# 3RD PARTIES AND BEYOND:

## PROMOTING INNOVATION THROUGH ENERGY DATA SHARING WITH "NTH" PARTIES

OCTOBER, 2019


**AUTHORS**

Klaar De Schepper

FLUX tailor

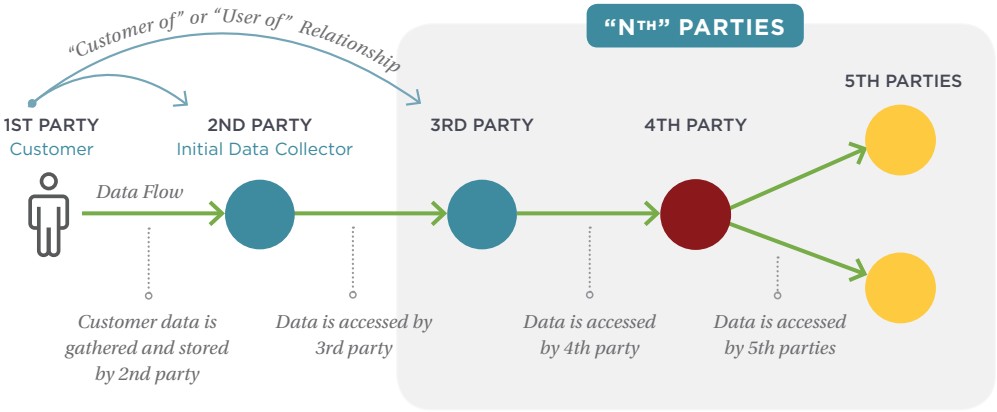
Michael Murray

MISSION DATA
empowering energy savings

# TABLE OF CONTENTS



# EXECUTIVE SUMMARY




An ecosystem of companies in the energy industry enables customers with numerous innovative products and services. When a customer shares his or her private electricity or natural gas data with a certain company, there are often several firms in a "digital supply chain" that acquire and process the data to eventually deliver services to that customer, whether the customer is aware of those entities or not. Referred to as "Nth" parties, these entities represent exciting innovations in the energy sector, but they will be stifled in the absence of thoughtful, targeted policies and customer-centric data exchange mechanisms.

First, this white paper highlights example scenarios from the energy management industry in which Nth parties are used to deliver innovative, energy-saving services to customers. Then we describe shortfalls of current state policies where overbroad prohibitions on data-sharing prevent even informed customers from exercising meaningful control over their energy data. Optimizing costs with information technology (IT) outsourcing is prevalent, especially for startups. Far-reaching privacy policies therefore have the effect of unnecessarily increasing costs to customers and stifling innovation by requiring energy management firms to "in-source" IT functions in order to avoid violating non-disclosure rules. We present a privacy model in which customer choice and sovereignty is better balanced with privacy protections by accommodating Nth parties. Finally, we conclude with a review of new technologies that can make Nth party data sharing more efficient, secure and customer-directed.

### KEY RECOMMENDATIONS

- Policy frameworks should understand and anticipate Nth parties by instituting "cascading liability" for data breaches, in which a firm is responsible for a breach caused by its downstream contractor(s), rather than rely on non-disclosure requirements, which are often unattainable in today's digital world.
- Authorization protocols should be expanded to incorporate Nth parties, machine-readable terms and conditions, "cascading authorizations," and the tracking of the customer consent "chain of command."
- Web scraping — the practice of a customer sharing his or her username and password to a utility's website with an energy management firm — can be reduced by increasing the availability of energy data, such as utility bill data, in machine readable format via application programming interfaces (API).

# INTRODUCTION

Modern customers and businesses increasingly share their private information with various companies seeking to remake energy, finance, healthcare and other sectors of the economy. For example, customers increasingly use finance "apps" to manage budgets and spending, with software aggregating transactions across the customer's financial institutions.

In the energy industry, businesses buy energy management software that accesses energy usage and cost data held by multiple electric and natural gas utilities. Customers want their information collected into a single, user-friendly application; however, accomplishing that goal requires one or more entities to "touch" private information. We refer to all of these organizations touching private information as *Nth parties* in this white paper, a term that captures *"third parties," "fourth parties"* and so on, in order to better understand the ecosystem of organizations involved.

Our overall objectives in this white paper are: (1) to demonstrate the important and legitimate role of Nth parties in energy management today; (2) to explore solutions to both policy and technical issues relating to privacy; and (3) to advance productive debate about ways to protect customers' privacy while also giving customers meaningful control over their personal data.

It is important to distinguish legitimate, customer-authorized data sharing from the unauthorized and illegitimate collection and sale of personal data. Recently highlighting the illegitimate sale of personal data is the Cambridge Analytica scandal, which caught many by surprise because it was thought that Facebook did not share its users' data with another firm — let alone a chain of multiple firms. But what makes the Cambridge Analytica incident different from other cases of data sharing in the energy or finance sectors isn't clear at first glance; after all, many customers are happy to have invisible entities analyze or process their data if they find it beneficial. We argue that what distinguishes "good" data sharing arrangements from "bad" ones is whether the data sharing is consistent with the "scope" of the customer's original authorization, and whether the manner in which the customer consented constitutes "informed consent." In other words, sharing personal information with Nth parties is legitimate only if doing so is directly related to delivering a product or service to which customers have consented.

As state and federal regulators in various sectors delve into these issues, they must better understand the commercial and legal relationships among firms today in order to distinguish good arrangements from bad ones. Toward that end, we explore a number of data sharing scenarios that occur in the energy industry today. We review the level of customer visibility and control over data sharing that occurs in the U.S. energy management industry. We also examine several states' policies that inadvertently prohibit certain data sharing practices that are desirable. Only by better understanding informed customer consent and the prevalence of outsourcing in today's digital economy can we craft better policies and technologies that ensure customers have agency over their personal information and are protected against abuse.

# WHY THIS REPORT?

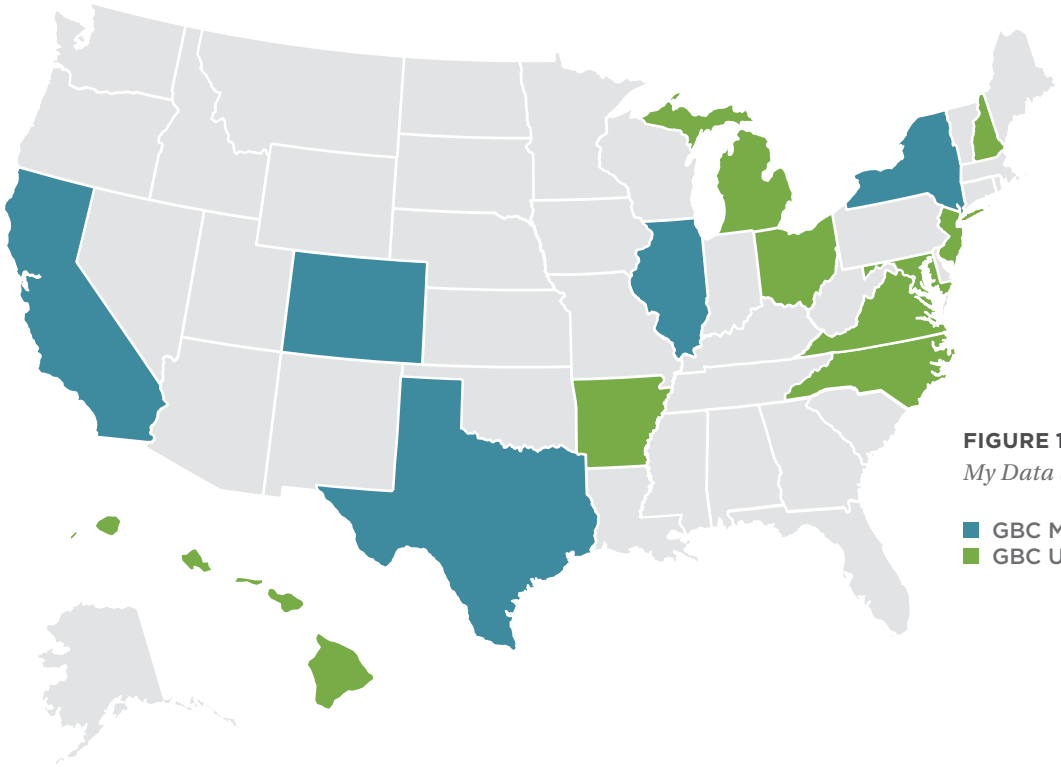



**FIGURE 1.** *Green Button Connect My Data (GBC) Across the U.S.*

Electric and gas utilities are increasingly required by state regulators to provide customer energy information (CEI) to any entity selected by the customer. CEI includes data about energy usage, costs, account details, etc. Customers might want to share their CEI with energy management firms that help lower monthly bills, or solar installers that provide price quotes for renewable energy and/or battery storage systems. Green Button Connect My Data (GBC)[1], now mandated by five states covering over 36 million electric meters nationwide, has emerged as the leading technical standard for transmitting CEI from utilities to various customer-authorized entities.

