalignment of incentives.

2.1. The Data Trustee model risks being unrepresentative.

Per Section 7.7 of the Framework, a Data Trustee is any government or non-profit private organisation that decides to host an HVD for representing the interests of a community (pp. 18-19). In principle, the Framework enables any group of members from a community to organise themselves to create a Data Trustee. Further, per section 7.8 (iii) of the Framework, support from a "*minimum number of community entities*" is an important criterion for the NPDA to consider when assessing the applications for formation of Data Trustees. (p. 19). However, we worry that though necessary, these safeguards may be insufficient to ensure the representativeness of Data Trustees.

Learnings from the pilot of a Data Trust in the UK suggest that deliberative effort and democratic decision making is crucial to improve legitimacy of the data trust, peoples' willingness to share their data with them, and also affects the value that can be generated from the sharing of that data. A report on the learnings of the pilot, co-authored with the Open Data Institute, emphasises that "*engagement and deliberation are central to the way that data trusts build trust*" (Open Data Institute, 2019). Engagement and deliberation gain heightened significance in the context of civic data, i.e., data trusts that use citizens' data for solving citizens' issues. On ground experience of a prominent data trust experiment, Toronto's Quayside, provides another useful example in this regard. Among the many criticisms of the project, a significant one has been its proposal to create a civic data trust for controlling data collected in the area, without citizens' engagement and participation in its design. It has left an enduring lesson for involving citizens in the creation of datasets based on their data, and directed at solving their problems (McDonald, 2018; Open Data Institute, 2019).

First, in its current form, the Framework does not contain specific guidelines to ensure how Data Trustees would engage and conduct consultations with the digitally marginalised, historically under-represented and the harder-to-reach segments of society. The Framework lacks provisions that can guarantee representation and service for diverse communities. A representation of minimum community members does not necessarily translate into the representation of the most vulnerable members of the community.This is especially true for the Indian demographic where estimates suggest only 25-40% of the population own a smartphone (Chugh & Raghavan, 2019), and computer ownership continues to remain low with a mere 4.4% of rural households and 23.4% urban households reporting having a computer as of June 2018 (Ministry of Statistics and Programme Implementation, 2020). In such instances, a digital-first data trust may not be inclusive and risks leaving out the digitally excluded from making the decision on how the data about them, collected by public and private infrastructure, should be used (Open Data Institute, 2019).

Further, there also exists significant barriers that prevent under-represented communities from organising themselves and creating their own Data Trusts. In its current form, the Framework requires communities to register themselves as section 8 companies, possess high levels of technical expertise to maintain databases, and expend significant resources to maintain the technical infrastructure to host HVDs. There does not appear to be any indication that the Government is required to upskill or fund the efforts of marginalized communities that wish to perform the functions of a Data Trustee. In the absence of public support, these technical requirements pose significant barriers for marginalized communities to become Data Trusts.

2.2. The limitation of only one Data Trustee per HVD appears arbitrary and prone to abuse of dominance.

Section 7.7 (iv) of the Framework mandates that only one Data Trustee can be appointed to oversee an HVD (p. 19). The rationale for limiting the number of Data Trustees that can exercise control over an HVD appears unclear. A preliminary analysis suggests that it creates a condition of both monopoly and monopsony in the data-sharing framework. By limiting the number of Data Trustees per HVD, the Framework risks creating a monopoly, forcing people to share their data with the Data Trust even when they are not satisfied with their governance or decision-making practices. Further, the lack of competition among Data Trustees also leaves little incentives for a Data Trustee to invest in improving the quality or format of data, forcing end-users to keep accepting inferior quality data.

This preliminary analysis is validated by emerging evidence on competition among Data Trustees. In their seminal paper, Delacroix & Lawrence (2018) find that the effectiveness of a Data Trust framework to give users control over their data increases when users are free to choose among multiple Trusts. The authors write that "*there should be a plurality of Trusts, allowing data subjects to choose a Trust that reflects their aspirations, and to switch Trusts when needed.*" In light of growing scholarly support of the consumer protecting and market disciplining effect of multiple Data Trusts, it is unclear why the Framework has chosen to shut competition among Data Trustees.

