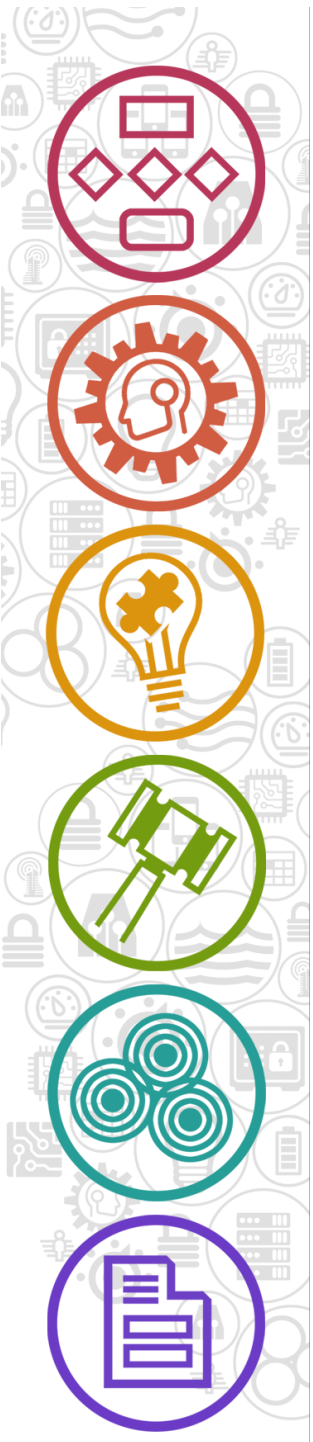


White Paper

A Modern Data Ownership Framework

- based on a model that includes :

A. Data Originator

B. Primary Data Ownership

C. Co-Owners

D. Enabled Parties

By Ron Rock, Michael Moran and Ron Thompson

A Modern Data Ownership Framework

Executive Summary

Data is increasingly subject to ownership confusion – from individuals, companies, industries, and countries – and this confusion is acting as a barrier to the $1 trillion data marketplace that is emerging as this decade draws to a close. Competent, compliant data sharing unlocks this barrier. Realizing the new value that data sharing unleashes through new revenue streams, transformed business models, operational efficiencies, and more, we first need to embrace a modern scalable data ownership framework. With such a framework in place, global data marts can thrive and create the foundation of a new data driven economy. The founders of Microshare have spent a good portion of our careers answering the question: "How do I securely share the right data, with the right entity, at the right time, with complete control, compliance and auditability?" This white paper will introduce you to our 21st Century Data Ownership Framework, an approach for how to recognize who/what owns the data, who sets the rules of who can access/edit the data, how to enforce the rules, and how data can be shared and monetized downstream with complete control. We will define and articulate that for each piece of individual data, there are a Data Originator, a Primary Owner, Co-Owners, and Enabled Parties. In addition to our framework, we introduce the notion of the Digital Ombudsman (DO), a trusted broker and enforcer of data ownership rules and conflict resolution. Finally, with ownership clearly defined and the DO in place, our Microshare product allows data ingestion, annotation, storage and sharing at scale to realize the Trillion Dollar data market opportunity.