The spread of new digital services in the energy sector — such as smartphone "apps" for home energy management, and the Internet of Things (IoT) — is exciting, but many privacy rules imposed by state regulators on utilities are outdated or crudely constructed, limiting customer choice without meaningfully increasing privacy. Some states' data privacy rules cast too wide a net, indiscriminately prohibiting relationships between customers and energy management firms. For example, some utilities require energy management firms to sign non-disclosure agreements (NDAs) that effectively prohibit the use of software vendors, causing increased costs and eliminating certain products from the market. In addition, the 50-state patchwork of data security rules imposes substantial burdens on Internet-based companies who seek to do business across multiple jurisdictions. This white paper aims to assist policymakers in crafting sensible, targeted, and consistent privacy rules that do not unfairly penalize private sector innovations or digital outsourcing. We have two mantras: state policies should be as consistent as possible, and policymakers can be pro-privacy and pro-customer choice simultaneously.

Solutions lie in both policy and technical realms. Policies should acknowledge the role of digital supply chains in helping individuals and businesses manage utility bills and lower

1 See http://www.greenbuttondata.org

their carbon footprint. Instead of blanket prohibitions on data sharing, disclosures of CEI with Nth parties should be permitted when necessary to provide a service that a customer knowingly consented to use. This requires bringing customers' wishes into privacy frameworks. Currently, many privacy laws or rules focus exclusively on *restricting* access to data, not permitting it. On the technical side, well-designed permissioning systems that provide customers with a clear view of their data authorizations, including the ability to revoke access, are essential to putting customers in control of their data. Energy management firms should also review the cybersecurity practices of their vendors in order to take full responsibility for any "downstream" privacy risks.

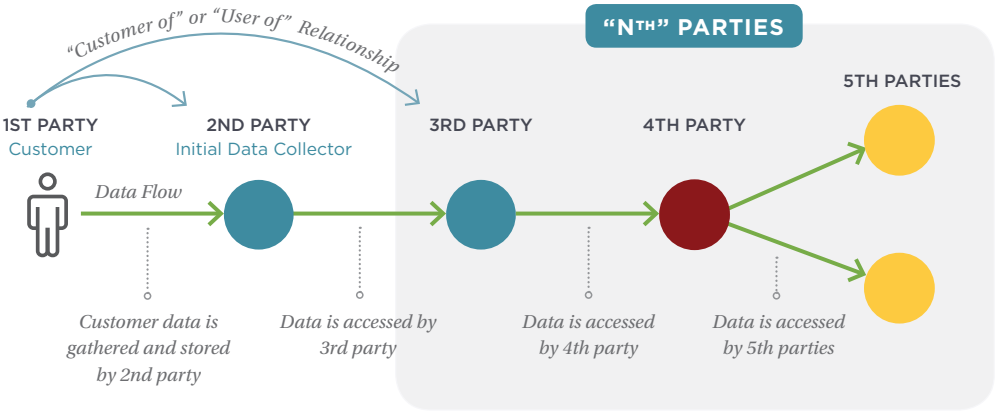
But before delving into solutions, we must first clearly define what is meant by "Nth parties." Distinguishing legitimate, customer-directed data sharing from illegitimate data sharing is central to crafting sound policy. Then we examine policy solutions, recommending targeted language that permits data sharing under certain limited conditions. Finally, we examine technological solutions that give customers meaningful control over their data held by electric or gas utilities and significantly reduce the risk of unauthorized access.

## WHAT ARE NTH PARTIES?

An Nth party collects or manages certain data on behalf of another entity that serves a customer. Diagrammatically, Nth party data access can be described as a directed graph with 3+n "nodes" connected by data sharing "links," as demonstrated in Figure 1.[2] We order the parties involved in data sharing by data flow and start by counting the customer as the first party. A "customer" can refer to an individual or an organization. The customer's electric distribution utility, bank, social network, or other entity that initially collects and subsequently shares the customer's data with Nth parties is counted as the 2nd party.

Nth parties are any parties starting with the 3rd party that access private customer data held by a 2nd party (see the grey circle in Figure 1). The green arrows signify data flows, whereas blue arrows denote a contractual "customer of" or "user of" relationship. These figures will be used throughout this paper to describe a number of Nth Party data sharing scenarios. Note that in the example in Figure 1, there is no direct relationship between the customer and the 4th party or 5th party. As we explain later on, Nth parties need not have a direct customer relationship themselves and are often invisible to customers.

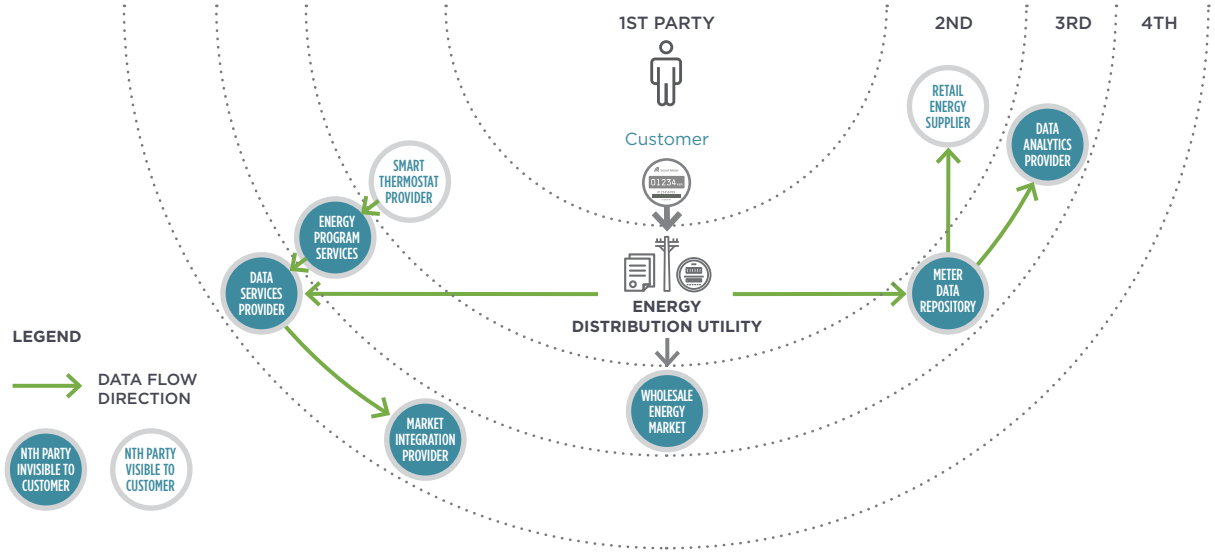
**FIGURE 2.** *Nth Party data sharing scenario diagram template*




2 Wikipedia: Directed graph: https://en.wikipedia.org/wiki/Directed_graph

The classification of a party can be made either on the basis of data flow (see Figure 2) or their distance to the customer in terms of contractual relationship (see Figure 3). For example, retail electric providers (REPs) in states such as Texas have a direct relationship with customers, and therefore could be seen as a 2nd party if one orders entities based upon contractual relationships emanating from the customer. Alternatively, REPs in Texas could be classified as 3rd parties because they receive data from a distribution utility (or even as 4th parties because REPs access data from a 3rd party smart meter data repository). Both approaches to classification are valid, and each is useful for understanding the nature of these complex relationships. Since we are focused on data access in this white paper, we order entities by data flow in the diagrams that follow in Figures 4-7. Again, we refer to any 3rd party or beyond as an Nth party.