Recommendations for creating socially legitimate Data Trustees

If a Data Trustee is to represent the interests of diverse communities within a larger community, and owe a duty of care, there must be an institutional mechanism that can promote democratic process to (i) define interests (ii) make decisions (iii) bargain for benefits (iv) ensure robust governance (v) resolve conflicts and (vi) enforce the duty of care (Jindal & Nigam, 2020)**.** Adding these nuances will strengthen the representativeness of the proposed Data Trustee framework.

Further, the recently concluded Data Trust pilots in the UK have led to the recognition of six stages for the creation of socially legitimate data trusts. These stages set out the actions that a Data Trust must perform to ensure it is democratic, upholds the interests of the communities it seeks to represent and demonstrate that it acted in the best interest of the community. These stages and the specific actions they command are set in Box 2, and can serve as guidelines for creating socially legitimate Data Trustees.

Box 2: Phases of the life cycle of a Data Trust | Source: (Open Data Institute, 2019).

Phases of the life cycle of a Data Trust

- **Scope –** This stage is needed to determine *if* a Data Trust is needed. It requires entities willing to create a Data Trust to search on existing bodies and intermediaries that may already collect the proposed data set that the Data Trust seeks to share. It also requires the prospective Data Trust to investigate if a Data Trust is the most suitable mechanism to share the prospective dataset or if for instance an open sharing mechanism may be more suitable. This stage also requires a prospective Data Trust to engage with all stakeholders including prospective data holders [custodian in this Framework], beneficiaries and end-users and explain the objectives of the data trust, the use cases it is trying to solve for, and assess if there is demand for the database.
- **Co-design –** This stage requires prospective Data Trusts to build consensus, purpose, its legal and organisational structure, how it will be staffed, and the roles of all stakeholders. This stage focuses on deciding how benefits will be created and shared by the data trust, who can provide data to the trust, and charting out rules around how decisions will be made regarding granting access to the data held by the Trust.
- **Launch** – While launching the Data Trust, it should be mandatory to set up and register the organisation in line with its agreed purpose, and ensure it publishes information transparently about its processes. Communication should be targeted at all stakeholders in ways that are most accessible to them, so they know the Data Trust exists and are able to exercise scrutiny over its functioning.
- **Operate** – This stage focuses on the need to ensure that data is maintained and will continue to be available. Data contributions, and data requests, will need to be accepted, processed and responded to, and the complementary technical systems needed to support these requests will have to be created and maintained. Further, the benefits from harnessing the data should be administered and audits or checks may be needed to ensure that stakeholders conform to the Data Trust rules. Breaches of rules about how the data is used will need to be detected and dealt with.
- **Evaluate** – When evaluating a Data Trust, it will be important to consider both positive and negative impacts on people. Stakeholders should be surveyed to gather feedback and assess if the decisions being made are consistent with the trust’s purpose. Some of this evaluation may need to be done by external third-parties to ensure independent evaluation in the operations of the Data Trust. Regulators should also evaluate Data Trusts.
- **Retire** – If a Data Trust has been evaluated and a decision has been made to retire it, the timeline for its close-down period will need to be determined and communicated to stakeholders. Services will need to be wound down and the information that it contained should be archived.

3. The contextual definition of NPD introduces infirmities in the regulatory remit of the NPDA.

Principles of effective regulation require that the objectives of a regulation are clear and regulators do not have competing, conflicting objectives (OECD, 2014). We submit that the context-sensitive and constantly evolving definition of NPD introduces infirmities in the regulatory objectives of the NPDA.

The definition of NPD as stated in the Framework (p. 7) is "*data that is not personal data (as defined under the PDP Bill), or data that is without any Personally Identifiable Information (PII)*". The distinction between NPD and personal data is drawn on the basis of *identifiability*. Information is considered personally identifiable if it either directly identifies individuals or identifies individuals when it is considered in conjunction with other available information (Medical Research Council, 2019). Although, these definitions appear to be theoretically distinct, in practice they are mutually exclusive.

Identifiability of data is continuously evolving and context-sensitive and cannot be established in an absolute manner. Often NPD can be combined to reveal PII. In one study, anonymised data that had information about the movie preferences of Netflix users was used in conjunction with publicly available information from the Internet Movie Database (IMDb) to deanonymize the original data set (Narayanan & Shmatikov, 2008). Another study used anonymised census data from 1990 and found that 87% of the American Population could be uniquely identified on the basis of just three data variables – the 5-digit ZIP code, gender, and date of birth (Sweeney, 2000). As such, what is not personal data now might well be so in the future (Dvara Research, 2020; Graef, Gellert, & Husovec, 2018).

