POWER PERSPECTIVES

An initiative by Prayas (Energy Group)

Handling smart meter data: privacy concerns, preparedness and safeguards

February 2021

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

The landmark Supreme Court ruling upholding privacy as fundamental right has warranted a response from every sector that deals with personal data. Power sector also requires collecting and storing personal data of consumers for its efficient functioning. Further, high-resolution smart meter data too has the potential to reveal personal information of consumers such as occupancy, appliance usage patterns and even sensitive information like entertainment preferences, religious sentiments through analysis and inference. The time is right to examine provisions to safeguard private consumer data, as already about 2.1 million smart meters have been installed and are operational across the country; with another 9.1 million under deployment. As Ministry of Power (MoP) aims to replace 250 million conventional electricity meters in Indian homes with smart meters by 2022, various issues of deploying and managing such a large number of smart meters, and handling large volume of personal data becomes crucial to examine and prepare for. Furthermore, a new Personal Data protection legislation is in its final stages of becoming the law. Smart meters in the power sector have a transformational potential to alleviate DISCOM stresses, better manage grid, and improve quality of service to the consumers. Thus, it is not only prudent to examine these issues but also prepare the various actors in the sector, especially the DISCOM, towards this fast changing data regulatory space. In this article, we provide the rationale for a Smart Meter Energy Consumption Data Privacy and Security Framework to be adopted by the sector ahead of the legislation.

1. Introduction:

In 2017, the Supreme Court of India upheld privacy as an integral part of fundamental right to life, setting off the discourse on how various aspects of individual privacy is linked to administrative data. As the Indian government has repeatedly expressed its ambitious plans of replacing ordinary electricity meters in India's 250 million homes with smart meters by 2022, it is pertinent to examine the aspect of data privacy, primarily to assess the sector's preparedness. Unarguably, smart meters can be used to effectively plan distribution infrastructure, power purchase, improve billing and collection efficiencies, and offer value added services to the consumers, including time of day tariff incentives. However, smart meter energy consumption data, if used in tandem with other datasets, can reveal personal information making the consumer vulnerable to a host of illegal intrusions like surveillance, stalking, burglary, profiling, unsolicited marketing and so on[3].

World over, issues of data privacy of smart meter consumers, have been studied and fiercely debated in technical, judicial, legislative and civil society spaces[4]. At the policy level, many attempts have been made to strike a balance between the promise of operational efficiencies, and protecting data privacy while doing so. For instance, the European Union Electricity Directive was amended in 2019, to explicitly mention the requirement that smart meters must comply with the its General Data Protection Rules. In the US, California

was one of the first states to establish rules to prevent utilities from sharing smart meter data with third parties without explicit consumer consent. Today at least half of the US states have similar safeguards. As an extreme example of the perils of a mandatory smart meter programme, which did not consider consumer privacy, Netherlands saw smart grid legislations repeatedly fail to get passed without privacy provisions. Finally, as an example of judicial intervention, the Spanish Supreme Court held that energy consumption data is indeed personal data. Similar institutional arrangements to prevent and tackle privacy breaches are in place in the UK and Germany.

1.1. Indian power sector policy and regulatory context

In 2015, the Forum of Regulators (FoR) released Model Smart Grid Regulations[5], a guiding document for power sector regulators. It clearly mentioned that distribution licensees and other agencies responsible for implementation of smart grid projects should *"ensure that protection of consumer data and consumer privacy is accorded the highest levels of priority"*; the document however lacked in operational elements to ensure the same. Following this, only few State Regulatory Commissions have adopted the privacy provision in their regulations[6].

In 2016, the Central Electricity Authority (CEA), a statutory body that advises the government on technical and policy matters related to electricity, came up with '*Functional Requirements*' for Advanced Metering Infrastructure Service Providers (AMISP)[7], which provides detailed technical requirements. While the DISCOMs verbatim reproduce it in most of the smart meter implementation contracts, the functional requirements themselves do not address consumer privacy.

Finally, in 2020, MoP released the Standard Bidding Document[8] for procurement of prepaid smart meter providers, which is a detailed guiding document on various aspects of smart meter implementation including technical specifications, functional requirements and service level agreement. While this document has privacy provisions in compliance with the Information Technology Act 2000 and upcoming Personal Data Protection Bill 2019, the same is yet to translate in various DISCOMs' articles of associations with AMISPs, or are not in the public domain to examine.