**FIGURE 3.** *Nth Party data sharing relationships visualized by contractual distance from the customer*

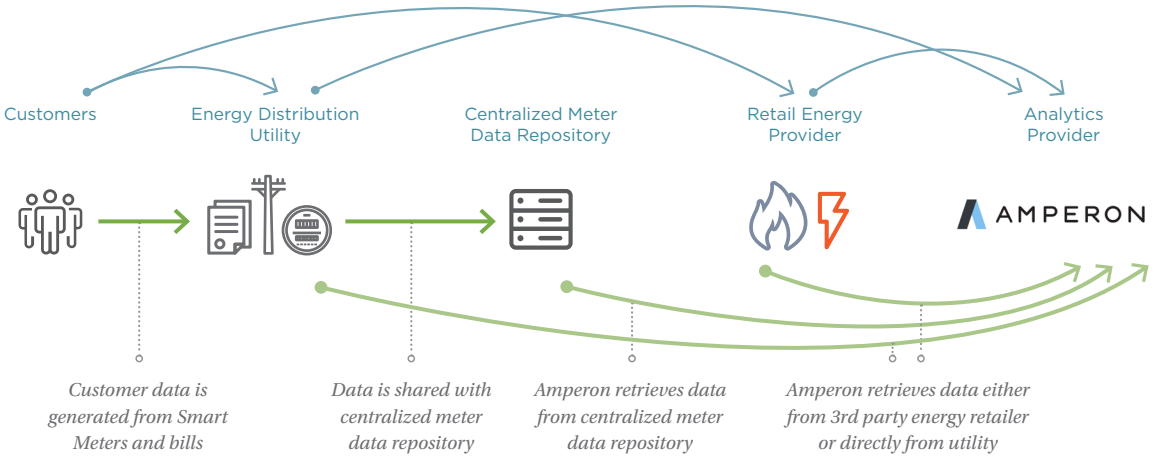



# NTH PARTY SCENARIOS AND STATE POLICIES

### ENERGY INDUSTRY EXAMPLES OF NTH PARTIES

Energy management companies need access to customer data held by an electric or gas utility in order to operate. These companies — for example, bill payment services for commercial or multifamily properties, or energy management software firms — wish to serve a national market. The U.S. has approximately 3,500 retail electric utilities, making development of a consistent, nationwide energy management offering particularly challenging. As a result, some energy management companies limit their target market to certain utility territories, while others, seeking a larger opportunity, might contract with an "aggregator" in order to acquire energy usage and billing information from various utilities. Before explaining aggregators in detail, let us begin with a simpler example in which a firm serves REPs to reduce energy costs.

**FIGURE 4.** *Amperon Data Access Scenarios*




### *Smart Meter Analytics Provider — Amperon*

Amperon is a data intelligence company for distribution utilities and REPs. Amperon uses meter data from advanced metering infrastructure (AMI) and artificial intelligence (AI) to lower energy costs by more accurately predicting price and demand spikes in wholesale electricity markets. In Texas, interval usage data in 15-minute intervals can be accessed from the Smart Meter Texas repository. In other territories, Amperon could also access interval usage data from the REP, or the distribution utility, as shown in the green arrows. In any case, Amperon is an Nth party. The customer is unaware of Amperon, but Amperon is helping reduce the customer's monthly bills by helping the utility or REP save money on its wholesale power purchasing.

### *Energy Management Specialist and Energy Star Portfolio Manager Benchmarking*

For a slightly more complex example, consider Figure 5, which describes a scenario commonly seen among energy management specialists. In this case, both energy usage data and utility bill data is used to assess energy efficiency upgrades in commercial or multifamily

**FIGURE 5.** *Energy Management Specialist, Data Aggregator, and EnergyStar benchmarking for commercial or multifamily buildings*

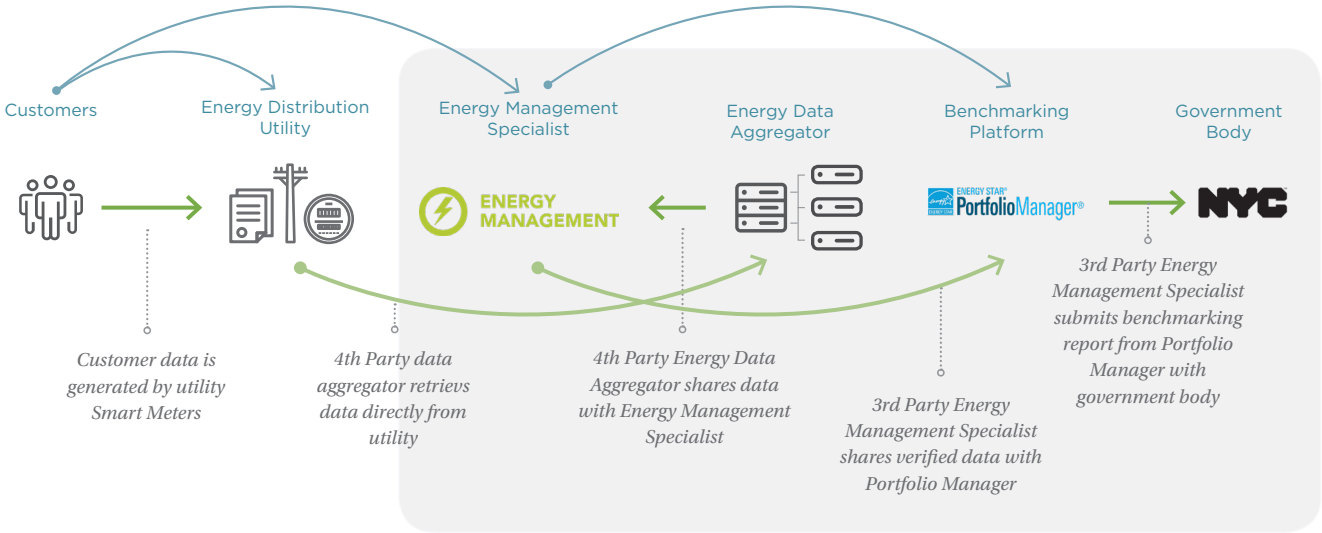
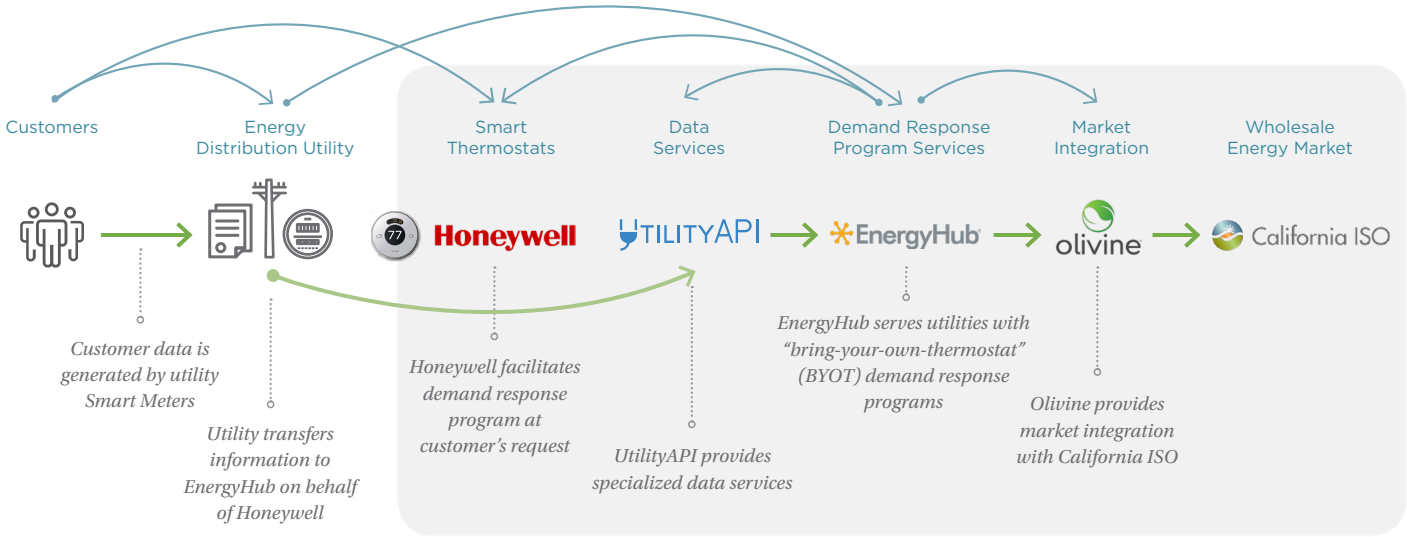


**FIGURE 6.** *Demand Response Nth Party Data Sharing in California*




buildings. The Energy Management Specialist engages a data aggregator with the customer's authorization to acquire electricity and natural gas usage information either through Green Button Connect, or from the utility's website. As described later on, customer-authorized web scraping is often the only automated way for Nth parties to retrieve utility bill data. Another common use of utility bill data retrieved by utility data aggregator services is bill payment across portfolios of properties that span different utility territories. The "Energy Management Specialist," as we call it, also combines bill data with aggregate whole building energy usage data to help the building owner attain an EnergyStar score, which is then transmitted to a municipal government (such as New York City) in order to comply with local benchmarking and disclosure laws. The customer may or may not have a pre-established relationship with EnergyStar.

### *Demand Response Scenario — California*

When considering a demand response program that involves smart thermostats, the CEI-sharing relationships become considerably more complex. From the customer's perspective, she is simply paid $50 by the electric utility in order to control her thermostat a few hours during the summer months; she would have no reason to be aware of the intricacies of the network of specialist firms operating in the background that process her $50 payment. See Figure 5 for a hypothetical scenario involving multiple firms. Note that these scenarios contain hypothetical business relationships and are not intended to reflect actual contracts between, or endorsements of, any of the entities mentioned.