Consequently, basing the regulatory remit of the NPDA on *identifiability* would mean that some data points in one context may fall under the jurisdiction of the NPDA while in another context the same datapoints may be used to extract PII and therefore fall out of the jurisdiction of the NPDA. This implies that the NPDA will not be able to regulate all anonymised data in the same manner or using the same tools. It necessitates the NPDA to engage with each instance of use of NPD to investigate if it in that context reveals PII. For a regulatory body to effectively discharge its objectives, its regulatory remit ought to be observable, certain and static. However, NPD is dynamic and context-dependent and cannot be established in an absolute manner, making it hard to establish a certain regulatory remit (Dvara Research, 2020). The illusive notion of NPD as a starting point for new regulation could create major legal uncertainties and undermine the effectiveness of the objectives that it aims to pursue (Dvara Research, 2020; Graef, Gellert, & Husovec, 2018).

Section III: Gaps in consumer protection in the Framework

The Framework seems to have two chief tools for ensuring the protection of consumers/communities: (i) the communities' right to minimise the harm that arises from the re-identification and misuse of their NPD, and (ii) the "duty of care" imposed on Data Custodians and Data Trustees in relation to the data principal and community respectively. Our analysis suggests that these tools are inadequate and do not offer robust consumer protection. Four specific gaps in the Framework's formulation of consumer protection are:

1. "*Harm*" is not defined, is narrowly conceptualised and is not adequately mitigated under the Framework.

The Framework sets the goal of minimising data-related harms from the re-identification and misuse of NPD (pp. 5-6), and recognises the right of communities to minimise the harms from the use and misuse of their NPD (p. 16). Despite these provisions, the Framework does not provide a definition of harm.

The Framework also has a very narrow conceptualisation of harm. In section 3.5, the Framework seeks to "*address privacy, re-identification of anonymized personal data, and prevent misuse of and harms from data"* (pp. 5-6). The content of the Framework disproportionately focuses on the privacy harms that can arise from the sharing and use of NPD (such as in section 3.6, section 7.4 (iv) and section 8.6). It does not consider the range of harms that can accrue to a community due to a misuse of their data. Some of these can be an increased probability of collusion among firms after the strategic information about a particular market has been revealed, as discussed in Section 1.2 of this Response. Similarly, other harms can include revealing sensitive information such as political preferences and sexual orientation of a community. Revealing this information does not necessarily invade the privacy of a specific person – but it does reveal sensitive information about a group of people. The Framework does not seem to expressly articulate these harms and explain how they can be mitigated in the proposed set-up.

Finally, the Framework does not have adequate mechanisms to mitigate these narrowly conceived harms. The Framework seems to have two chief tools for ensuring the protection of consumers/communities, which are: (i) the communities' right to minimise the harm that arises from the re-identification and misuse of their NPD, and (ii) the "duty of care" imposed on Data Custodians and Data Trustees in relation to the data principal and community respectively. The first invests a right in the community to protect themselves from harm, and the second makes it illegal for Data Custodians or Data Trustees to intentionally harm the data principal or community. However, the mechanisms for communities to *actually* protect themselves from harm are absent. It also does not state what the consequences of harming communities could be, and how the victims can be compensated.

2. Relying on consent for anonymisation of personal data is unsuitable for user protection in relation to NPD.

Section 5.4 of the Framework recommends that Data Custodians must provide a notice to the data principal, at the time of collection of personal data, indicating that said data might be anonymised and used for other purposes. It also recommends that the notice must provide an opt-out mechanism for the same (pp. 11-12).

It is well-recognised that consent should be explicit to the purpose of processing specific data, informs an individual on how and where their data is being used, and it should be revocable at any time (EU GDPR, n.a.; Office of the High Commissioner, United Nations Human Rights, 2013). However, by requiring data principals to sign up for non-specific consent i.e., the consent that neither states which parties can use their data and for what purposes and for how long, this consent does not qualify as either informed or specific.

There exists rich literature to suggest that even informed consent artifacts have limitations on how well they are able to support consumers in making informed and rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data (Solove, 2012). Acquisti (2004) has highlighted how immediate gratification bias — due to which individuals overvalue the immediate period as compared to all future periods — can cause individuals to make suboptimal privacy decisions (Dvara Research, 2020). Therefore, a lack of these crucial details in the Framework with respect to consent makes it an even weaker tool for consumer protection.

