POWER PERSPECTIVES

An initiative by Prayas (Energy Group)

Handling smart meter data: a privacy and security framework

April 2021

Narendra Pai, Aditya Chunekar, Shweta Kulkarni and Manabika Mandal[1], Prayas (Energy Group)[2]

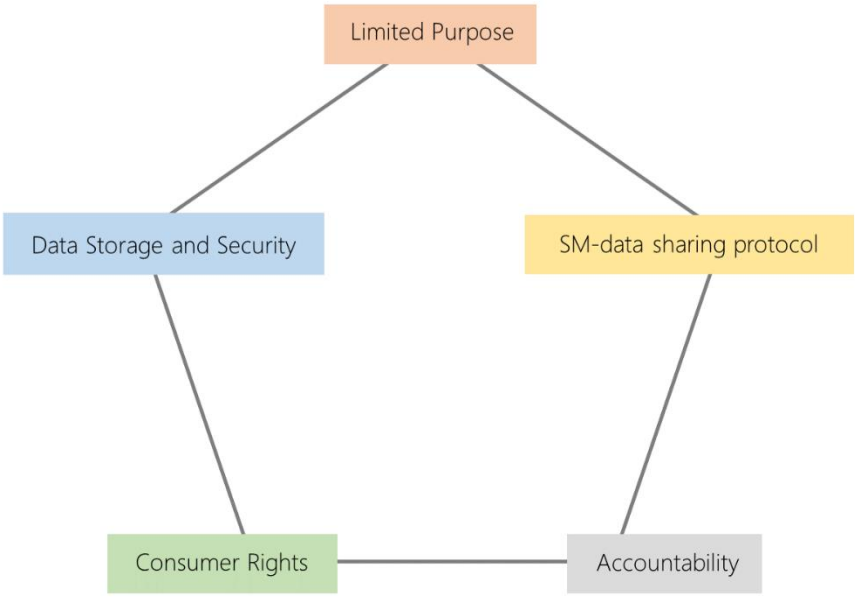
Smart meter data is personal data and needs to be treated accordingly. This gains importance as the ambitious project of replacing about 250 million conventional electricity meters in Indian homes with smart meters by 2022 picks pace. In the previous article, we discussed the prevalent privacy concerns of smart meter programmes and assessed the preparedness of the Indian electricity sector to address them. We concluded that a comprehensive data privacy and security framework is required to reap the full benefits of smart meters while at the same time ensuring consumer rights and interests. In this follow up article, we provide a Smart Meter Energy Consumption Data Privacy and Security Framework that can act as a starting point for further deliberations among the sector stakeholders ahead of the Personal data protection legislation.

1. Introduction

As discussed in the previous article, smart meter data can reveal personal details of the consumers. As the smart meter programme picks pace across the country, it is pertinent to understand these issues and address them. Further, a comprehensive personal data legislation is upcoming and likely to become the law soon. This new legislation, Personal Data Protection Bill 2019 (PDPB), will empower an independent data regulator – Data Protection Authority (DPA), to regulate matters of data privacy. DPA will possibly help evolve sector specific standards and regulations in consultation with sector regulators. However, with or without this legislation, the electricity sector needs to develop and adopt a data privacy and security framework to ensure consumer rights and interests. This needs due deliberation and consultation among various actors, including the consumers. Towards this end, the Ministry of Power (MoP) could come up with a whitepaper that provides a framework with various details of privacy and security aspects and measures that need to be adopted.

We propose broad contours of such a comprehensive Smart Meter Energy Consumption Data Privacy and Security Framework (SMEC-DPSF) (Figure 1).

Figure 1: Elements of a smart meter energy consumption data privacy and security framework



Source: Prayas (Energy Group)

Such a framework needs to clearly delineate the following-

i. Legitimate purposes with well-defined boundaries for collection, storage, processing and sharing of smart meter data and consumer consent requirements.
ii. The specific details of collection, storage and processing protocols and the manner in which these protocols, roles and responsibilities of concerned actors are operationalised
iii. Data storage and security aspects, which include clear definition of concerned actors' roles in ensuring correctness and security of the data stored and having a data breach response plan
iv. Consumer rights, which provide reliable and meaningful access to their data along with effective grievance redressal mechanisms.
v. Accountability mechanisms to ensure that concerned actors comply with the rules and regulations prescribed in the framework.

Next, we discuss each aspect of a proposed framework in detail.

2. Data privacy and security framework

2.1. Limited purposes of collection, storage, processing and sharing

A strong security and privacy framework requires clarity on the legitimate purposes of the use of smart meter data for the benefit of the sector and consumers. That is, the framework needs to define the boundaries of who can collect, store and share the smart meter data with whom and for what purposes. It is proposed that insofar as collection and storage of data is concerned, it should not be precluded by a 'purpose', provided necessary data privacy and security measures are followed.

As per the Personal Data Protection Bill 2019 (PDPB), explicit consent from the 'data principal' (or electricity consumer, in this case) is not required for processing personal data if those fall under the 'reasonable purposes', or for any purposes defined by the Data Protection Authority (DPA). However, combining the goals of the Electricity Act 2003 and the PDPB is important when handling smart meter data. Therefore, there must be a clear, comprehensive and exhaustive list of purposes for processing and sharing smart meter data. This should include a clear distinction between purposes of processing and sharing for which explicit consumer consent is required, and otherwise.