In this scenario in California, the customer is aware of Honeywell, a thermostat maker, and the Electric Utility. But several other entities are unknown to the customer: EnergyHub is a provider of "bring your own thermostat" software and programs for electric utilities; UtilityAPI specializes in acquiring CEI (with customer permission) from electric utilities across the U.S.; and Olivine is a specialist in wholesale electricity market integration, facilitating the financial settlements of demand response events at the California Independent System Operator (CAISO). The reason for the number of Nth parties in this scenario is simple: Each entity has a business need that can be more cost-effectively satisfied through outsourcing. Ultimately, in order for the customer to receive $50, her CEI must be sent to CAISO for settlement. Although this is a hypothetical example, it is plausible set of relationships that ensures CEI is properly transmitted to CAISO.

## EXAMPLES OF STATE PRIVACY RULES AND PRACTICES

Previously, we established that Nth party relationships in the energy sector are common and can help achieve customer-directed goals such as managing energy costs and reducing greenhouse gas emissions in cost-effective ways. Let us now turn to specific state privacy rules and practices that inhibit the development of such relationships. Whether due to poor drafting, misunderstanding of the prevalence of outsourcing or other reasons, some state rules governing electric and natural gas utilities prohibit data sharing with Nth parties, even when the customer knowingly gives permission for such sharing. In other cases, the absence of explicit state policies regarding Nth parties has led utilities to require non-disclosure agreements that prohibit the utilization of Nth parties. Although well-intentioned, such practices create unnecessary obstacles for energy management services.

### *Illinois: Confusion About Disclosure*

In 2014, the Illinois Commerce Commission (ICC), which regulates electric and natural gas utilities in the state, initiated a formal proceeding regarding an "Open Data Access Framework" as proposed by Citizens' Utility Board and Environmental Defense Fund. In a 2016 order, the ICC made two determinations concerning its data privacy rules that appear to conflict with one another. First, the ICC said that "third parties" — the term used by the ICC for energy management firms, solar installers, and the like — may disclose CEI to their contracted vendors or affiliates as long as such disclosure conforms with the customer-authorized purpose. This determination would appear to support the notion of Nth party data-sharing, so long as it is consistent with the product's or service's purpose, to which the customer agrees. However, in the same order, the ICC declared that third parties are not permitted to "sell or license" CEI "to any other party for any purpose."[3] This latter conclusion by the ICC has been seen by some in the industry as a prohibition on data management firms selling their services to energy management or rooftop solar companies.

Although the ICC's two statements did not appear to be in conflict to the ICC at the time, the order's language has become an obstacle due to the development of the energy management market in the past decade. Initially, many energy management firms expected to interact directly with a utility's information technology (IT) systems such as GBC. However, many of these firms realized it was difficult and/or costly to do so. Specialized data aggregators such as UtilityAPI, Urjanet and WattzOn emerged that charge distributed energy resources (DERs) a fee for collecting CEI electronically from utilities. By tailoring their software to each utility's web-based interfaces and covering a large number of utilities nationwide, these specialists began offering DERs a cost-effective alternative.

Unfortunately, cost-saving data aggregators are threatened by the uncertainty created by the ICC's order. Perceived as a prohibition against using contractors, distributed energy firms must "in-source" rather than out-source their CEI-gathering functions. The first effect of mandatory in-sourcing is increased costs, which are probably passed on to customers in the form of higher fees. The costs of compulsory in-sourcing are hard to quantify, but they are not trivial. Maintaining API connections with utilities throughout version changes and glitches can be expensive, as Mission:data detailed in a recent report.[4] Furthermore, the ICC's order could drive innovative firms out of Illinois altogether, eliminating choices for customers.

### *New York: Non-Disclosure Agreements*

As part of the state's wide-ranging Reforming the Energy Vision (REV) initiative, the New York Public Service Commission (PSC) required electric utilities with advanced metering infrastructure to provide Green Button Connect My Data (GBC). However, the "Joint Utilities"

3 Illinois Commerce Commission, Docket No. 15-0073. Final Order dated March 23, 2016. Available at https://www.icc.illinois.gov/docket/files.aspx?no=15-0073&docId=240497

4 *Energy Data Portability: Assessing Utility Performance and Preventing "Evil Nudges."* Mission:data Coalition, January, 2019. Available at http://www.missiondata.io/reports/

of New York (including Consolidated Edison, Central Hudson Gas & Electric, National Grid, New York State Electric & Gas and Rochester Gas & Electric) recently instituted a requirement that GBC users must sign a "Data Security Agreement." The Data Security Agreement contains non-disclosure provisions that make it challenging for energy management firms to outsource CEI collection to specialized software firms, even with customer knowledge and consent. For example, specialized software firms acting on behalf of energy management companies are very broadly defined in the Data Security Agreement, appearing to encompass cloud hosting firms such as Amazon Web Services and Microsoft Azure, or even Internet Service Providers (ISPs) who carry CEI over their networks. However, the likelihood that Amazon, Microsoft or ISPs will sign such agreements is near zero.

Requiring Data Security Agreements from all entities that "touch" CEI — even cloud computing providers and ISPs — is a rejection of a much simpler, "flow-down" model of liability in which an entity is contractually responsible for the acts of its contractors. Not only is New York's practice unnecessary and cumbersome, but its inclusion of cloud computing providers and ISPs makes it impossible to execute in practice.

### VISIBLE AND INVISIBLE NTH PARTIES

Nth parties can take many forms. Sometimes they are invisible to customers, as when a small, regional bank outsources its online portal to a contractor, unbeknownst to customers. Other times, Nth parties might appear to customers online with a notice such as "this service is provided to you by…."

In the case of invisible Nth parties, authorization for data sharing to these entities is often included in terms and conditions. For instance, life insurance companies might have terms and conditions that state, "We will share your personal information with our partners solely for the purposes of providing you with life insurance." Those "partners" — such as the insurance company's consultants, medical clinics or re-insurance providers — do not have a direct relationship with the customer, and their identities are often not disclosed. Similarly, many financial services firms — particularly smartphone apps — contract with financial data "aggregators" that invisibly access customer financial information from banks. Several of the Nth parties in the energy data sharing scenarios featured in this white paper are similarly invisible to customers.

In cases where Nth parties are not visible to customers, we must make a key distinction between legitimate and illegitimate sharing: namely, what is the *purpose* of Nth party data-sharing? Does it directly serve the customer's interests, and is it necessary for the product or service to function? Or does the data sharing serve only the Nth party's business interests, with data being sold or traded between organizations for profit by taking advantage of customers? The line between legitimate and illegitimate use of private data can sometimes be blurry, but often it is clear enough. For example, when a financial institution contracts with an Nth party fraud prevention service, customers generally understand it is the financial institution's duty to protect the customer's money, and such data-sharing serves a legitimate purpose. However, if the financial institution sells private transaction data to hedge funds simply to make a profit, most customers will view that practice as illegitimate.

If customers were to simply have greater awareness of Nth parties, would they make better decisions? Policymakers have asked this question before. The desire to enforce good behavior among market actors with the threat of reputational damage stemming from a data breach is in part the motivation behind many state policies requiring websites to post a privacy policy. In practice, however, good behavior is rarely enforced by customers choosing with their wallets or web browsers after carefully reading online privacy policies; the cognitive burden is simply too onerous. However, technical and policy solutions can be effective in informing customers and giving them choices without requiring a detailed review of privacy policies for each authorized Nth party. We explain how in the sections that follow.

# POLICY SOLUTIONS

Previously, we explained that it's becoming common for energy management businesses to outsource certain IT functions to specialists in order to focus on their core strengths. Given the large number of Nth parties involved in delivering many online services, we now turn to the question of how policy can limit the risks of data breaches to customers without banning outsourcing altogether.

In our experience, it is all too easy for regulators to draft rules with crude oversimplifications: A customer wishes to share their information with a single entity — and that's that. One-to-one relationships between customer and service provider certainly simplify roles and responsibilities, but the commercial reality is more complex. Modern privacy frameworks must also address liability among a large potential number of Nth parties. Who should be responsible for making the customer whole if an Nth party, somewhere in a chain of vendors, has a security breach? Privacy frameworks must also address when and how Nth parties must be disclosed to customers in order to secure their informed consent.

In addition to building in support for Nth parties, policies should require increased technical standardization across utilities with "privacy-by-design" web services. Part of the reason for the proliferation of Nth parties in the energy management industry is that utilities across the U.S. each have their own level and type of data access, from paper bills and spreadsheets to manually-signed letters of authorization (LOA), each providing different datasets. If an energy management firm needs its customers' utility bill data electronically from a number of different utilities, the firm has virtually no choice but to obtain such data through web scraping due to the differences in datasets and authorization processes. Improving the availability of all types of energy data — including bill data — through secure, standards-based APIs across all utilities would improve security and reduce the need for web scraping. This is explained further in the Technology Solutions section.

### POLICY FRAMEWORKS SHOULD ADDRESS NTH PARTIES

Since many U.S. privacy regulations don't even mention Nth parties, the first challenge is deciding what regulation applies to which entity. Untangling existing privacy regulations should begin with a common terminology to describe the various roles and responsibilities involved in handling energy data.