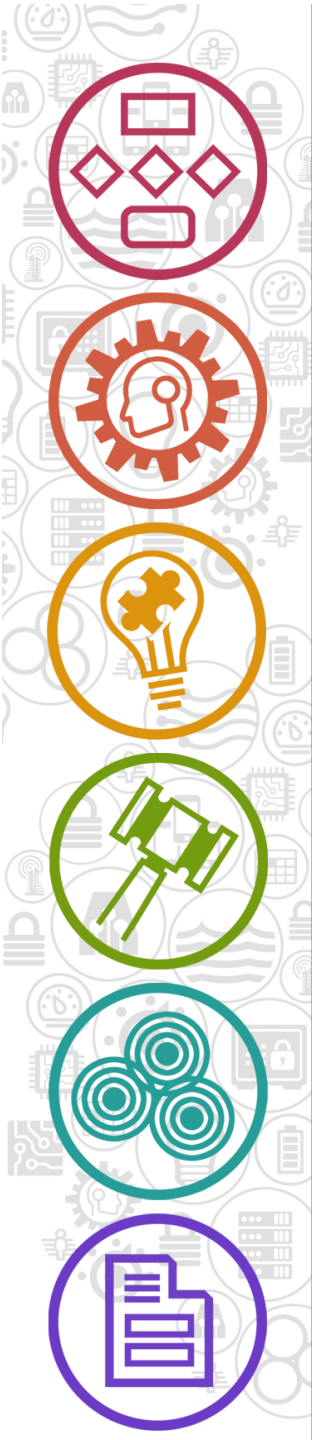
Introduction

Data is consuming every industry. Data is the new oil. He who owns the data wins. In God we trust, all others must bring data. Data is everywhere, and every industry is working to define new business models, create new revenue, unlock the value, and establish strategic differentiation. A singular set of data, in and of itself, is of little value, either in analytics, or in consumption. But when we combine numerous sets of disparate data across an entire ecosystem, new business models are born, new value is unlocked, and disruptive advantages are gained. Sharing of the data is the foundation, the keystone, to unlocking all of these data opportunities moving forward.

Without sharing, we cannot create new insights, we cannot monetize, and we cannot create new experiences across many disparate entities. Sharing makes all of this possible. But sharing assumes ownership and ownership assumes rights. To make good on the opportunity, the question is "How do I securely share the right data, with the right entity, at the right time, with complete control, compliance and auditability?"

The advent of a new paradigm —— whether in commerce, culture, geopolitics or any other realm —— rarely arrives peacefully. Nor is the disruption it causes welcomed by those whose own ideas enjoy primacy in their day. Guttenberg's printing press threw a lot of scribes out of work! The combustion engine changed transportation as well as challenged a century of investment in railroads, and the first plane further expanded the options for transportation, and the list goes on. Such a moment is upon us again, with the passage from history of the quaint notion that data ownership is a binary formula inherited from the transactional structures of the 20th century. Amazingly, some 24 years since the technologist Tim Berners Lee led the development of the World Wide Web, our legal and commercial conception of data ownership remains rooted in the brick–and–mortar practices of old, when a tangible product, formula, or patented process could be developed, marketed, and sold to a new owner with relative transparency and assurance. We no longer live in that world.

Yet only now has this become apparent. As recently as 2016, before the Facebook Cambridge Analytica incident, even the titans of technology – the FAANGs (Facebook, Amazon, Apple, Netflix, and Google) – proceeded on the assumption that data ownership would follow roughly the same rules that had applied for Customers. Ownership was singular based on the notion: I paid for it, therefore I own it. What's more, I control how the asset is governed, transferred or monetized until someone else assumes those rights. If all this seems like ancient history, consider this – Facebook, assumed it held similar sway over the individual data of its 2 billion users. Its' data privacy and governance policies which many users unknowingly agreed to, has led to a massive leak of personal information to third parties whose subsequent conduct concerned it little if at all.



While Facebook is facing the majority of the public wrath of data abuse from the data ownership and respect for personal privacy, as enterprises become more technology centric, they need to ensure appropriate policies and good governance for the increasing amounts of data in their organization – or expose themselves to new risks, brand damage, regulatory scrutiny, etc.

Toward a Rational Approach to Data Stewardship

Various data governance advocates have been warning of the reckoning in the making. The notion that data ownership could be binary - or even governed by the burdensome legal and regulatory practices of the past is absurd in a world where the Internet of Things (IoT), Artificial Intelligence (AI) and Machine Learning (ML) needs data to be shared at increasing speeds and quantity. Because of this, a new data ownership framework is required to survive the tsunami of information associated with the increasing pervasiveness of technology in business and society.

The need for a new data ownership model that has been building for years now must be understood as an evolutionary step beyond the old binary data model of owners and consumers. Even before the advent of IoT, sensors, etc. the old transactional model of a single data originator and a related single data consumer was obsolete. For instance, consider foot traffic in the mall with a store or a sensor capturing the number of times an elevator stops at your floor. This is clearly data of potential interest to various parties – insurers, financial services firms, security, public safety officials, etc. As a result, there is a need for organizations to provide stewardship of the data to better manage their business and respect personal privacy of information since there is no legal precedent to define whether or not the owner of the shopping mall or the apartment building needs to ask tenants' permission before selling such data.