Therefore, evidently, the existing instruments do not appear to pay attention to the privacy aspects of smart meter data, especially high-resolution data.

2. Changing regulatory space

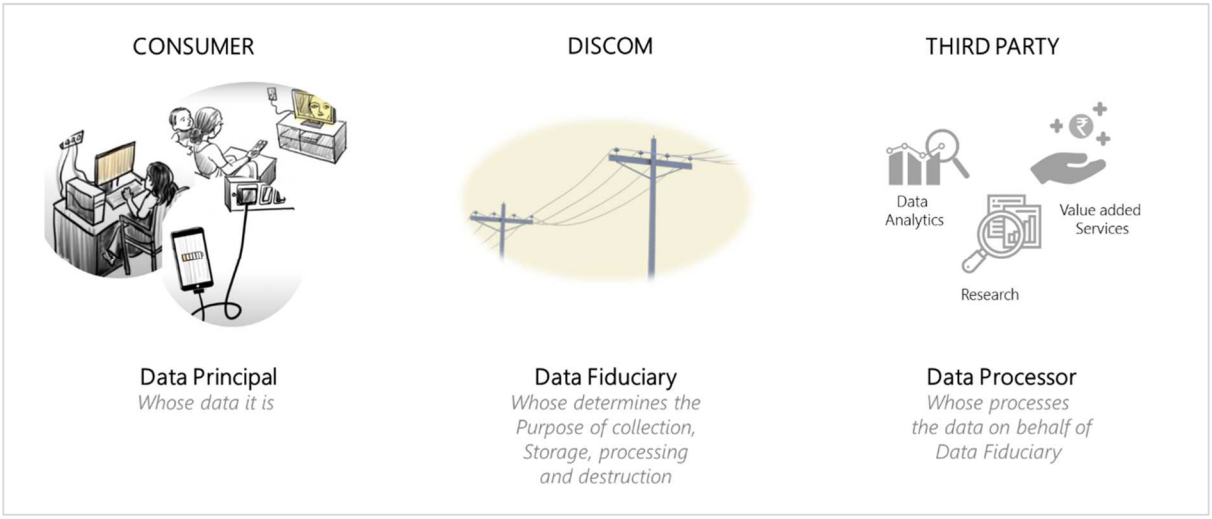
2.1. Upcoming Personal Data protection legislation

Presently, while the Information Technology Act 2000 and the "*reasonable security practices and procedures*" rules under section 43A, by definition, apply to billing data and smart meter data, many DISCOM privacy policies have applied it to only the data collected on their websites. However, these sections of the IT Act will soon be replaced by a new personal data legislation. Following the Supreme Court's privacy judgement, the Government of India tabled the Personal Data Protection Bill 2019 (PDPB) in the Parliament, in order to strike a balance between utilizing the economic value of personal data and upholding the individual's right to privacy. The bill outlines rights of the individual (data principal), whose personal data is being collected and processed, roles and responsibilities of various actors (data fiduciaries and data processors) handling personal data, as well as institutes a Data Protection Authority (DPA) to regulate personal data in all spheres.

2.2. DISCOM obligations under PDPB

The upcoming PDPB places several obligations on the 'data fiduciary', which is an entity that determines the purposes of collection, storage and processing[9] of personal data[10] vis-à-vis rights of the electricity consumer (i.e the data principal[11]). Under the PDPB, DISCOMs have the responsibility of ensuring the personal data collected follows the security and privacy standards set by the DPA. Figure 1 depicts the same. Failing to comply with the legislation and regulations of the DPA, can attract significantly high penalties (Rs. 15 Crore or up to 4% of the turnover, whichever higher). To put things in perspective, taking Uttar Pradesh's example, DISCOMs anticipate a 5-7% increase in billing efficiency and foresee a net gain of Rs. 4,056 Crore in 8 years through 40 lakh smart meter installations. However, 4% of the approved Annual Revenue Requirement (ARR) for FY18 is about Rs. 2,120 Crore; and this penalty can be levied for multiple instances over the years. Thus, even two instances of this penalty in the next 8 years would completely nullify the anticipated benefits of the smart metering programme, if adequate privacy and security safeguards are not ensured.