The European Union's General Data Protection Regulation (GDPR) has a helpful vocabulary that defines two roles with different responsibilities: the *Data Processor* and *Data Controller*.[5] The *Data Controller* is the party that decides on processing activities, whether or not it actually carries out the processing operations itself. A *Data Processor* is an entity contracted by the controller for carrying out the processing. The *Data Controller* is responsible for ensuring that customers have given informed consent for data. If a processor acts outside the scope of authority granted by a controller — for example, by acting as a controller by making data sharing decisions of its own — then GDPR treats the processor as a controller, and the processor becomes subject to the same rules as controllers.[6,7]

Regardless of the terms used, policies should first recognize a *chain* of entities receiving customer data, rather than merely a single entity.

### CUSTOMER-CENTRIC DATA PRIVACY POLICIES

A successful data privacy policy will focus not only on restricting access to personal information but also on articulating the conditions under which it may be transferred. Ensuring that such conditions are reasonable

5 What is a Data Controller or a Data Processor? European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

6 Top 10 operational impacts of the GDPR: Part 7 - Vendor Management - International Association of Privacy Professionals (IAPP). https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management

7 While offering clarity through for example this terminology, GDPR is considered overly prohibitive by some, and organizations are still struggling to implement its requirements. See, e.g., *The 10 Problems of the GDPR*. Roslyn Layton, American Enterprise Institute. Statement before the Senate Judiciary Committee. https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf

and reflect the actual wishes of the customer requires parsing the somewhat nebulous concept of "informed consent."[8] For guidance on this topic, we first recommend that policymakers review DataGuard. Developed by the Department of Energy for the energy management industry, DataGuard describes best practices for informed customer consent, customer control over data, cybersecurity risk management, and how data should be processed and maintained at rest.[9]

As for informed consent, we specifically recommend the following requirements for the sharing of CEI:

1. **Purpose specification.** A purpose statement — ideally a single sentence — is essential to informing customers. Purposes must: (a) never be excessively broad — for example, "any lawful purpose" would be an overreach; (b) explicitly mention if data will be used for marketing purposes of any kind; and (c) not be pre-approved or policed by utilities or state regulators (in order to promote innovation and customer choice, state regulators should limit their involvement only to cases in which a purpose statement is excessively broad, deceptive or illegal).
2. **A simple, clear, and accessible user experience using visual queues.** Rather than use multiple pages of text containing difficult-to-understand legal terms, customers should be presented with simple, concise explanations of how their data will be used. Ideally, these should contain iconography to represent the types of information to be shared. To minimize the cognitive burden on customers, the authorization language should be presented on a single "screen" (whether a web page or mobile device applications), use graphics intelligently, and be accessible for people with disabilities per section 508 standards. Ideally, various icons would be tested on a representative group to see which visual explanations are best understood.
3. **Revocation instructions.** A clear explanation of how to revoke access. Whatever method the customer used to initiate an authorization should also be available for the customer to revoke access.
4. **Avenues of redress.** Finally, an online customer authorization experience should include a description of a complaint process and different avenues the customer may pursue with state or federal law enforcement.

### CALIFORNIA: A POSITIVE MODEL FOR LIABILITY ALLOCATION

One state that has thoughtfully addressed Nth party relationships is the California Public Utilities Commission (CPUC). In its 2011 privacy ruling (D.11-07-056), the CPUC both knowingly incorporated Nth parties into the rule as well as established a chain of responsibility among data recipients:

> Section 6(c)(3): *Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances*. When a covered entity discloses covered information to a third party under this subsection 6(c), it shall specify by contract, unless otherwise ordered by the Commission, that it shall be considered a material breach if the third party engages in a pattern or practice of accessing, storing, using or disclosing the covered information in violation of the third party's contractual obligations to handle the covered information under policies no less protective than those under which the covered entity from which the covered information was initially derived operates in compliance with this rule.[10]

A "covered entity" includes energy management firms selected by customers. Any entity — including Nth party vendors to an energy management firm — that holds 11 or more customers' energy information is considered a

8 For an in-depth discussion of informed consent, see *A Critical Question Lost in the Facebook Story: What is Informed Consent?* Michael Murray and Klaar De Schepper. http://www.missiondata.io/news/2018/4/23/a-critical-question-lost-in-the-facebook-story-what-is-informed-consent

9 *DataGuard Energy Data Privacy Program: Voluntary Code of Conduct Final Concepts and Principles.* :https://www.dataguardprivacyprogram.org/downloads/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf

10 California Public Utilities Commission. Decision D.11-07-056, July, 2011. Attachment D, p. 8-9. http://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/GRAPHICS/140370.PDF

covered entity.[11]

For companies, putting this into practice requires taking a regular inventory of all the entities with whom data is shared. The first step in reducing the risk of breaches is for entities to inventory all of their contractors' data-management practices.[12] Inventory should be taken of both contractors and contractors' contractors. There should be a systematic and regular review of the security and privacy practices of both third parties and those of their contractors and vendors.

# TECHNOLOGY SOLUTIONS

Below, we discuss six (6) technology solutions that can improve delegation and access management challenges associated with Nth party data sharing, especially where Nth parties are invisible. These solutions are focused on Customer Energy Information (CEI) made available through the Green Button Connect My Data (GBC) standard but are generally applicable to other data exchange standards and scenarios.

### UPDATE MECHANISMS FOR CUSTOMER CONSENT TO ALLOW FOR CASCADING AUTHORIZATIONS

As mentioned previously, utilities and policymakers have often assumed that only one entity will need to access a customer's private data, with direct permission from a customer. A scenario in which the party that needs to access customer data has no direct relationship with the customer, but has been contracted to access the data by an organization that does, is not envisioned. This incomplete understanding of real-world data-sharing scenarios is also reflected in the technical configuration of most data exchange systems, including Green Button Connect; only one entity can be authorized to access data at a time, and neither the authorization nor the permission to authorize access can be passed on from one entity to another.

This challenge exists in all of our example scenarios. In the Energy Management Specialist example in Figure 5, a customer contracts with an Energy Management Specialist and authorizes the Energy Management Specialist to access CEI. The Energy Management Specialist, in turn, contracts with a data aggregator to acquire the CEI on its behalf. Let's say that the CEI is made available via a GBC-based API. In the current GBC standard, there is no way for the Energy Management Specialist to pass on its GBC authorization to the data aggregator. As a result, the data aggregator requests GBC authorization directly from customers, and the Green Button Connect process doesn't involve the party with whom the customer has a direct contract. To put it mildly, this is confusing for customers. If the customer is a multifamily or commercial real estate owner and sells or acquires properties, data access for these assets needs to be managed. While this process is facilitated by the Energy Management Specialist as part of their service, there currently isn't a technical way for the Energy Management Specialist to revoke or grant Green Button Connect access.

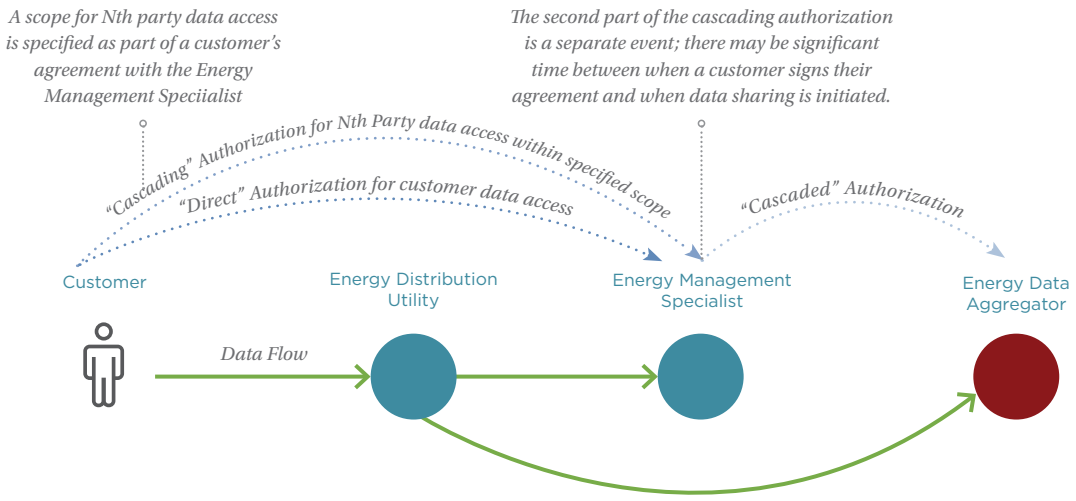
One solution would be to involve all parties in the authorization process by establishing a technical mechanism for customers to delegate data access permissioning rights to the Energy Management Specialist. This could be accomplished,when customers sign their initial agreement with the service. This solution, which we call "cascading authorizations," is illustrated in Figure 7.

