Privacy

Barrier Description: Privacy refers to consumer concerns about the mass collection of granular data on energy use and associated personal information. Consumers are worried about how data will be used, where the data are stored, and who can access the data.

Phase 1: *Planning of infrastructure for data handling and transmission*		**Phase 2:** *Pilot-scale implementation of privacy protection procedures*		**Phase 3:** *Wide-scale deployment of privacy protocols and data handling procedures*	
Challenges	**Practices**	**Challenges**	**Practices**	**Challenges**	**Practices**
Data on energy consumption is very sensitive: However, state of the network, generation, and consumption data are necessary for system functions [1].	🏢 🏛 **Determine the data retention period, where data is stored, and how often data is transmitted** based on the time resolution of the measurements and data type [2]. Each actor (e.g., utility company, building manager, building owner, government official) should only receive the data needed to carry out its tasks [1]. 🏛 **Enact data handling regulations** that includes data protection, data security, and data sovereignty [1].	**Smart meter data from individuals can lead to privacy and physical security concerns:** sensitive consumption data must be adequately protected [4] [5].	🏛 **Collect smart meter data via joint meter reading** to connect equipment owned by externally connected businesses and smart meters [2]. 🏢 Each actor (building owner and utility company) should receive data directly from devices when relevant [1]. **Anonymize and pseudonymize measurements** [1]. **Aggregate measurements in the SMGW** [1]. 🏢 🏛 **Aggregate metering data on a building level** that is shared by utility companies with building owners or managers [5]. 🏛 **Allow entities that are not energy service providers to access smart meter data only through an accreditation process** [6].	**Consumers worry about misuse of their data:** consumers should feel confident about data handling practices employed after the consumers agree to share their data [1].	🏢 **Create logbooks for data processing steps that are accessible by consumers** [1]. **Require** data owners (e.g., utility companies) **to gain** consumer **permissions** prior to sharing data with third-party service providers [3]. 🏢 🏛 **Require consumer facing tools to provide data only post-authentication of the user** [3].
				Certifications of some products and software require data from real-world tests: The certification process itself should adhere to appropriate privacy measures [3].	🏢 **Only transfer aggregated data to** a certification group [3].

Key Objectives

- Address consumer protection. Consumers should feel that their data is safe from misuse and unauthorized access. To achieve greater market penetration consumers must be able to trust the companies that manage their data. Government entities can reduce this current lack of trust by enacting and enforcing clear regulations on data storage, handling, and transmission.
- Use smart meter data responsibly. Smart meter data often contains very granular energy consumption information which can convey socioeconomic and occupancy information of end consumers. Smart meter data should be used responsibly with strong privacy protections in place to protect end users from social engineering, blackmail, and physical security threats.
- Protect proprietary information. Companies that feel their proprietary information is protected may be more likely to cooperate in digitalization efforts and share data essential to energy.

Description of Phases

Phase 1: *Planning of infrastructure for data handling and transmission*

Design of privacy protocols requires proper planning and coordination of data handling. Planning must be standardized and regulated to ensure that data is transmitted to the appropriate parties.

Phase 2: *Pilot-scale implementation of privacy protection procedures*

Pilot testing requires collection of individual energy consumption data, requiring concerted efforts to ensure that data is anonymized and transmitted in a secure manner.

Phase 3: *Wide-scale deployment of privacy protocols and data handling procedures*

At the large-scale level, consumers may be worried about the misuse of data. This phase often requires real-world data to appropriately certify products. At large scale, there must be particular attention to how energy certification schemes interact with individual privacy protection.

Examples cited in the report and other sources:

[1] Germany: Act on Digitalisation for the Energy Transition (Report section C.4)
[2] Japan: Next Generation Smart Meter System Study Group Summary (Report section C.5)
[3] United States: Green Button Initiative (Report sections 5.9, C.6)
[4] Privacy barrier (Report section 4.1)
[5] France overview (Report section 5.6)
[6] Japan: Electricity Business Act, https://www.meti.go.jp/english/press/index.html