A consent artefact lacking these crucial details will not be able to help consumers assess the riskiness of sharing their NPD. It will also fail to communicate which entities can be held liable for any lapse in consumer protection. It completely disempowers the consumer from being able to control how their NPD can be used, or bringing to account those who deviate from the agreed terms of use.

3. The proposed model for grievance redress in the Framework is unsuitable for safeguarding consumers' interests.

The NPD Framework in Section 7.7 (ii) states that "*Data Trustees have a responsibility towards responsible data stewardship and a 'duty of care' to the concerned community in relation to handling non-personal data related to it*". As part of this responsibility "*a Data Trustee is obligated to establish grievance redressal mechanisms so that the community can raise grievances*" (pp. 18-19). While this is an improvement from the first draft of the NPD Framework which lacked a grievance redress mechanism altogether, the current Framework does not expand on the grievance redress available to individuals/communities in case harms arise from the use of data.

Access to grievance redress is imperative, especially in the context of the digital economy, where risks exist that have not even been conceived (Prasad, 2019). The provision currently relating to grievance redress only confers upon Data Trustees the duty to set up a redress mechanism for communities to raise grievances. It does not provide any further elaboration.

The NPD Framework currently has only stated that the communities are to raise grievances with a regulator through the Data Trustees (pp. 16, 19). However, an analysis of the interactions between the various actors in the system indicate that data trustees might not be the appropriate entity to act as the point of contact for initiating redress by communities. Communities directly provide their data to Data Custodians, and Data Trustees then create high-value datasets by interacting with Data Custodians. Further, data in one HVD can belong to several communities. For instance, section 7. 9 (v) gives an example of how the Directorate of Urban Land Transport could become a data trustee of HVD of traffic data with data inputs from multiple ride-sharing platforms, city police department etc. (p. 20). Clearly, this HVD would contain datasets from multiple communities - those that hail cabs, those that are recorded in the databases of the police record, those who drive their own cars and so on. Similarly, one community may provide data to several HVDs. For instance, these communities may also provide data to the traffic department to create a dataset to manage traffic congestion in the city. Therefore, in the current system - there is no one-to-one mapping of communities, their databases and Data Trustees. Consequently, in the current system the onus would be on the communities to identify the relevant Data Trustee with whom they should register their grievance, as they do not have any insight on which Data Trustees are responsible for which datasets.

Our findings indicate that users consider themselves ill-equipped to seek remedies in the digital economy for want of digital literacy and an understanding of the digital economy (CGAP, Dalberg & Dvara Research, 2017). As such, lodging the responsibility on consumers to determine the exact nature of data-related harms that has been caused, and to identify the faulting entity could lead to their disempowerment. This could also create serious barriers in seeking redress.

To this end, we outline certain guiding principles that can be adhered to create an effective redress system.

Recommendations for effective grievance redressal in the Framework

We lay out some guiding principles recognised in other jurisdictions and by multilateral organisations that can be used as guidelines to create an effective grievance redress system within this Framework. These principles include:

i. ***Ensuring accessibility*****:** Providing ease of access to all is the most foundational principle of grievance redress. The sub-components of this principle include:
   a. Providing appropriate support to those who are unable to access redress forums.
   b. Ensuring redress systems are inclusive, suitable to the culture, gender perceptive, proportionate to the levels of literacy and the digital competencies of the population, perceptive to the needs of the differently abled etc. (Asian Development Bank, 2010; United Nations Office of the High Commissioner on Human Rights, 2011).

ii. ***Ensuring transparency*****:** To inspire confidence among consumers, the grievance redress system should function on two levels:
   a. The decision-making process in the redress system must be clearly communicated to the consumer who has raised the grievance. The consumer should also be continuously intimated about the progress made regarding the grievance.
   b. The grievance system should be kept accountable by requiring the publishing of various insights from its operation such as volume of complaints addressed, most recurring type of complaint etc. (International Commission of Jurists, 2019; International Finance Corporation, 2020).

iii. ***Ensuring seamless redress*****:** A grievance redress system must be procedurally effective by ensuring that:
   a. the process of filing complaints is simple; and
   b. genuine grievances are not declined on procedural grounds (International Commission of Jurists, 2019).

iv. ***Encouraging integrated redress management*****:** A grievance redress system must ensure that it does not impose cognitive burdens on the consumers which might create a barrier in seeking redress. Therefore, the redress system must be easily accessible, and front a unified consumer-facing system which assumes the responsibility of directing the consumer grievance to the appropriate regulator, government body or service provider (Bondy & Le Sueur, 2012).

v. ***Enabling cost-effective and timely redress*****:** Grievance redress systems should not create barriers in the form of high monetary and time costs. Complaints must be addressed in a time-bound manner, and the burden imposed should not be disproportionate to the economic value in dispute, thereby defeating its very motivation (Raghavan, 2015).