The mechanism for "cascading authorizations" could allow customers to explicitly delegate permission for an Energy Management Specialist to grant its own authorizations to

11 The threshold of 11 customers was determined as a compromise in order to avoid criminalizing individuals who manage utility accounts on behalf of family members. It was thought that rarely, if ever, would an individual manage utility accounts (such as bill payment and online account access) for more than 10 family members at once.

12 *Data Risk in the Third-Party Ecosystem Second Annual Study* (2017). https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/sep2017/cs2017_0340.pdf

**FIGURE 7.** *Concept diagram for "Cascading Authorization"*



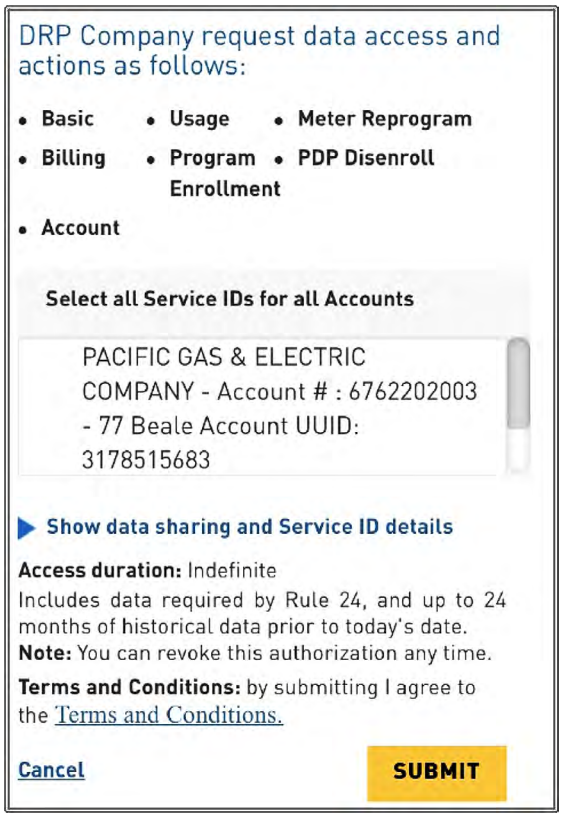




**FIGURE 8.** *Example of PG&E authorization popup that appears for a customer to give "DRP Company" access to customer data using Green Button Connect.*

downstream Nth parties on the customer's behalf. What distinguishes the concept of cascading authorizations from current practices is that the customer sets data access authorization preferences once with the Energy Management Specialist, rather than having to act each time a downstream entity requests authorization. Furthermore, this solution provides a technical mechanism for the customer to be aware of downstream Nth parties and to revoke their access if needed.

To give an example of a cascading authorization, consider a Pacific Gas & Electric implementation of GBC that customers use to authorize data-sharing with a demand response provider (DRP). The authorization screen in Figure 8 is presented to the customer. If the demand response provider writes its own software, and thus there are no Nth parties involved, then the authorization screen will say "DRP Company requests data access and actions as follows," as shown in Figure 8. If, however, the demand response provider contracts with a data aggregator, then, if state policies require customer assent to a named data recipient prior to transfer, the authorization screen in Figure 8 would need to be amended to read "Data Aggregator XYZ, on behalf of Energy Management Specialist, requests data access and actions as follows…" Now imagine if multiple data aggregators were involved — or data aggregators' contractors, their contractors' contractors, and so on. The notice quickly

**FIGURE 9A.** *Current Green Button Connect OAuth 2.0 authorization and registration with separate Nth Party OAuth Client Ids A, B, and C for each Energy Management Specialist, but no OAuth Client ID for the Data Aggregator. Authorization is facilitated by the Nth Party Data Aggregator.*

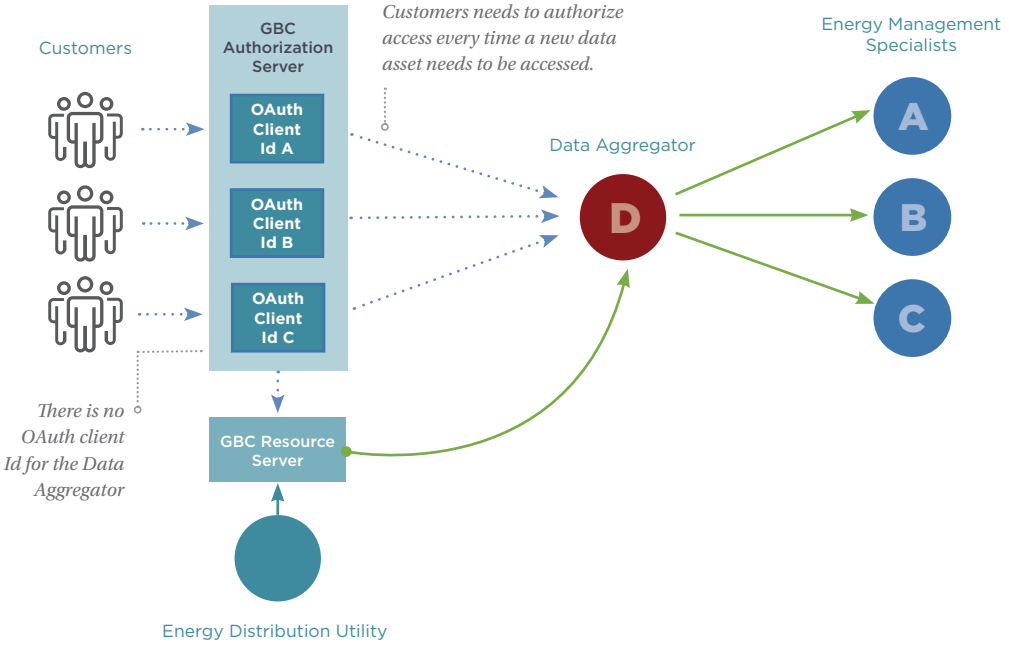
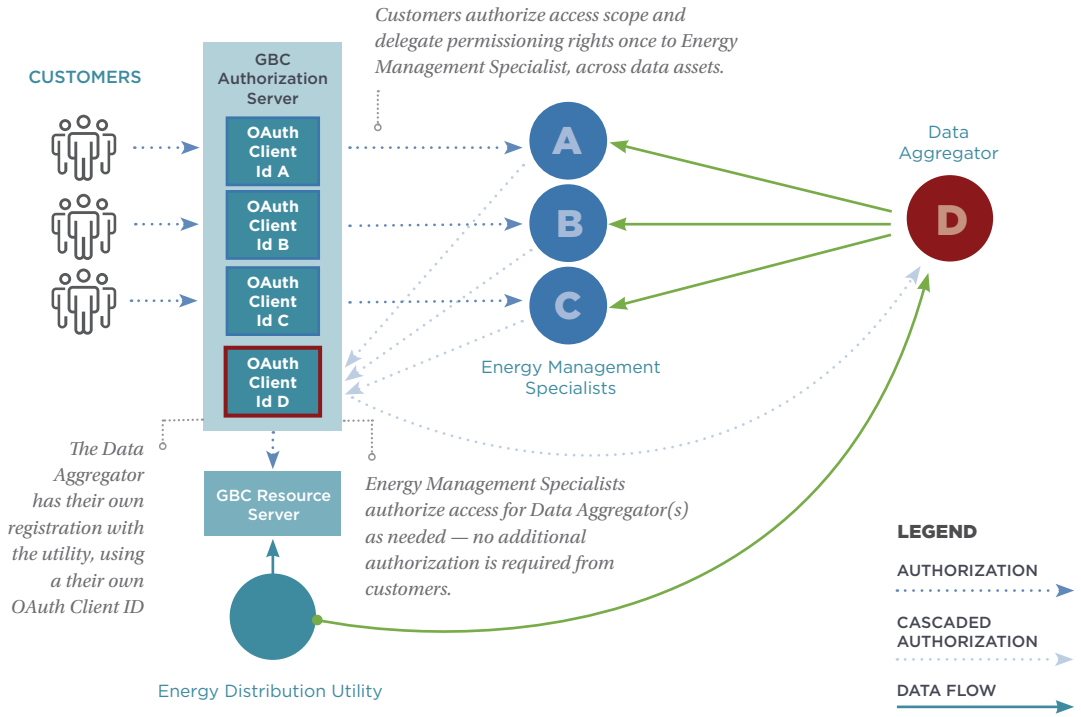



**FIGURE 9B.** *Concept diagram for "Cascading" Green Button Connect OAuth 2.0 authorization. Authorization is facilitated by the Energy Management Specialists, using their OAuth Client Ids A, B, and C. Customers delegate permissioning rights to Energy Management Specialists, who pass on access rights to a Data Aggregator as needed to access data using their own OAuth Client id D.*



becomes unwieldy and confusing to customers. Customers are required to explicitly authorize data access each time a new Nth party is contracted by the demand response provider to retrieve data for a usage point.

