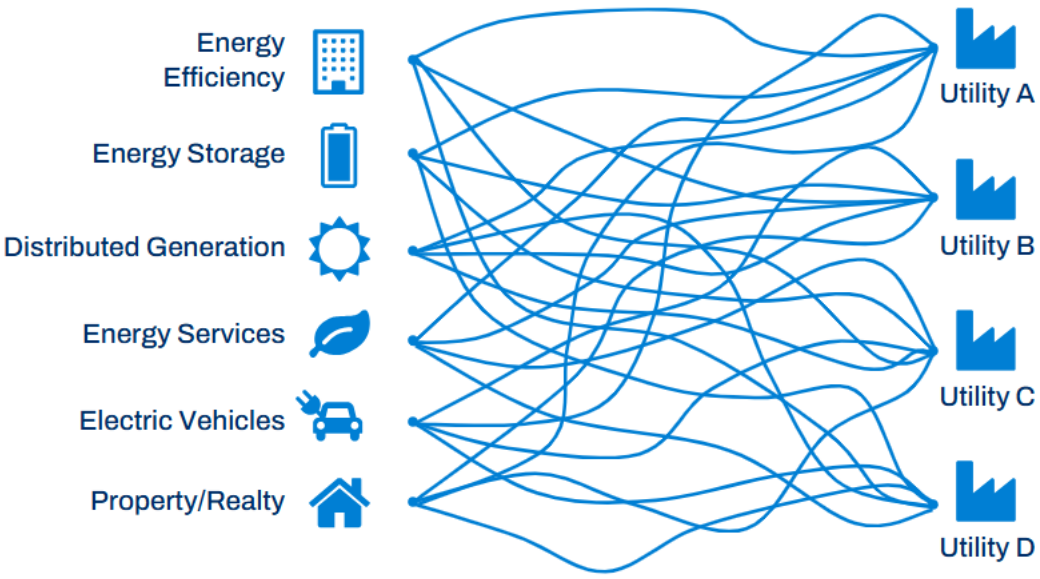
NARUC Data Access Series Webinar 2: Consent-Based Data-Sharing Summary

On August 12, 2025, NARUC CPI hosted a webinar on consent-based data-sharing. Expert speakers were: Kelly Crandall, Vice President of Regulatory and Policy, UtilityAPI; Simon Evans, Director, ARUP; Adrianne Bletz, Energy Policy Analyst, Office of Markets and Innovation New York Department of Public Service; and Nina Suetake, Deputy Director of Policy, NASUCA. The full presentation and recording are available. The following summary is a product of the NARUC Center of Partnerships and Innovation.

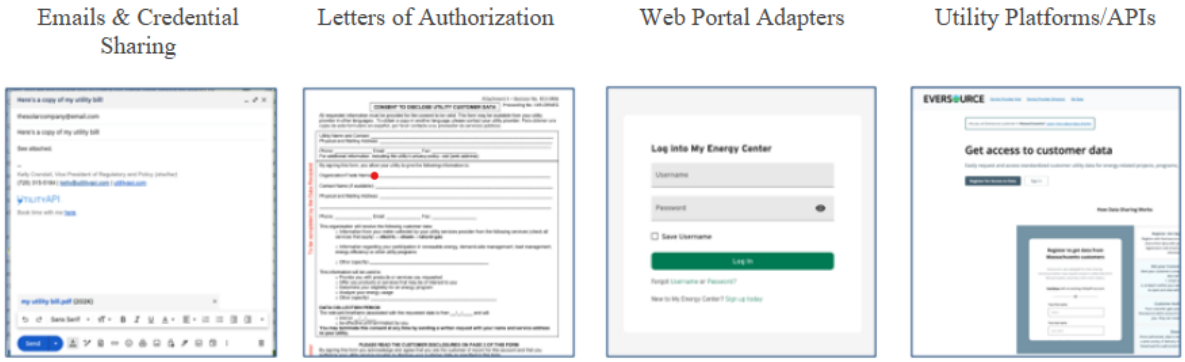
Kelly Crandall, UtilityAPI

Kelly Crandall, from UtilityAPI, a software company that enables secure, customer-authorized sharing of energy data between utilities and third-party providers, shared insights based on her prior experience as an advisor to the Colorado PUC, where data access has been a topic since 2009. She focused on situations requiring **customer consent for data sharing**, specifically energy usage data, account data, and program participation information. Crandall highlighted that most customers do not analyze their own data in spreadsheets but instead share it with platforms that perform analysis and guide next steps, such as smart thermostat companies or contractors.