MoP can come up with this list of purposes or use-cases for processing and sharing. The same needs to be mapped to the specific provisions and goals of Electricity Act 2003 and must be discussed among stakeholders before finalising. Table 1 shows an illustrative *Limited Purposes Matrix* listing some specific purposes for which explicit consumer consent is required (List A) and purposes where explicit consumer consent is not required (List B). Once the matrix is finalised and operational, an entity wishing to process or share the data for a purpose outside this matrix, should seek the approval of the appropriate regulatory or executive authority. Subsequently, the lists may be amended periodically to allow for such purposes.

Table 1: Illustrative 'Limited Purposes' matrix for processing and sharing

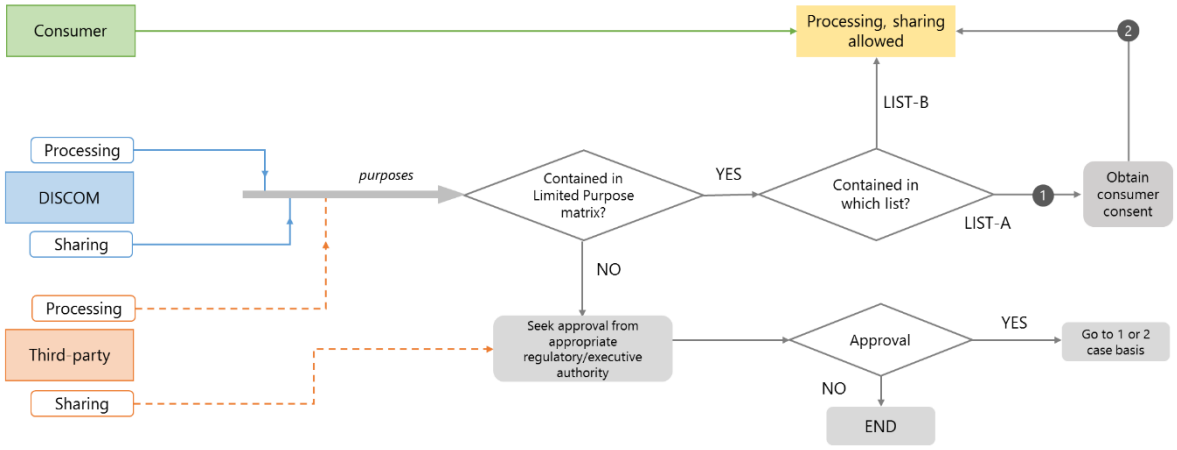
Sl no	List A: Explicit consumer consent required
1	In-house advertising by DISCOMs through electricity bills
2	Customised energy services to consumers by third-party entities
3	Selling of data to appliance manufacturers to promote sales of efficient appliances
.	
k	
Sl no	List B: Explicit consumer consent not required
1	Bill generation
2	Data requests to process consumer grievances
3	Resolve disputes on inflated consumption
4	Examine own consumption data for any purpose
.	
n	

Source: Prayas (Energy Group)

2.2. Smart meter data use and sharing protocol

In addition to informing energy efficiency programmes, smart meter programme also seeks to improve DISCOMs' operational efficiencies. Therefore, DISCOMs should be the sole custodians of their respective consumer specific energy use (CEUD) regardless of the smart meter programme implementation model (CAPEX, OPEX etc). In this proposed framework, while processing can be carried out by different entities, only DISCOMs and consumers themselves can be allowed to share the data with third-party entities. Figure 2 is the proposed flow-chart for processing and sharing for various actors and purposes. Any vendor or sub-vendor hired to implement and manage the smart metering systems will have no ownership of the CEUD and can access it only on a need basis and for the limited purposes only. DISCOMs should make the data handling protocol clear in its third-party contracts. For any purposes they are required to share anonymised data with third-parties, DISCOMs should also ensure that the anonymization is periodically tested against evolving deanonymization techniques.

Figure 2: Application of the proposed 'Limited purpose' matrix to data processing and sharing



Source: Prayas (Energy Group)

As discussed, DISCOMs can share the personally identifiable information along with CEUD with a third party only for a specific requirement such as bill generation, consumer grievance redressal or value added services. The *Limited Purposes matrix* should guide such decisions. As custodians, DISCOMs are responsible to ensure the data privacy and security of the smart meter data on behalf of the consumer.

2.3. Data Storage and Security

DISCOMs should ensure that the smart meter data is stored in a manner that privacy of the consumers and security of the data is ensured. DISCOM can store the data for a time duration as required for processing under the limited purposes. DISCOMs should ensure that the stored personally identifiable information (PII), like names, addresses, and phone numbers is correct and updated. Consumers should have access to both their PII and Consumer-specific energy use data (CEUD) and can request for modification if the data is found to be incorrect using appropriate validating mechanisms.