Figure 1: Smart Meters and Personal Data Protection Bill 2019



Source: Prayas (Energy Group)

Emerging technical methods have exposed anonymised datasets to the risk of de-anonymisation, revealing the personal details[12]. Therefore, while PDPB deals with non-anonymised personal data, it also ensures that re-identification of personal data is a punishable offence. At the DISCOM level, there will always be non-anonymised smart meter datasets, regardless of who processes it thereafter. Therefore, it puts the onus on DISCOMs to ensure that the smart meter data is not de-anonymised down the line. The PDPB indeed provides for this risk sharing by requiring DISCOMs to ensure that such third-party engagements happen through contracts that can ensure compliance with the legislation and regulations of the DPA. Table 2 and Table 3 in Annexure detail out the specific obligations and penalties PDPB places on DISCOMs and AMISPs.

As for the governance of non-personal data (NPD) i.e., anonymised smart meter data, a general NPD governance framework has been made public by the Ministry of Electronics and Information Technology[13]. As NPD governance is an evolving concept, DISCOMs need to ensure their systems are compliant with any such upcoming legislations. Since the PDPB requires DISCOMs to build capacity to tackle privacy challenges, following the obligations under PDPB–which is more likely to be the law sooner–will only further ensure that DISCOMs are better-prepared for obligations under any NPD law or policy.

2.3. Role of power sector regulators

Power sector regulators would have to play a key role in determining the specifics of DISCOM and AMISP obligations with respect to data privacy. As the sole personal data regulator in the country, DPA would have to possibly consult power sector regulators, in order to understand the specific data privacy challenges in the sector and evolve sector specific data regulations.

Smart meter programmes would not be the first instance where power sector regulators would be applying themselves on the matter of personal data sharing. In fact, in 2015, Reserve Bank of India (RBI) attempted to bring electricity and telecom regulators and credit information companies (CIC) to evolve data-sharing frameworks in order to develop credit scores for those who have not accessed credit. It wanted to do so by combining telecom and power utilities consumer billing data.

In this matter, while suggesting that state electricity regulators can come up with regulations enabling such sharing, the Forum of Regulators (FoR) opined that until sector specific laws and personal data regulations are evolved, such sharing would infringe upon consumer privacy. One can assume this regulatory stance and understanding holds for smart meter data too, which as discussed, has more potential of revealing personal details of consumers in comparison to ordinary billing data.

The lacunae in regulatory oversight over every aspect of smart meter implementation was highlighted recently in the case of automatic disconnection of supply to about 1.6 lakh smart metered consumers in UP on 12th August 2020. Uttar Pradesh Power Corporation Limited (UPPCL), in response to being fined by the UPERC for the same, stated that as far as Standards of Performance (SoPs) are concerned; there are no relevant regulations with respect to smart meters.

Indeed, in the absence of a well-defined framework, the power sector regulators would not be able to anticipate data privacy concerns, investigate such breaches and adequately hold licensees and third-party service providers accountable to electricity consumers whose privacy has been breached. On its part, the UPERC had acted swiftly with its suo-motu powers under the Electricity Act 2003 and UPERC regulation. It accepted DISCOMs' submission that 'technical malfunction' was the prima facie issue and ordered an internal investigation from the DISCOMs to find out the root cause. While ruling on this unprecedented matter, UPERC opined that *"[…] the incident has not only exposed the loopholes in the implementation of smart meter plan but has also shown a glimpse of bigger issues that may occur as the number of smart meters will increase in future."*[14] Perhaps the glimpse of bigger issues includes matters of data privacy that have largely gone unnoticed in the sector. Suffice to say that this is an alarm bell for the entire sector to thoroughly examine and prepare for various challenges in smart meter programme implementation, including data privacy.