Data stewardship will require a new framework for data ownership based on four separate ownership levels: the Data Originator, the Primary Data Owner, co-owners, and Enabled Parties

In today's commercial and regulatory environment, with privacy and security fears raising the reputational and legal risks for anyone generating, using, buying, or selling data, a more complex data overlay is required to prevent abuse and empower data owners to reap the rich insights and high potential revenue from their digital assets. Because of this, there is need for a new framework for data ownership based on four separate ownership levels:

- the Data Originator
- the Primary Data Owner
- Co-Owners
- Enabled Parties

Each of the four levels of data ownership would be empowered with specific roles, permissions, and limitations and overstepping those boundaries without express consent of the appropriate data owners further up the chain would trigger alerts and, ultimately, expose the violator to financial or legal consequences.

Before describing the four ownership levels, consider this – when an artist records an album, they were the Data Originator, the record label was the Primary Owner, the retailer (who bought the album from the label) was the Co–Owner, and the consumer, who bought the album, was the Enabled Party. Each has a role to play, a level of authority, and value to spend or receive. The main difference now is that frequently there are many Data Originators, as well as having a data ownership role.

With this insight, let's explore the four levels of the **new Data Ownership Framework (DOF) :**

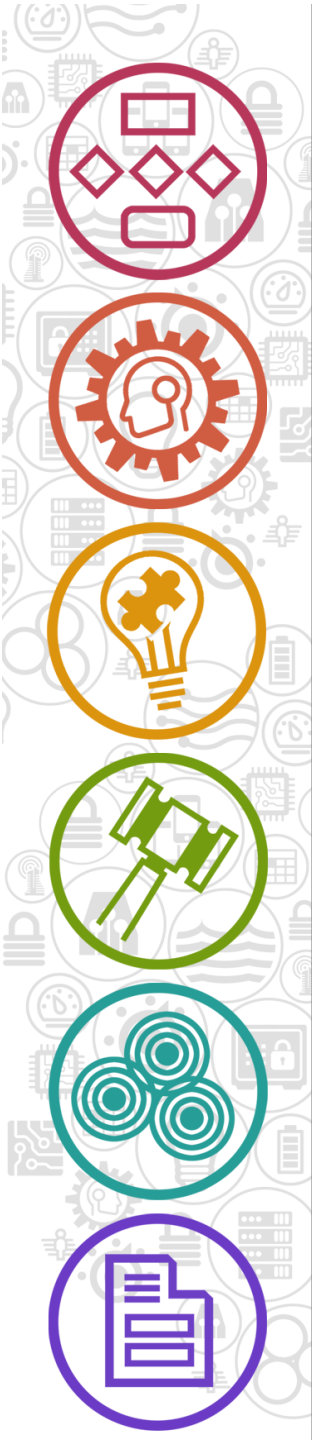
1. **The Data Originator :** A Data Originator, creates the information. Sometimes it is an individual, a distinct entity, a regulatory entity, etc. The Data Originator controls the rules of disclosure at the data's inception. The inherent rights of the Data Originator will vary between jurisdictions, but they generally will have the right to limit or even prevent the sharing, sale, or other use of said data and to demand anonymization. Furthermore, most jurisdictions now expect subsequent users of data to seek and obtain explicit permission from the Data Originator and/or the Primary Owner, to access and otherwise manipulate their data, like the new GDPR privacy rules in effect in Europe.

An example of a Data Originator is swiping a credit card. The consumer is the one and only originator, who defines the rights of influence and rules on how that data gets consumed further down the ecosystem. The consumer's rights are defined in this case by regulated financial services industry, so that the personal identifiable information is never shared.

Another attribute of the Data Originator is that their influence is applied at the time of inception, and then is done. This is an important consideration since any future permissioning around the data post inception falls to the Primary Data Owner.

2. **The Primary Data Owner :** The Primary Owner of data is the next level of ownership with–in the framework and makes ongoing decisions about how the data is consumed after its' initial creation. Often the Primary Data Owner and the Data Originator are the same. In other circumstances, they differ. The Primary Data Owner can define restrictions, constraints, and permissions. They can negotiate contracts, payments, limit use, and set timelines around how the data is shared. The only constraints of the Primary Data Owner are those initiated by the Originator.