Crandall noted the current reality for customers involves navigating different tools, portals, and enrollment pathways, with data access varying by state. The diagram illustrates several of these variations.

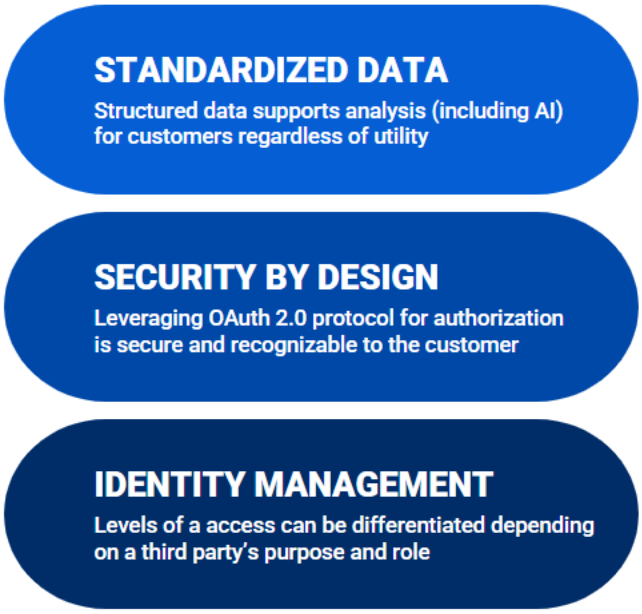


Crandall then outlined **four common data sharing** approaches, as illustrated in the graphic below.



- **Email & Credential Sharing:** Perhaps the most common approach, customers email bill PDFs or share utility account credentials with a third party.
- **Letters of Authorization:** Manual, paper-based or email forms often sent to utilities, which are typically unsecure and manual.
- **Web Portal Adapters:** A third party uses customer credentials to copy data from the utility's website, which is typically fast but can be inefficient and difficult to maintain.
- **Digital Platform/API Authorization:** This approach uses an API (software intermediary) to connect service providers with utility data vendors, allowing secure, specific data pulls from third parties after customer authorization. Crandall believes this will be a major emerging tool for energy data-sharing given its use for other common online interactions: integrating Zoom meetings with Google Calendar or paying for an eBay purchase with PayPal.

Crandall explained that key features for successful digital authorization include a **clear consent process** where customers understand what data is shared, with whom, for how long, and the ability to revoke consent. Authorization should be straightforward, using methods like passcodes via text/email instead of hard-to-find account numbers. Best practices from the software industry that make this work include using **standardized data** (like Green Button Connect for structured datasets), **security by design** (like OAuth 2.0 for embedded protocols), and **identity management** (varying access levels based on user roles).



Crandall also identified several **friction points** that hinder data sharing adoption, including:

- Third-party registration hurdles (long review processes, aggressive terms and conditions)
- Confusing, multi-step customer processes (with unclear revocation options)
- Ambiguous or unclear consent
- Manual processes and long lag times
- Incomplete datasets and coverage

She encouraged testing data tools from both customer and third-party perspectives to identify these friction points. A positive example of a smooth authorization experience is the pilot program between **Pacific Gas and Electric and Apple Home**, which Crandall describes as clear, easy, and effective.