Elaborate measures should be put in place to prevent data breaches. Further, advanced metering infrastructure service providers (AMISP) should have a *Data Breach Response Plan* ready and should immediately contact the consumers, in case of a data breach, explaining the breach, steps taken and action needed, if any, by the consumer. At all levels, storage and transfer of personal data should comply with security standards set by the Ministry of Information Ministry of Electronics and Information Technology (MeitY) under the various rules of the Information Technology Act 2000 (IT Act).

2.4. Accountability

DISCOMs should prepare a Data Privacy and Security Plan

DISCOMs are accountable to the consumers with respect to data privacy and security, and should thus prepare a *Data Privacy and Security Plan* which details out the specific purposes and policies, practices, processes and technologies employed to collect, manage, and process the smart meter data in a fair, transparent, and secure manner. This plan should be available for public comments and subsequently approved by an appropriate authority before the DISCOMs start collecting, managing, and processing smart meter data. A shorter version of this plan explaining the key features in easy to understand terms should also be made public.

There should be a periodic review of the Data Privacy and Security Plan

There should be a periodic review of the plan with various details of data utilisation, intended and realised outcomes. In order to do so, independent audit into DISCOMs' processes to ascertain the prevailing standards of privacy and security and areas of improvement could be considered. The periodic evaluation should be based on criteria pre-identified by the DISCOM in consultation with data experts and approved by appropriate regulators. The audit report could also specify instances of data breaches and actions taken thereof and should be made publicly available on the DISCOM's website. While petitioning Regulatory Commissions for approval of costs of smart meter rollout programmes, DISCOMs should include the costs of ensuring data privacy and security.

2.5. Consumer rights

For a smart meter programme to be effective, the consumers should have the opportunity to gain more awareness of their own usage patterns. Therefore, in order to make it easier for the consumer to understand their usage behaviour, they should be provided with summary insights based on their CEUD at regular intervals. This information, presented in an easy to understand manner, can enable them to take decisions related to their energy consumption. It is important to consider that a majority of domestic electricity consumers are unlikely to be technologically well versed. This fact must be taken into consideration while designing appropriate mechanisms and interfaces such as consent management, data access and grievance redressal that are discussed below.

Consumers should have access to their data and insights

Consumers should be able to download their entire CEUD through appropriate mechanisms. Smart meter programme must empower electricity consumers to access and analyse their own data in whatever manner and for whatever purposes they see fit. At the data download stage, DISCOMs can provide an option to consumers to acknowledge that the consumer is aware of the privacy risk associated with sharing the same. Additionally, DISCOM should enforce strong password protection policies (e.g., password strength, multi-factor authentication etc.) and educate the consumer regarding their responsibility to maintain password confidentiality.

Consumers should be informed who their data is being shared with

DISCOMs should also inform the consumers of the frequency at which the smart meter data is collected, and how it is managed and processed. Consumers should also have access to the details of all the third parties with which the data is being shared. Any updates to this list must be consented by the consumer, especially if it falls outside the limited purposes as described earlier. DISCOMs should also make a shorter and clearer document, which summarises the key features of the *Data Privacy and Security Plan*. This will help consumers decide on consenting to third-party share requests through DISCOMs. DISCOMs should consider clubbing outreach efforts to encourage using efficient appliances and switching to smart meters with information regarding data privacy and protection.

Grievance redressal mechanisms should be set up

A well-defined grievance redressal system will help resolve consumer complaints regarding privacy and security and can help reassure consumers that their privacy is not being violated. Until the Data Privacy legislation is enacted, existing grievance redressal mechanisms should be made equipped to receive data privacy and security related grievances. Thereafter, DISCOMs have to appoint a Data Officer, who would be responsible for the same.

3. Conclusion

Given the rapid pace of smart meter installation, MoP should urgently develop such a framework in consultation with CEA, central and state regulators, DISCOMs, smart meter manufacturers, civil society organizations and other stakeholders, and publish it in the form of a white paper. MoP should also solicit wider public comments on the same. This framework can be a good starting point for the upcoming personal data regulator to deliberate with electricity regulators to evolve specific regulations. Meanwhile, it will be prudent on DISCOMs' part to understand their role as data custodians and start building internal capacity to safeguard consumer privacy in both consumer as well as DISCOM's mutual interest.

---

[1] We are grateful to our colleagues at Prayas for the rich discussions that enhanced the quality of our analysis. We also thank our colleague Srihari Dukkipati in particular for the valuable comments on the drafts. A condensed version of this article appeared in The Indian Express 21 January 2021- https://indianexpress.com/article/opinion/columns/discom-smart-meters-privacy-security-7156239/

[2] This article is part of an ongoing series called Power Perspectives, which provides brief commentaries and analysis of important developments in the Indian power sector, in various states and at the national level. The portal with all the articles can be accessed here. Comments and suggestions on the series are welcome, and can be addressed to powerperspectives@prayaspune.org

Contact us:

Prayas (Energy Group)
Unit III A & B, Devgiri,
Kothrud Industrial Area,
Joshi Railway Museum
Lane, Kothrud,
Pune 411 038 Maharashtra

020 – 2542 0720
energy@prayaspune.org
http://www.prayaspune.org/peg

Prayas (Energy Group)