These principles can be used as guidelines to create a grievance redress system that aids in addressing issues relating to harms from the sharing of non-personal data. As such, there is a need to institute a complete grievance redressal system at the core of the Framework's ecosystem, especially since the activity revolves around the sharing of data.

4. The Framework lacks clearly defined liability and accountability structures.

The Framework in Section 8.15 alludes to liability under the mechanisms which can provide certain checks and balances to the creation of HVDs and the sharing process. It states that "*organisations are to be indemnified against any vulnerability found as long as they swiftly remedy it and adopt a standards-driven approach (like annual light-weight, self-reported, self-audited digital compliance reports)*" (p. 31). However, the Framework does not provide any detail regarding how liability is to be apportioned among the users of the shared data in instances where harm arises from such usage.

A liability framework is essential as it helps to strike a balance between improving the confidence of consumers in a product or service while also providing room for innovation and improvement in the product/service. The question of who ultimately bears the cost of possible damages is also imperative for the roll-out of redress. Liability frameworks have been previously apportioned with the use of product liability directives and safety regimes. However there are certain specific concerns that arise in the context of emerging digital technologies which makes it difficult to allocate liability based on these laws. These concerns and limitations must be looked into in further detail for the creation of a liability framework.

Liability is broadly understood as one entity (or several) being responsible for any harm or damage realised by another party, which may provide reasons for compensation, functionally or otherwise by the responsible party to the latter (Debussche, César, & Mortier, 2019). The purpose of liability law, from an economic perspective, is to provide adequate incentives to entities to invest in precaution, and also to distribute the risk of accidents (Franzoni, 2014). As such, any liability framework should seek to induce confidence in the safety, reliability and consistency of products and services so as to balance the outcomes of protecting prospective victims of harm but also providing enough flexibility to help in the development of new technologies, products or services (European Parliament, 2020). It also enables to enforce claims of the victims. Any lack of clarity in apportioning liability could result in difficulty in enforcing claims (European Commission, 2018).

Recommendations concerning the liability and accountability structures in the Framework

Therefore, the creation of legal certainty with respect to liability is an essential component for driving innovation and for enforcing consumers' claims should they be harmed. Some approaches that can be considered in the context of emerging technologies include:

i. ***Risk generating or risk management approaches:*** In this approach liability could be apportioned to those entities generating a substantial risk for others or to those entities that are in an appropriate position to curtail or circumvent the realisation of the risk.

ii. ***Voluntary or mandatory insurance schemes:*** This scheme can be combined with other liability approaches. These schemes could compensate the party that has been affected (e.g., the consumer). This scheme would need to furnish legal protection to a business' investments while also ensuring that the victims of damage receive the appropriate compensation or insurance (European Commission, 2017).

References

Agarwal, A. (2020, September 9). *#NAMA: Assessing the Concepts Introduced in the Non-Personal Data Report*. Retrieved from Medianama: https://www.medianama.com/2020/09/223-non-personal-data-report-definitions/

Agrawal, D. (2017, April 17). *Intellectual property rights: Locating public interest in the law*. Retrieved from Firstpost: https://www.firstpost.com/long-reads/intellectual-property-rights-locating-public-interest-in-the-law-3388388.html

Asian Development Bank. (2010). *Designing and Implementing Grievance Redressal Mechanisms*. Retrieved from Asian Development Bank: https://www.adb.org/sites/default/files/institutional-document/32956/files/grievance-redress-mechanisms.pdf

Baranoff, E., Brockett, P. L., & Kahane, Y. (2009). *Risk Management for Enterprises and Individuals*. Retrieved from Saylor Foundation: https://open.umn.edu/opentextbooks/textbooks/37

Benjamin, S., Bhuvaneswari, P., & Rajan, P. (2007). *Bhoomi: 'E-Governance', Or ,An Anti-Politics Machine Necessary to Globalize Bangalore?* Retrieved from CASUM-m Working Paper: https://casumm.files.wordpress.com/2008/09/bhoomi-e-governance.pdf