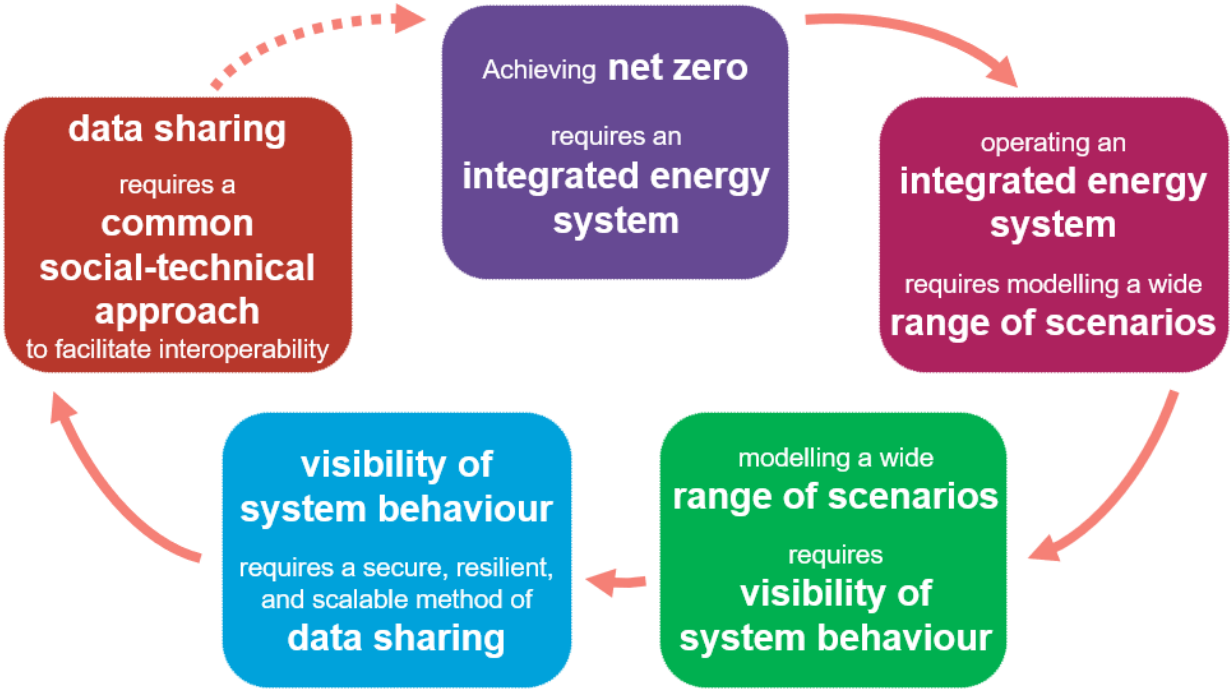
Simon Evans, ARUP

Simon Evans discussed ARUP's work on the **Data Sharing Infrastructure (previously "digital spine")** in the UK, aimed at enabling ubiquitous and frictionless data sharing across the energy sector. He noted that for nearly a decade, UK policies have called for better data sharing to address sector-level challenges, drawing inspiration from Open Banking, which fostered the fintech economy. The sector sought "machine-to-machine integration" rather than manual data exchange.

Evans emphasized that achieving any objective within the energy sector, such as net zero, requires **an integrated energy system** that can model various scenarios, which in turn necessitates visibility of system behavior, especially with distributed energy resources. This visibility intrinsically requires a **secure, resilient, and scalable method of data sharing** between participants. He stressed the importance of a **socio-technical approach**, where technical

aspects (models, taxonomies) are crucial, but the "socio side" (policy, regulatory, legal, skills, procurement) is key to success. This type of data sharing, commonly referred to as interoperability between participants, is seen as a key economic enabler for the future.

The image below displays the components of an integrated energy system:



ARUP's work concluded that data sharing is crucial for achieving net zero at the lowest cost to the consumer. This is summarized by **five points** for introducing the minimum possible solution that is socio and technical in nature, reduces costs and barriers, is secure and scalable, allows sharing of any energy sector data between any participants, and enables seamless data transfer with adjacent sectors (telecommunications, water, transport) for broader economic benefits.