The GBC standard permits authorization only to the entity that registered in advance with the utility. Currently, data aggregators either register separate GBC registrations with a utility for each of their clients, or their clients reference the data aggregator's resources in their registration. Either way, on a technical level, the data aggregator does not hold its own registration, and SSL certificates are digitally "signed" by only one entity, so not everyone in the chain of command is tracked.

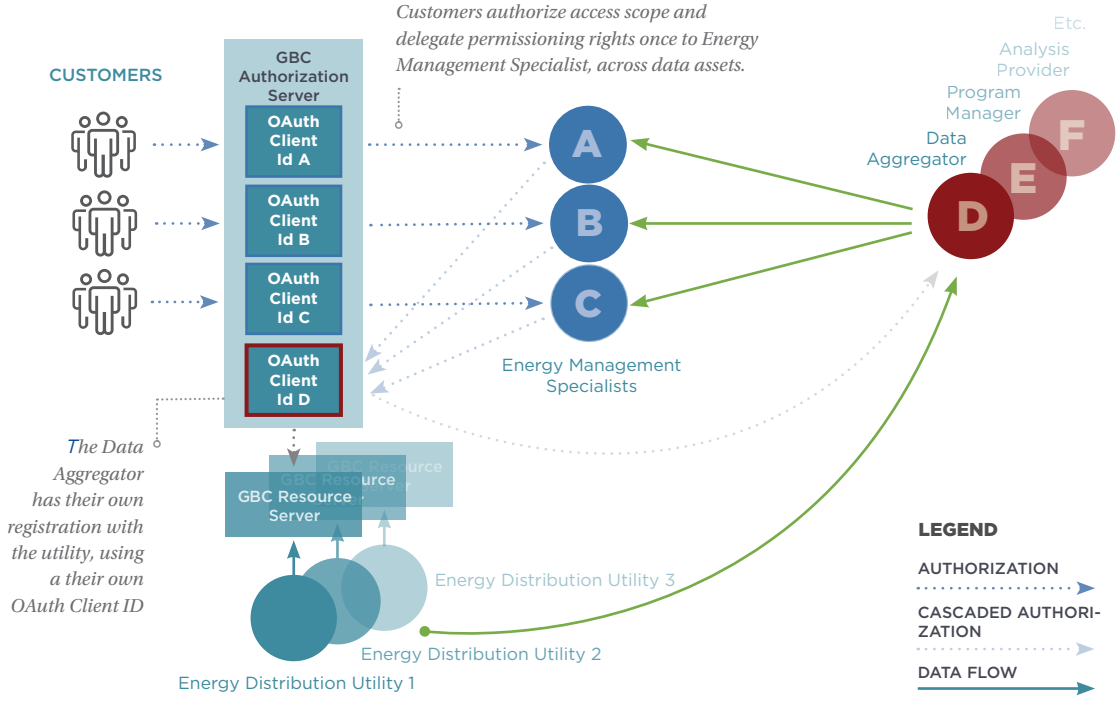
Additionally, the authorization process is initiated by the data aggregator, which can be confusing to customers. Figure 9a shows a data aggregator serving multiple clients. There is a separate "OAuth Client ID" — a reference to the OAuth 2.0 authorization standard — for each energy management specialist but not one for the data aggregator. An energy management specialist who wants to grant access to several Nth parties has to be registered separately for each Nth party. The volume of separate registrations for each data aggregator-customer combination can introduce administrative burdens on utilities.

Figure 9b shows a proposed alternative in which all Nth parties, both energy management specialists and data aggregators, are registered with the utility as participants in the OAuth process. Authorization can, at the customer's direction, "cascade" from an initial Nth Party to other Nth parties, such that these Nth parties can take on data retrieval or processing tasks — as long as it is within the scope authorized by the customer. This affords customers the ability to have visibility into which authorizations were granted by which Nth parties to which Nth parties. In addition, distribution utilities have a reliable audit trail to ensure that only data sharing consistent with the customer's specified scope has occurred.

### ESTABLISH SHARED AUTHENTICATION AND REGISTRATION FOR NTH PARTY DATA ACCESS

Currently, Nth parties such as distributed energy resource (DER) providers and data aggregators register separately with each utility. The U.S.

**FIGURE 9C.** *Concept diagram for "Cascading" Green Button Connect OAuth 2.0 authorization with a central authorization server. Customers can manage data access across providers and utility territories.*



has over 3,500 electric distribution utilities; significant efficiencies could be gained from registering Nth parties centrally, rather than at each utility. A common platform for Nth party registration would lower barriers to entry for DERs, decrease time-to-launch for innovative projects, and avoid redundant administrative activities. To realize this, an independent entity could be created that centralizes customer identification and Nth party registration.

As an extension of centralized registration, the centralized authorization server described in Figure 9C could further extend the platform provided by the independent entity. An existing example of a platform that allows for centralized cross-territory data access authorization is EPA EnergyStar Portfolio Manager. A group of New York utilities, supported by Indigo Advisory and Flux Tailor, has explored centralized data sharing registration and authorization as part of an evaluation of use cases for potential blockchain technology applications in shared infrastructure.[13]

### SUPPORT AUTOMATED ACCESS TO BILL DATA

An increasing number of utilities have implemented Green Button Connect-based API access to consumption data, but complete cost data is often not made available. Besides web scraping, the options for automated access to utility bill data are very limited. One option for energy management firms, often mentioned by utilities, is to use Electronic Data Interchange (EDI). EDI is a file-deposit data exchange system introduced in the 1990s that was designed for exchanging customer data with retail energy providers (REPs). But the problems with EDI are numerous: customer consent is entirely absent in EDI transactions; schemas and protocols differ widely between utilities; and encryption in transit using HTTPS is not required. EDI is not practical for innovative energy management companies that serve customers across the

13 New York Utilities: We Believe Blockchain Is 'Transformative':https://www.greentechmedia.com/articles/read/utilities-and-blockchain

### WHAT IS WEB SCRAPING?

Web scraping is a method of extracting large amounts of information from websites. It is used widely and across industries, sometimes with publicly accessible websites, but also by using a customer's login credentials (username and password) for a customer's online account. Nth parties like energy management specialists, bill pay companies, and data aggregators leverage web scraping software to extract data from online accounts and downloaded PDF bills.

### DATA PRIVACY

**Usernames and passwords are exposed:** Best practice in the web scraping industry is to encrypt credentials, but even with encryption there are often still weak spots in the process where credentials may be accessible in plain text.

**Utilities lack visibility:** The only thing identifying a scraper is its IP address, and frequently companies use cloud services with dynamic IP addresses, so it is hard to trace their origin.

**Unnecessary Data and Functionality Exposure:** Customer login credentials give access to full user functionality, including the ability to start or stop utility service and access possibly sensitive customer account information. This may be much broader than what customers want to delegate. On their part, Nth parties prefer to limit their risk exposure by limiting data collection to only the information necessary to deliver their service.

### WORKFLOW EFFICIENCY

**IT problems:** While under development, web scrapers can result in highly repetitive requests, increasing traffic loads.

**Customer usernames and passwords are not a reliable access method:** When a customer changes login information, access is interrupted, and the updated information has to be passed along the chain of parties involved.

**Multi Factor Authentication:** Utility account portals increasingly require multi factor authentication (MFA) to log in. The most common example of MFA is when the website texts a one-time passcode to the user's mobile phone. MFA can be a barrier to web scraping, as the entity logging in cannot directly verify the identity of the party that authorized data access, and it forces the customer to be online at the time of access.

U.S. In the absence of alternatives, web scraping of utility bill images is thus the only practical way for energy management firms to automate access to their customers' utility bill data. Until a better alternative exists for automated utility bill data retrieval, web scraping will remain prevalent.

Utilities should work towards making bill data available through more reliable and standardized channels. Eventually, a standard schema for machine-readable utility bill data could eliminate the need for web scraping techniques altogether. Achieving this will take some time; meanwhile, however, utility bill images could be made available via a web service, with URLs linking to encrypted utility bill images in a standards-based API gateway such as GBC. Nth parties could request authorization from customers to retrieve bill images through the web service and retrieve them within the customer authorized scope, just as they would receive other energy information via Green Button Connect. Existing mechanisms for automatically extracting data from the bill images can then be used to make the data machine-readable.[14]

### IMPLEMENT VENDOR RELATIONSHIP MANAGEMENT AND PROVIDE TRANSPARENCY

"Vendor Relationship Management" (VRM) is the vendor-centric equivalent of "Customer Relationship Management" (CRM). Companies that access private information need to reliably track which users authorized different levels of data sharing, and what data was shared with each vendor. If a contract between a company and its vendor ends, all customer data records should be deleted. Additionally, when an end customer revokes access for any reason, customer data shared with Nth parties should be deleted as well.