Bondy, V., & Le Sueur, A. (2012, August). *Designing Redress: A Study about Grievances against Public Bodies*. Retrieved from The Public Law Project: https://publiclawproject.org.uk/wp-content/uploads/data/resources/123/PLP_2012_Designing_redress.pdf

Brunner, J. (2019, November 29). *RTI Judgment: Confusions about Public Interest*. Retrieved from Centre for Law & Policy: https://clpr.org.in/blog/rti-judgment-confusions-about-public-interest/

CGAP, Dalberg & Dvara Research. (2017). *Privacy on the Line*. Retrieved from Dvara Research Blog: https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-TheLine.pdf

Chopra, S., & Saikia, N. (2018, December 02). *Cross-Sectoral Conceptions of 'Public Interest'*. Retrieved from Bar and Bench: https://www.barandbench.com/columns/cross-sectoral-conceptions-of-public-interest

Chugh, B., & Raghavan, M. (2019, June 18). *The RBI's proposed Public Credit Registry and its implications for the credit reporting system in India*. Retrieved from Dvara Research Blog: https://www.dvara.com/blog/2019/06/18/the-rbis-proposed-public-credit-registry-and-its-implications-for-the-credit-reporting-system-in-india/

CODATA-PASTD. (2015, May 26). *Geneva Data Sharing Principles in Developing Countries* . Retrieved from International Telecommunication Union: http://www.itu.int/en/itu-wsis/SiteAssets/hls/statements/5/CODATA_PASTD_WSIS_Statement_2015_Geneva_20150526.doc

Competition Commission of India. (2020). *Provisions Relating to Abuse of Dominance*. Retrieved from Competition Commission of India: https://www.cci.gov.in/sites/default/files/advocacy_booklet_document/AOD.pdf

Contracts for Data Collaboration. (n.a.). *Understanding Public-Private Data Sharing Agreements*. Retrieved from Contracts for Data Collaboration: https://directus.thegovlab.com/uploads/thegovlab/blog_img_archive/2020/04/WORKING-DRAFT-4.20-C4DC-Questions-to-Consider.pdf

Debussche, J., César, J., & Mortier, S. (2019, February). *Big Data & Issues & Opportunities: Liability*. Retrieved from Bird & Bird: https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-liabilityhttps://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-liability

Delacroix, S., & Lawrence, N. (2018, November 9). *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265315

Department of Consumer Affairs. (2011). *Report of the Working Group on Consumer Protection*. Retrieved from NITI Aayog: https://niti.gov.in/planningcommission.gov.in/docs/aboutus/committee/wrkgrp12/pp/wg_cp1.pdf

Department of Economic Affairs. (2016). *Report of the Task Force on Financial Redress Agency*. Retrieved from Department of Economic Affairs: https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf

Dvara Research. (2020, September 13). *Our Response to the Report of the Committee of Experts on Non-Personal Data.* Retrieved from Dvara Research Blog: https://www.dvara.com/research/wp-content/uploads/2020/10/Our-Response-to-the-Report-of-the-Committee-of-Experts-on-Non-Personal-Data.pdf

Economic Commission for Latin America and the Caribbean. (2013). *Women in the digital economy*. Retrieved from Digital Repository: Economic Commission for Latin America and the Caribbean: https://repositorio.cepal.org/bitstream/handle/11362/16562/1/S2013529_en.pdf

EU GDPR. (n.a.). *What are the GDPR consent requirements?* Retrieved from GDPR.EU: https://gdpr.eu/gdpr-consent-requirements/

EuroCities. (n.a.). *About Us*. Retrieved from EuroCities: https://eurocities.eu/about-us/

European Commission. (2011, January 14). *Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements*. Retrieved from NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XC0114(04)&from=EN

European Commission. (2017). *Building a European Data Economy*. Retrieved from Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.: https://eur-lex.europa.eu/content/news/building_EU_data_economy.html

European Commission. (2018). *Liability for Emerging Digital Technologies*. Retrieved from Commission Staff Working Document: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0137&from=en

European Commission. (2019, May 14). *Antitrust: Commission opens investigation into Insurance Ireland data pooling system*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2509

European Commission. (2020). *Towards a European strategy on business-to-government data sharing for the public interest*. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/news/commission-appoints-expert-group-business-government-data-sharing