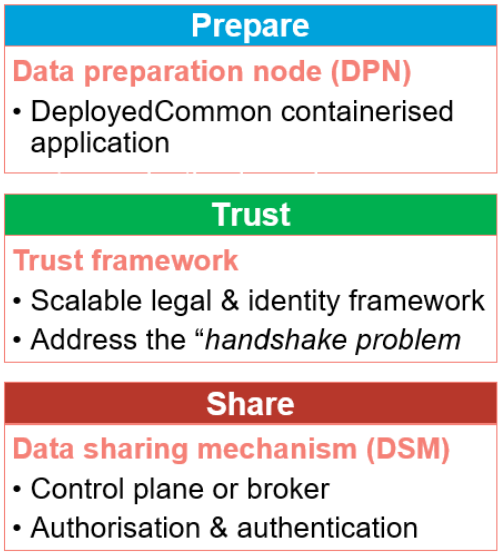
The Data Sharing Infrastructure has three components: **Prepare, Trust, and Share**

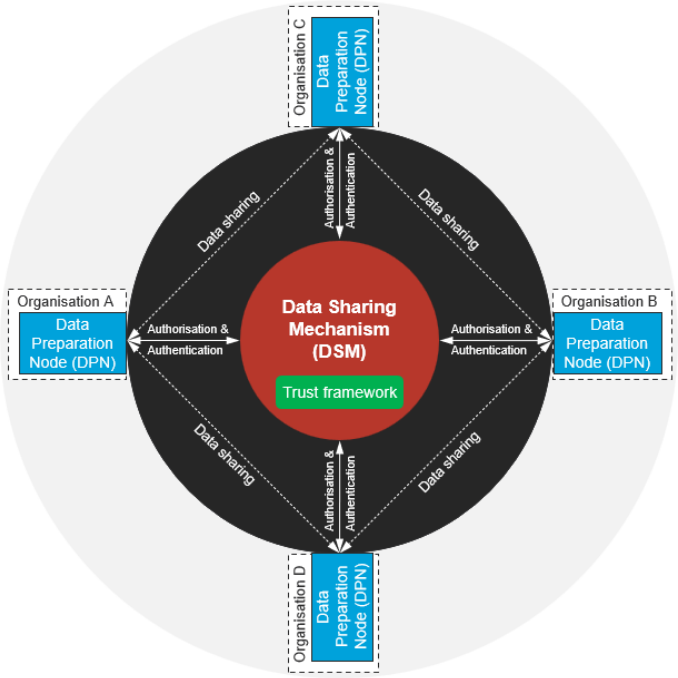
- **Prepare:** Organizations and participants deploy an open-source, containerized piece of technology at their boundary, acting as a "window into the shared ecosystem." It is designed to be thin, lightweight, opensource (free from commercial vendor influence), and allows anyone to partake.
- **Trust:** This central "control plane" or "broker" handles authorization and authentication, ensuring transactions are valid. Crucially, no data is ever stored in or passes through the middle; it is purely a broker for connectivity.
    - **Trust Framework:** Inspired by Open Banking, this provides identity management (know your customer checks) and a scalable legal framework. It

addresses the "handshake problem," where bilateral contracts for every data transaction become crippling as the number of participants grows by providing a scalable, legal framework to address this problem.

- **Share:** Participants register with the data sharing mechanism and can then search for data within a central data catalog. Permissions are scaled based on the user's role. If the transaction is valid, data is shared directly between participants through a centralized, secure channel.