In our credit card example, lets look at the merchant who owns their Point of Sale (POS) system. They are the primary owner of the data generated in their store, even though ac–cording to the regulations of the payments industry, the consumer is the originator of that data. The merchant cannot access or use the consumer' s name, for example, since as the Data Originator, the consumer, has the right to remain anonymous.



In this example, the Primary Owner of the consumer's transaction data is the consumer. The Primary owner of the merchant's POS data is the merchant. Yet like with the recording artist, there is only one piece of data. Context helps define the ownership. In the context of the POS, the merchant is the primary owner, like in the context of the record label, they are the primary owner of the recorded album.

3. **Co- Owners of Data :** Unlike Data Originators and Primary Data Owners, where there is only one of each, there can be unlimited Co-owners of data. Co-owners have rights to use the data so long as they adhere to the rules defined by the Primary Data Owner. Co-Owners have the right to further provision, sell, rent, exchange, and manipulate the data.

From our example, every one of the thousands of retailers who received the album can resell it and set their price as Co-Owners. In today's world, consider any integrated data exchange scenario; sensors in a shopping mall, data being generated from intelligent cars, payment systems, security cameras, smart buildings, and more. All of these examples have many parties who participate in a co-ownership role. From the credit card example, Visa/ MasterCard can sell, ingest and annotate all of their data for AI or Machine to Machine (M2M) projects, etc. as well as consume the data themselves to create new products and offerings. They can do this because they have an ownership stake in the data, but they still must adhere to the conditions implemented by Originators and/or Primary Owners. With this the credit card company cannot legally disclose the name of the consumer making a purchase.

4. **Enabled Parties :** Enabled parties are any entity (ie. person, organization, application, AI, M2M, etc.) that consumes all or a portion of the data. Enabled Parties do not own the data and typically consume the data in an exchange for value.

With our album example, the consumer is the Enabled Party. They have paid for the Album, and in exchange for that payment, they are enabled to listen to the album for their own personal enjoyment. They are not able to change the album, resell it, play it on the radio, etc. For a value exchange, their consumption is restricted. In the credit card example, enabled parties include credit bureaus, loyalty programs, and insurance companies. Other examples include analytics firms, retail stores, bond agencies, and consumer marketing firms. Enabled third parties typically pay for data either directly with cash, or indirectly with value services. Your insurance company, for example, gives you a discount for sharing your driving behavior or for sharing your alarm system data for homeowners.