European Parliament. (2020). *Report with Recommendations to the Commission on a Civil Liability Regime or Artificial Intelligence*. Retrieved from European Parliament: https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.pdf

Federal Trade Commission. (2014). *Data Brokers: A Call for Transparency & Accountability.*

Federation of German Consumer Organisations. (2017). *Indicators of consumer protection and empowerment in the digital world*. Retrieved from Bundesministerium der Justiz und fur Verbaucherschutz: https://www.bmjv.de/DE/Startseite/Startseite_node.html

Financial Sector Legislative Reforms Commission. (2013). *Report of the Financial Sectors Legislative Reforms Commission*. Retrieved from Department of Economic Affairs: https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

Franzoni, L. A. (2014, February 28). *Liability Law and Uncertainty Spreading*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2432861

Graef, I., Gellert, R., & Husovec, M. (2018, September 28). *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is*

Counterproductive to Data Innovation. Retrieved from TILEC Discussion Paper No. 2018-029: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189

Graef, I., Tombal, T., & Streel, A. (2019, November). *Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law*. Retrieved from TILEC Discussion Paper: https://www.researchgate.net/profile/Alexandre-Streel/publication/337595029_Limits_and_Enablers_of_Data_Sharing_An_Analytical_Framework_for_EU_Competition_Data_Protection_and_Consumer_Law/links/5e96c264299bf130799ad8cf/Limits-and-Enablers-of-Data-Sharing-

International Commission of Jurists. (2019). *Effective Operational-level Grievance Mechanisms*. Retrieved from International Commission of Jurists: https://www.icj.org/wp-content/uploads/2019/11/Universal-Grievance-Mechanisms-Publications-Reports-Thematic-reports-2019-ENG.pdf

International Finance Corporation. (2020). *Grievance Management*. Retrieved from International Finance Corporation: https://www.ifc.org/wps/wcm/connect/963ec017-2b1f-4487-b533-14fda473b1a5/PartOne_GrievanceManagement.pdf?MOD=AJPERES&CVID=jqewwBr

Intersoft Consulting. (n.d.). Retrieved from https://gdpr-info.eu/art-17-gdpr/

Jindal, T., & Nigam, A. (2020, November 20). *Data Stewarship for Non-Personal Data in India: A Position Paper on Data Trusts*. Retrieved from Vidhi Centre for Legal Policy: https://vidhilegalpolicy.in/research/data-stewardship-for-non-personal-data-in-india/

Kammourieh, L., Baar, T., Berens, J., Letouze, E., Manske, J., Palmer, J., . . . Vinck, P. (2017). Group Privacy in the Age of Big Data. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group Privacy New Challenges of Data Technologies* (pp. 37-67). Springer International Publishing. Retrieved from https://www.springer.com/gp/book/9783319466064#aboutAuthors

Kapoor, A. (2020, December 30). *Observer Research Foundation*. Retrieved from https://www.orfonline.org/expert-speak/data-development-revisiting-non-personal-data-governance-framework/#:~:text=In%20July%202020%2C%20an%20expert,need%20to%20democratise%20its%20use.

Kurth, H. A. (2021, January 15). *The National Law Review*. Retrieved from https://www.natlawreview.com/article/india-releases-revised-non-personal-data-framework

Lomas, N. (2019, 24 July). Retrieved from https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

Marda, V. (2020, October 15). *Ada Lovelace Institute.* Retrieved from https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/

Mason, S. (2015, December 30). *Benefits and Harms of "Big Data"* . Retrieved from The Centre for Internet & Society: https://cis-india.org/internet-governance/blog/benefits-and-harms-of-big-data

Matakis, L. (2019, February 15). *The WIRED Guide to Your Personal Data (and Who Is Using It)*. Retrieved from Wired: https://www.wired.com/story/wired-guide-personal-data-collection/

McDonald, S. (2018, October 17). *Toronto, Civic Data, and Trust*. Retrieved from Medium: https://medium.com/@digitalpublic/toronto-civic-data-and-trust-ee7ab928fb68

Medical Research Council. (2019, September). *GDPR Guidance Note 5: Identifiability, Anonymisation and Pseudonymisation*. Retrieved from Regulatory Support Centre: https://mrc.ukri.org/documents/pdf/gdpr-guidance-note-5-identifiability-anonymisation-and-pseudonymisation/