The introduction of the GDPR has had widespread implications on vendor oversight in Europe. Websites (*Data Controllers*) are required to expose with which entities they share data (*Data Processors*) and for what purpose.[15] In response, systems for vendor registration and tracking are being offered by major firms in the EU and innovative solutions using blockchain for tracking authorizations and data-sharing events are being explored as a possible solution.[16] While vendor tracking has been prompted by regulations in Europe, VRM is still nascent for U.S. companies.

As for the level of transparency that firms should be required to provide about their vendors' access to private data, we propose that firms should be required to list the types of entities with whom they share customer data and the purpose of data sharing. This is consistent with the California Consumer Privacy Act, which requires firms to disclose categories of Nth parties with whom data is shared, but not individual firms, which could change frequently.[17] The goal is to increase transparency while avoiding undue administrative overhead.

### STANDARDIZE CONSENT PROCESSES WITH MACHINE-READABLE TERMS

Open standards are needed not just to promote automation and interoperability but to help customers choose services that align with their privacy goals by having web browsers automatically enforce access to services that comply with the customer's stated aims. Customers should be able to broadcast, in standardized schemas, what data they are willing to share, for how long, who can access it, whether those entities may share it with others, and for what purpose. Standardized protocols are under development at various international industry venues. A working group at the International Standards Organization is developing guidelines for online notice-based consent,[18] and IEEE features a working group for

14 Flux Tailor is working with organizations interested in supporting automated access to bill data and has introduced the concept of incorporating bill images in the Green Button standards working group. Reach out to utilitybilldata@fluxtailor.com for more information.

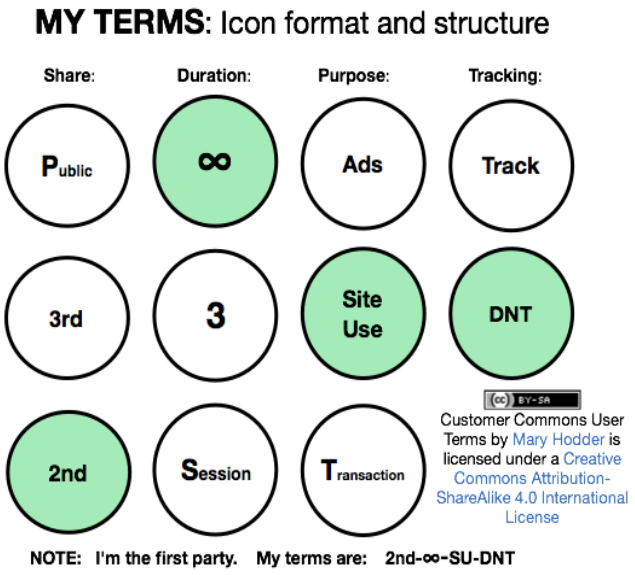
15 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

16 See, e.g., Onik, M. M. H. et al. (2019). *Privacy-Aware Blockchain for Personal Data Sharing and Tracking*. Open Computer Science. Walter de Gruyter GmbH, 9(1), pp. 80–91. doi: 10.1515/comp-2019-0005. Neisse, R., Steri, G. and Nai-Fovino, I. (2017). *A Blockchain-based Approach for Data Accountability and Provenance Tracking*. http://arxiv.org/abs/1706.04507

17 California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

18 ISO/IEC DIS 29184 Online Privacy Notices and Consent: https://www.iso.org/standard/70331.html

**FIGURE 10.** *Iconographic representation of Customer Commons User Terms*




machine-readable privacy terms.[19]

The Kantara Initiative is taking an innovative approach to standardizing user-directed preferences with User Managed Access (UMA). UMA, like GBC, is built on top of OAuth 2.0, and UMA uses machine-readable licenses to enable users to grant access to data. UMA is user-centric in that it gives customers the ability to leverage an authorization server to manage access to their various resources, regardless of where the resources reside. Like GBC, access is determined by predefined settings, and customers do not need to be present online at the time that an Nth party requests data access.[20] UMA is different from GBC in that customers can provide instructions to a service provider to grant access to other service providers using the same OAuth Authorization Server. Related to UMA is ongoing work on "consent receipt," a standard for what could be described as a reverse cookie: both the individual and the organization have a record of the consent, and the individual can use the receipt to track and profile the organization and/or service along with consent and information sharing preferences.[21]

### ENABLE CUSTOMER-CENTRIC DATA SHARING

Not only should customers be able to view their data-sharing agreements, but they should also have agency over their preferences in order to establish mutually beneficial agreements with Nth parties. As envisioned in the UMA protocol, more centralized authorization would allow customers to proactively review and control their data privacy preferences. Here are two initiatives that promote this model of customer-centric data sharing:

The **Me2B Alliance** certifies products and services to ensure that they (and their suppliers) are helping and not harming customers with data management practices, and that customers have an active role in setting up fair agreements.[22] Similarly, **Customer Commons** is modeled after Creative Commons, which developed more flexible alternatives to copyright for artistic work.[23] The goal is to create terms and conditions by which individuals control how their information is used by companies, rather than submitting to company-generated terms and conditions. Customer Commons' is currently focused on enabling users to control whether their user behavior is tracked by third parties to customize ads. The icons in Figure 10 were recently proposed. Customers can proactively "broadcast" their intent and data privacy preferences to organizations that may want to have business relationships or otherwise use customer data. In the energy industry, this "intent-casting" concept could translate into customers' proactive sharing of anonymized utility meter data for certain research purposes.[24]

19 P7012 - Standard for Machine Readable Personal Privacy Terms: https://standards.ieee.org/project/7012.html
20 User Managed Access Protocol - Kantara Initiative: https://kantarainitiative.org/confluence/display/uma
21 Consent Receipt Specification - Kantara Initiative: https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification
22 Me2B Alliance: https://www.me2b.us
23 Customer Commons: http://customercommons.org
24 See, e.g., ecobee's "Donate My Data" initiative: https://www.ecobee.com/donateyourdata

# CONCLUSION

The scenarios illustrating the sharing of customer energy information (CEI) in this white paper highlight just a few variations of circumstances in which Nth parties help deliver innovative energy solutions to customers. Specialized Nth party services — whether visible or invisible to customers — help companies focus on their core business, thereby shortening on-ramp times to new markets, providing geographic scalability and offering advanced analysis.

In the absence of a national U.S. data privacy law, states have filled the void. But state-specific regulations have sometimes been impractical and overly restrictive, limiting customers' ability to share their own data with any service provider of their choice. Poorly drafted policies have created unnecessary barriers for innovative startup companies in the energy management industry.

There are several promising avenues that can further empower energy customers. Existing data sharing standards like Green Button Connect could be expanded to allow for customer authorization to "cascade" to other parties, and to include bill images. Terms of use could be digitized so customers can control access differentially and have visibility and control over who has access to their data. Unlocking data access with privacy-by-design principles will promote "Me2B" and business-to-business relationships that are mutually beneficial and help us reach greenhouse gas emission reduction targets.

Finally, we would like to issue a call for cross-sector collaboration. Despite many differences, there is nevertheless considerable overlap between the energy, finance and healthcare sectors: the healthcare industry is developing data sharing principles and standards for authentication, consent and data transfer of sensitive patient information in the U.S., and the fintech sector is developing solutions to Open Banking in the United Kingdom and the Payment Services Directive 2 (PSD2) regulations in Europe. We look forward to collaborating with our colleagues in these industries to collectively solve the challenges discussed in this white paper.

# ABOUT US

MISSION:DATA
empowering energy savings

Mission:data Coalition is a non-profit coalition of 35+ innovative technology companies that empower customers with access to their own energy usage data. Mission:data advocates for modern, customer-friendly, standards-based data portability policies throughout the country, with the objective of achieving zero marginal cost data access to support a vibrant market for energy management services. See missiondata.io

FLUX tailor

Flux Tailor provides information management expertise in utility data exchange to software developers, utilities, data acquisition companies, and Distributed Energy Resource (DER) Solution Providers. The consulting company supports software implementation projects and facilitates multi-stakeholder research and development processes. Flux Tailor regularly engages in public service commission proceedings and data standards working groups to support the implementation and development of open data standards such as Green Button Connect. See fluxtailor.com

AMPERON

Amperon builds best-in-class, AI-powered electricity demand forecasts derived from high-resolution AMI data to enable lower electricity procurement costs and ensure grid stability for energy suppliers, utilities, and grid operators. Founded in 2017 by a former energy trader and a veteran data engineer, Amperon has customers throughout North America and Australia. Amperon's mission is to usher in a more sustainable, reliable, and efficient energy future by reigning in grid volatility through smart meter data analytics. See: amperon.co

# ACKNOWLEDGEMENTS

We would like to express our appreciation Daniel Roesler from UtilityAPI, Sean Grimes from LO3, and Jonah Bossewitch for their valuable and constructive remarks. We offer special thanks to Eve Maler, chair of the User-Managed Access (UMA) work group, for her generous intellectual exchange and for answering our technical questions about how "cascading authorizations" work in UMA.

# QUESTIONS?

**nthparties@fluxtailor.com**