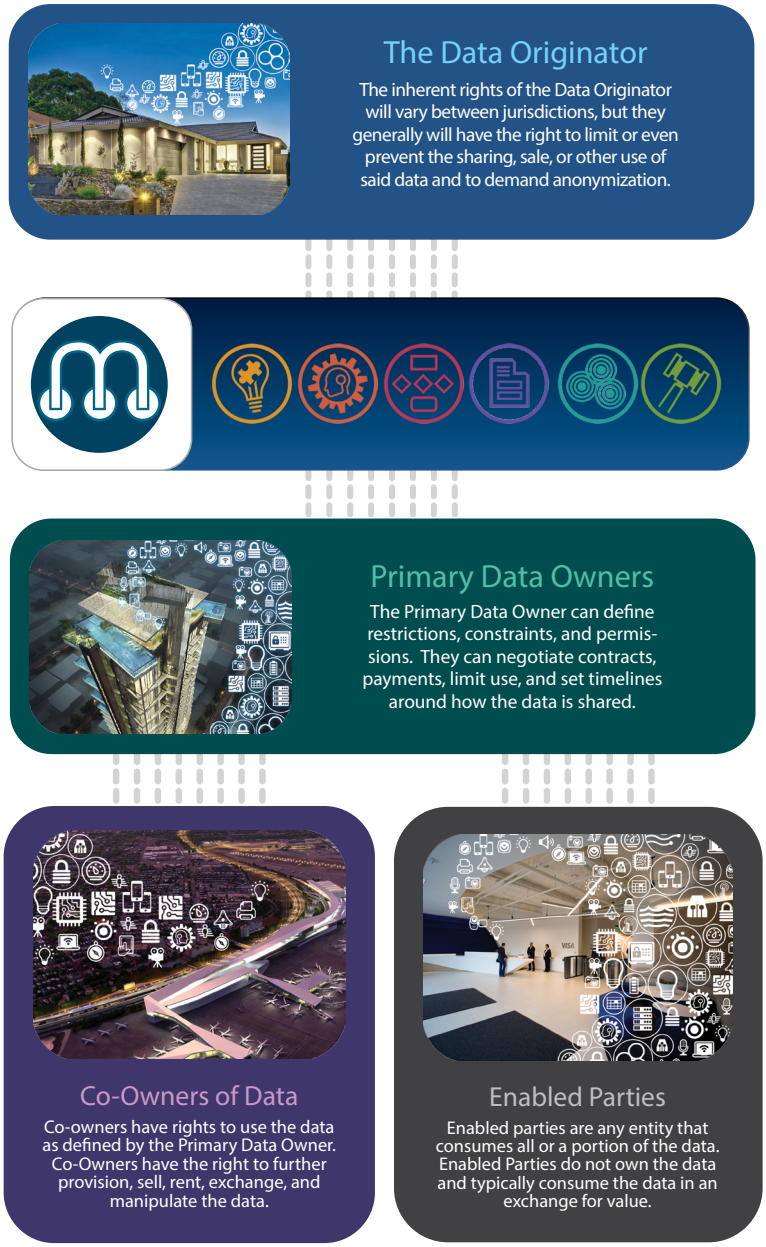
While this framework may appear simple, implementation is typically very challenging – without an appropriate platform. This is because all the data ownership roles in the framework need to co-exist and resolve any discrepancies or conflicts in the data sharing ecosystem. Rules need to be set, by ownership rules, including permission, pricing, timing, and more. Many organizations now recognize as data increasingly drives insight and opportunity, enterprises need to ensure a proper framework is in place.

Further cross industry cooperation is needed to ensure transparency and trust by mitigating privacy violations, data theft, and to prevent other issues that will eventually invite regulators. This is to be avoided, since these are impediments that undermine monetization of value creation.

The Digital Ombudsman

To address this challenge is there is a need for a Digital Ombudsman (The DO) – to ensure transparency, control, and compliance by all participants in data transactions. The DO ensures the rights, restrictions, and inherent roles of all four data ownership elements are enforced. These permissions are expressed in the form of Rules and Context in the Data Sharing Platform. This automated watchdog ensures that all data collection and data requests flow through the DO so that the privacy intents are honored uniformly and that usage is completely and immediately logged for billing and audit as needed.
An example of Data Ownership Facility (DOF) is –

.



Key to this capability is incorporating the Data Ownership Framework by utilizing a platform where the co-ownership relationships for a given datum is governed automatically and can evolve.

An example is a section of security camera video that includes facial recognition, and the requirement to tag that section of recording as belonging to both the owner of the camera and also each individual whose likeness is captured in each frame, as the Originator, and Primary Owner. A complete solution would allow that video data to be analyzed on a pixel-by-pixel basis so that value from consenting participants may be realized even in the presence of a single non-consenter among a crowd. To put it simply, data must be chopped and sorted to make best use while remaining in compliance. That is the role of the DO.