Mejia, W. (2019, April 4). *10 principles for good data*. Retrieved from European Commission: https://ec.europa.eu/futurium/en/digital-transition/10-principles-good-data

Ministry of Electronics and Information Technology. (2020, December 16). *Report by the Committee of Experts on Non-Personal Data Governance Framework*. Retrieved from Ministry of Electronics and Information Technology (MeitY): https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

Ministry of Science and Technology. (2012, March 17). *National Data Sharing and Accessibility Policy*. Retrieved from Department of Science: https://dst.gov.in/national-data-sharing-and-accessibility-policy-0

Ministry of Statistics and Programme Implementation. (2020, March 4). *NSS 75th Round (July 2017 – June, 2018)*. Retrieved from The Hindu Centre for Politics and Public Policy: https://www.thehinducentre.com/resources/article30980071.ece

Mittelstadt, B. (2016). *From Individual to Group Privacy in Big Data Analytics*. Retrieved from Springer: https://link.springer.com/article/10.1007/s13347-017-0253-7

Narayanan, A., & Shmatikov, V. (2008). *Robust De-anonymization of Large Sparse Datasets*. Retrieved from IEEE Symposium on Security and Privacy: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

OECD. (2014, July 29). *The Governance of Regulators* . Retrieved from OECD iLibrary: https://www.oecd-ilibrary.org/docserver/9789264209015-6-

en.pdf?expires=1612104209&id=id&accname=guest&checksum=204EF6BD0C8380DCB0DE5C3887F6114B

OECD. (2018). *Bridging the Digital Gender Divide: Include, Upskill, Innovate*. Retrieved from Organisation for Economic Co-operation and Development: http://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf

Office of the High Commissioner, United Nations Human Rights . (2013, September). *Free, Prior and Informed Consent of Indigenous Peoples* . Retrieved from United Nations Human Rights Office of the High Commissioner: https://www.ohchr.org/Documents/Issues/ipeoples/freepriorandinformedconsent.pdf

Open Data Institute. (2019). *Data trusts: lessons from three pilots*. Retrieved from Google Documents: https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#

Prasad, S. (2019). *Defining 'Harm' in the Digital Ecosystem.* Retrieved from Dvara Research Blog: https://www.dvara.com/blog/2019/05/06/defining-harm-in-the-digital-ecosystem/

Raghavan, M. (2015, September). *Upholding Customer Protection: Tales from Indian Courts*. Retrieved from Dvara Research Blog: https://www.dvara.com/blog/2015/09/07/upholding-customer-protection-tales-from-the-indian-courts/

Rijmenam, D. v. (2013, February 11). Retrieved from https://datafloq.com/read/re-identifying-anonymous-people-with-big-data/228#:~:text=Re%2Didentification%20of%20individuals%20can,embarrassment%20or%20even%20identity%2Dtheft.&text=A%20well%2Dknown%20example%20is,Netflix%20done%20by%20Arvind%20Narayanan.

Solove, D. (2012, November). *Privacy Self-Management and the Consent Dilemma*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Supreme Court Observer. (n.a.). *RTI & Judicial Independence: Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*. Retrieved from Supreme Court Observer: https://www.scobserver.in/court-case/rti-act-and-judicial-independence/rti-judgment-in-plain-english

Sweeney, L. (2000). *Simple Demographics Often Identify People Uniquely*. Retrieved from Carnegie Mellon University: https://dataprivacylab.org/projects/identifiability/paper1.pdf

UNCTAD. (2019). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries.* UNCTAD. Retrieved from https://unctad.org/system/files/official-document/der2019_en.pdf

United Nations Office of the High Commissioner on Human Rights. (2011). *Guiding Principles on Business and Human Rights*. Retrieved from United Nations Office of the High Commissioner on Human Rights: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

United Nations Sustainable Development Group. (2017, November). *Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda* . Retrieved from United Nations Sustainable Development Group: https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda

World Economic Forum. (2019, December 11). *Competition Policy in a Globalized, Digitalized Economy*. Retrieved from World Economic Forum: https://www.weforum.org/whitepapers/competition-policy-in-a-globalized-digitalized-economy

Wright, G., Prakash, P., Abraham, S., & Shah, N. (n.a.). *Report on Open Government Data in India*. Retrieved from The Centre for Internet and Society: https://cis-india.org/openness/publications/ogd-report/