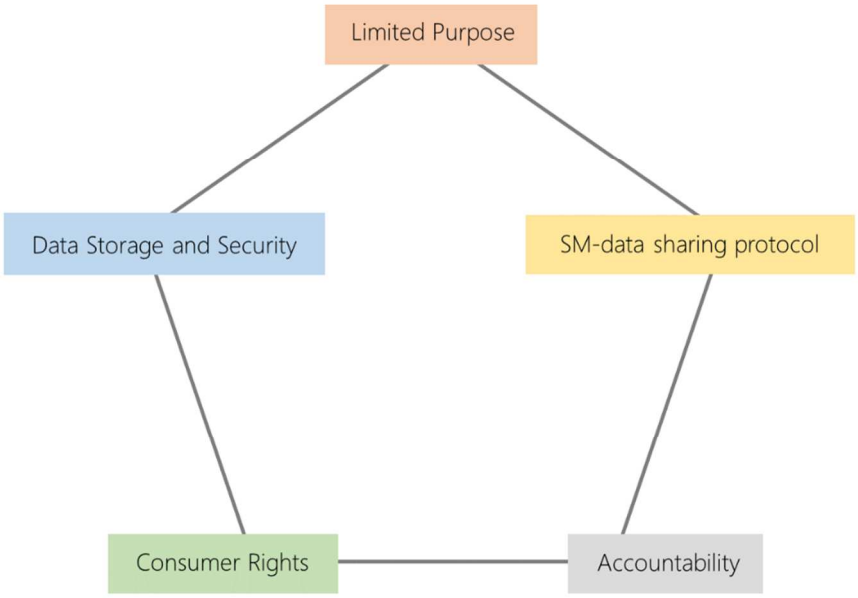
3. Data privacy and security framework

As a Joint Parliamentary Select Committee is currently examining PDPB, it is in its final stages of becoming the law. In fact, provisions akin to the PDPB have started applying to other sectors, such as public health, through the National Health Management Policy[15]. This signals the government's intent to bring in the legislation at the earliest, underscoring the need for an urgent intervention in the power sector. Other sectors dealing with personal data appear better prepared in terms of institutional frameworks. For instance, the Data Empowerment and Protection Architecture (DEPA) framework that outlines methods and institutions of data sharing and consent management among financial and telecom entities, is currently

being piloted[16]. Regardless of how DISCOMs view smart meter data, DISCOMs are constantly handling personal data.

In order for the DISCOMs to be prepared to follow DPA regulations, a comprehensive Smart Meter Energy Consumption Data Privacy and Security Framework (SMEC-DPSF) has to be in place (Figure 2).

Figure 2: 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 of collection, storage, processing and sharing. This could be done by considering various use-cases that fall under the purview of the purposes mentioned in the Electricity Act (2003) provided they do not violate privacy. The framework should define the boundaries of purposes of collection, storage and sharing that does not require explicit consumer consent.
ii. Data storage and security aspects, which clearly defines DISCOM, AMISP roles in ensuring correctness of the data stored (identifiers, for example) and having a data breach response plans to ensure that consumers are informed about security breaches
iii. Data sharing protocols, which defines roles and responsibilities of DISCOMs, AMISPs and any other third party vendors.
iv. Consumer rights and entitlements that define the level, mode and frequency of access a consumer has over their data. Ensures consumers are provided some easily accessible insights of their data. The framework should provide for grievance redressal mechanism for grievances related to smart meter data privacy and security.
v. Accountability mechanisms like 'Data privacy and Security Plan', annual reports on data breaches, grievances received and resolved, details of the data shared, benefits of such sharing etc

The onus of consultatively and deliberatively defining the parameters of privacy, security, and roles and responsibilities is on MoP, and regulatory commissions. In the next article, we will describe our proposal for a Smart Meter Energy Consumption Data Privacy and Security Framework in detail.

4. Annexure

Table 1: Summary of example privacy concerns related to Smart Meter data

Commercial uses	Targeted advertising: use of individual or aggregated household smart meter data to target advertising at a specific household or individual.
	Insurance adjusting e.g. do you tend to leave your appliances on when away from home?
Illegal uses	Burglars finding out when homes are unoccupied.
	Stalkers tracking the movements of their victims.
Use by family members and other co-inhabitants	One householder 'spying' on another e.g. parents checking if their children are sleeping or staying up late playing video games.
	Partners investigating each other's behavior.
Uses by law enforcement agencies	Detection of illegal activities e.g. sweatshops, unlicensed commercial activities, and drug production.
	Verifying defendant's claims e.g. that they were 'at home all evening'.
Uses by other parties for legal purposes	In a custody battle: do you leave your child home alone?
	In a landlord–tenant dispute: is the property over-occupied?