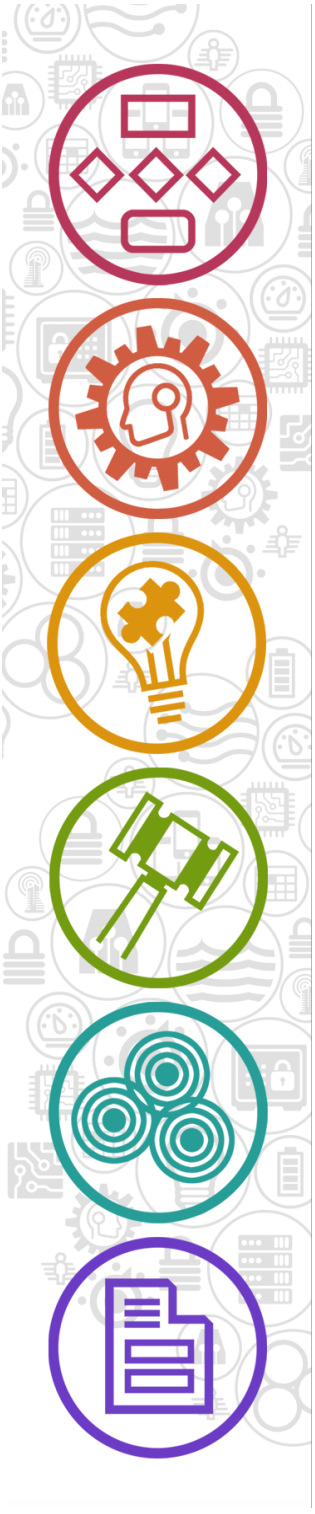
The Digital Ombudsman: a multi-owner/multi-party data management facility that forms the core of the allocation of rights and the expression of policy through rules and context. This is critical for the universal enforcement of intent across all data interactions. The policy fabric underneath the DO must leverage the wealth of data and evolving machine learning tools to automate the ongoing analysis and enrichment of data-at-rest with co-ownership metadata. At the same time, the DOF Platform must capture the intent of individuals, corporations, governments, and other digitally-expressed collectives in a clear and flexible fashion. Clear so that it is understandable. Flexible so that rules may evolve over time; keeping up with regulation and consumer sentiment seamlessly. In doing so, data management can remain compliant without the need for constant updates to software and infrastructure.

At Microshare, we have focused on the creation of the Digital Ombudsman: a multi-owner/multi-party data management facility that forms the core of the allocation of rights and the expression of policy through rules and context.

Building for Global Realities

The evolution of individual data ownership regimes varies by region, nation, enterprise, etc. In the United States, for instance, a relatively laissez faire attitude about data governance has prevailed. However this is changing because of data breaches and losses to third parties (ie: Cambridge Analytica) will raise the consequences of poor corporate governance and the level of regulatory risk significantly. The real risk to US corporations who eschew a responsible and scientific approach to data is the kind of reputational damage now being experienced by Facebook. That damage - and the share price erosion it entails - will drive change.

The European Union (EU), with its 508 million-strong customer base, is a larger and more affluent market than the United States. Its regulators have devised a characteristically burdensome set of regulations around the capture and uses of data generated by EU citizens called GDPR. We believe this will set the stage for global standards for individual and commercial data protections across most advanced economies. Microshare's granular controls not only navigate these evolving realities, but also allow real time audits



of what entities may be doing with the data they collect. In Brazil and Malaysia for example, two growing digitally advanced markets, new regulations forbid personal data from being stored on servers outside the country of the data's inception, an approach being studied widely across other Emerging Market nations suspicious of recent scandals involving the collection of sensitive foreign data. In an increasingly global world, data and data ownership need the flexibility to adhere to many and diverse compliant requirements.

Conclusion : A Data Ownership Opportunity

Information technology has continuously generated and processed data. Until recently the growth of that data management has been linear. Manageable. Predictable. But, the world has hit the data singularity – a discontinuous spike in the volume, velocity, and variety of data. We live in a world where the marginal cost of generating, transmitting, and storing one additional byte of data is essentially zero. And because of many events generating data, the marginal value is minimal if anything.

As the volume of data explodes, the challenges around who owns the data and how to ensure compliance in increased regulatory environments needs to be resolved. As the global portability demands of data from innovation, new business opportunities, value creation, etc. – there will also be a demand for a Data Ownership Framework with a secure, scalable infrastructure to support it. And with a Digital Ombudsman to ensure management, audit, and compliance through rules and policy fabric governance, this foundation is important for success in the trillion-dollar global data management market, competitive advantage, and to increase the rewards from business innovation – for better outcomes. To learn more about having a Data Ownership Framework that clearly delineates and defines the roles of the Data Originator, Primary Owner, Co-Owners and Enabled Parties, please contact –

info@microshare.io

610-994-9660

+44-798-414-0314

info@cail.com

905-940-9000