See the images below for the three components of the Data Sharing Infrastructure:





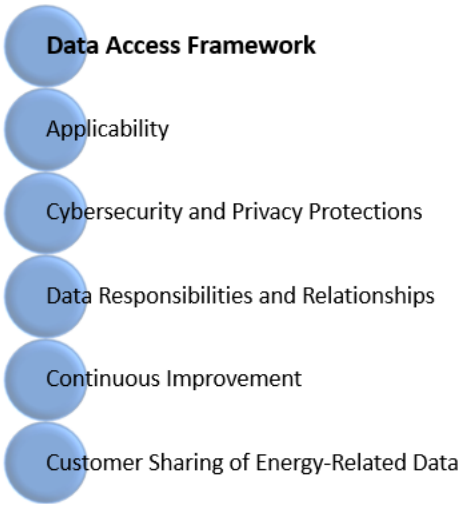
Evans noted that this concept has moved from theory to implementation in the UK, with a successful pilot led by the National Energy System Operator, which is now being rolled out to nearly every regulated participant in the country. He concluded by emphasizing the goal is to make all data **shareable**, not necessarily all data actually **shared**, and to ensure that data is shared securely and resiliently to the right participants with the right permissions. The aim is to allow participants to focus on use cases rather than core data movement infrastructure.

Adrianne Bletz, New York State Department of Public Service (NYS DPS)

Adrianne Bletz discussed New York's efforts to enable useful access to useful data to support clean energy goals, spur market innovation, and promote customer choice. She introduced New York's **Data Access Framework (DAF)**, a single, statewide set of rules for energy-related data access designed to be consistent and transparent. DAF applies to all Energy Service Entities (ESEs) requesting customer or system data from a data custodian (usually the utility, or New York's integrated energy data resource). DAF also sets clear responsibilities for data custodians,

ensuring data quality, integrity, and timely delivery. Importantly, it supports a **customer's right to access and share their own data** to make informed decisions.

See the image below for more information on the Data Access Framework:



The DAF defines cybersecurity and privacy requirements based on three factors:

- Whether the request is for **consented or unconsented data**
- The **mechanism of access** (direct connection through a utility system, secure platform, or email)
- The **type of data** requested (system, customer-level, interval usage, aggregated).

Bletz explained that even without individual customer consent, data sharing is allowed and necessary for **"valid purposes."** Examples of valid purposes include opt-out programs like community choice aggregation, benchmarking building energy use, compliance with local laws, energy planning, commission-authorized programs, or utility operational needs. For these cases, **privacy protections are mandatory**, primarily through:

- **Aggregation**: Combining data from multiple customers to prevent individual identification, typically for community or building-level energy usage totals.
- **Anonymization**: Removing personally identifying details (names, addresses, account numbers), making it highly impractical to link data to a specific customer, often achieved by aggregation of the data or using proxy IDs for customer-level data.
- **Application of Applicable Privacy screens**: Privacy screens are rules or filters to prevent identifying details from slipping through. For example, New York uses a statewide 4x50 privacy screen: at least 4 customers in the dataset, and no single customer can represent more than 50% of the total usage.

She acknowledged the balancing act between making protections restrictive enough to safeguard privacy and loose enough for data to be useful for planning and innovation.

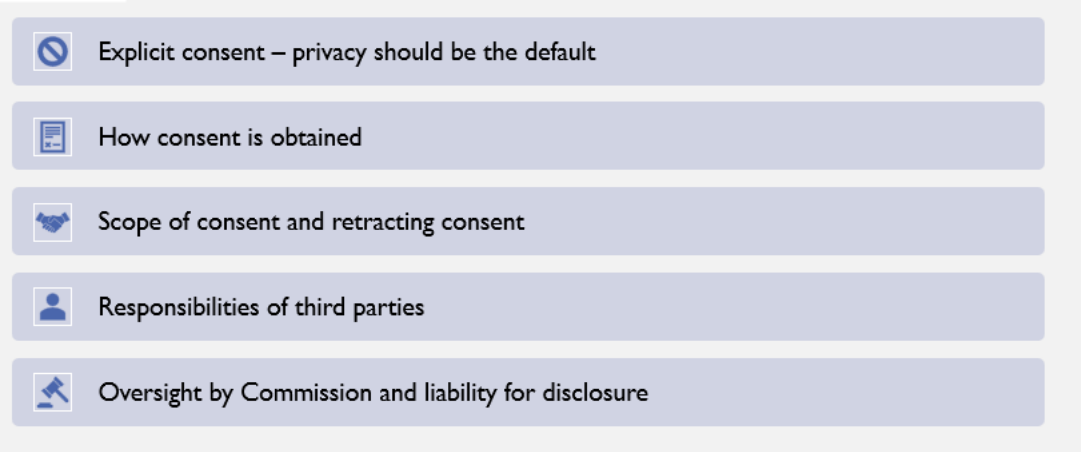
Bletz then posed **key questions regulators should ask** to strike this balance in enabling innovation and protecting customers when reviewing data access proposals:

- How will privacy and security be **verified and maintained** (e.g., ongoing monitoring, audits, breach response plans)?
- How will utility implementations be **standardized** to avoid a patchwork of rules that vary among utilities and may drive up costs?
- How will **usability and timeliness** be ensured, because some programs require timely data to provide value (e.g., demand response, real-time energy management, targeted program delivery)
- Are **aggregation and anonymization methods sufficient**, and should they be periodically revisited as technology advances?
- What **oversight exists for energy service entities** once they have the data, including accountability and consequences for misuse?
- What is the process for **customer consent and revocation**, ensuring it is easy and in plain language to build trust?

Bletz concluded by stating that by asking these questions, regulators can ensure data access works in practice, fosters innovation, supports clean energy, while protecting customer privacy and trust.

Nina Suetake, National Association of State Utility Consumer Advocates (NASUCA)

Nina Suetake, Deputy Director of Policy for NASUCA, addressed concerns of consumer advocates regarding customer data sharing, echoing many points raised by Adrianne Bletz of the New York State Department of Public Service. She emphasized that these concerns should be considered in rulemakings or when utilities propose data sharing. See the image below for a list of the key concerns regarding customer data sharing from a consumer advocate perspective:



Suetake's primary concern is **obtaining explicit consent from consumers**, asserting that privacy should be the default. NASUCA supports a framework where consumers are not required to take action to protect their privacy, favoring opt-in programs for data sharing. If an opt-out program is developed, all associated steps must be carefully considered.

She raised critical questions about **how utilities and third parties obtain consent**:

- Consent must be specific and affirmative, given only after the consumer receives complete information about the proposed data sharing.
- While written consent is the old "gold standard," digital authorization processes must be inclusive. Suetake questioned if digital-only approaches might exclude customers who are not tech-savvy or face language barriers, such as non-native English speakers or elderly individuals who rely on family for help.
- Communications must make it very clear that consent is optional for programs, and for opt-out programs, it must be explicitly clear that action is needed to opt out. All vital information should be provided in multiple languages to serve diverse customer bases.

Regarding the **scope of consent and retracting consent**, Suetake stressed that utilities must clearly inform customers about what information will be shared, how it will be used, and to whom it will be disclosed before obtaining consent. Furthermore, there must be a very clear process for customers to retract their consent, and it must be unambiguous who the customer should contact (utility or vendor). She highlighted that customers will instinctively turn to their utility, so utilities must understand the vendor's revocation process and be able to share it.

For **responsibilities of third parties**, Suetake stated they must treat consumer information in a manner that protects privacy rights, meaning limited use of that information only within the exact scope of consent given. She strongly advocated for no resale of data, even if it is aggregated and anonymized. Both third parties and utilities should be responsible for preventing unauthorized disclosure, and it must be clear in statute or rules who is ultimately responsible and who will be penalized if customer data is disclosed improperly. She expressed concern that a "trust framework" model like that presented by Simon Evans might lack clarity on ultimate responsibility from a customer's perspective, emphasizing that the customer's interest should be prioritized.

Finally, Suetake called for **ongoing oversight by commissions** to ensure clear responsibility for disclosure and protection of customer information. She cited New York's DAF framework as an interesting example of a streamlined approach that also protects consumer rights and privacy. Her ultimate takeaway is that rules must focus not just on who shares data, but on how the customer has ultimate access to their own data, controls who sees it, and can retract that consent.