Source: Reproduced from- Eoghan McKenna, Ian Richardson, and Murray Thomson, "Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications," Energy Policy *41 (2012): 807–14.*

Table 2: Specific obligations and penalties on data fiduciaries and significant data fiduciaries

Clause	All Data fiduciaries	Penalty of non-compliance
7	Should give notice to Data Principal for collection/processing of personal data	Upto Rs. 15 crore or 4% of global turnover of preceding financial year whichever higher
9	Restriction on retention of personal data beyond what is necessary	
22	Should prepare privacy by design policy and get it approved by DPAI	
23 (1)	Should ensure transparency in processing personal data, and ensure information such as purpose of processing, Data Principal's rights, information on cross-border transfers etc --	
24	Ensure Security safeguards, review the same. Ensure practices like de-identification, encryption etc	
25	Should report personal data breaches to DPAI	
31	Should ensure a contract for processing by other data processors	
32	Should have a grievance redressal mechanism	
In addition to the above, Significant Data fiduciaries		
27	Should undertake data protection impact assessment	Upto Rs. 5 crore or 2% of global turnover of preceding financial year whichever higher
28	Should maintain accurate and up-to-date records, including requiring significant social media intermediaries to provide for voluntary verification mechanism.	
29	Should have their policies and conduct audited by independent data auditors.	
30	Should appoint a Data Protection Officer	

Source: Prayas (Energy Group) analysis of Personal Data Protection Bill 2019.

Table 3: Penalties that are blanket in nature

Clause	Penalties		
	All Data fiduciaries	Significant Data fiduciaries	Data processor
58	Rights of Data principal under Chapter V		
	Rs 5000/ day of default, maximum of Rs. 5 lakh	Rs 5000/ day of default, maximum of Rs. 10 lakh	NA
59	Failure to furnish report, returns, information to DPA		

	Rs 10,000/ day of default, maximum of Rs. 5 lakh	Rs 10,000/ day of default, maximum of Rs. 25 lakh	NA
60	**Failure to comply with direction of DPA**		
	Rs 25,000/ day of default, maximum of Rs. 2 crore		Rs 5000/ day of default, maximum of Rs. 50 lakh
61	**Contravention of any provision for which no separate penalty has been provided (reads as 'any person')**		
	Maximum Rs 25 lakh	Maximum Rs. 1 crore	Maximum Rs 25 lakh

Source: Prayas (Energy Group) analysis of Personal Data Protection Bill 2019.

References mentioned in footnote #4

Beckel, Christian, Leyna Sadamori, Thorsten Staake, and Silvia Santini. "Revealing Household Characteristics from Smart Meter Data." *Energy* 78 (2014): 397–410.

Brown, Marilyn A, Shan Zhou, and Majid Ahmadi. "Smart Grid Governance: An International Review of Evolving Policy Issues and Innovations." *Wiley Interdisciplinary Reviews: Energy and Environment* 7, no. 5 (2018): e290.

Cuijpers, Colette, and Bert-Jaap Koops. "Smart Metering and Privacy in Europe: Lessons from the Dutch Case." In *European Data Protection: Coming of Age*, 269–93. Springer, 2013.

Hess, David J. "Smart Meters and Public Acceptance: Comparative Analysis and Governance Implications." *Health, Risk & Society* 16, no. 3 (2014): 243–58.

Martinez, Jabier, Alejandra Ruiz, Javier Puelles, Ibon Arechalde, and Yuliya Miadzvetskaya. "Smart Grid Challenges Through the Lens of the European General Data Protection Regulation." In *Advances in Information Systems Development*, edited by Alena Siarheyeva, Chris Barry, Michael Lang, Henry Linger, and Christoph Schneider, 113–30. Cham: Springer International Publishing, 2020.

McHenry, Mark P. "Technical and Governance Considerations for Advanced Metering Infrastructure/Smart Meters: Technology, Security, Uncertainty, Costs, Benefits, and Risks." *Energy Policy* 59 (2013): 834–42.

Quinn, Elias Leake. "Smart Metering and Privacy: Existing Laws and Competing Policies." *Available at SSRN 1462285*, 2009.

Carbon Brief. "The Verdict on Smart Meter Privacy, Security and Health Concerns as UK Smart Meter Rollout Begins," July 8, 2014. https://www.carbonbrief.org/the-verdict-on-smart-meter-privacy-security-and-health-concerns-as-uk-smart-meter-rollout-begins.

Zhou, Shan, and Marilyn A Brown. "Smart Meter Deployment in Europe: A Comparative Case Study on the Impacts of National Policy Schemes." *Journal of Cleaner Production* 144 (2017): 22–32.