A 21st Century Framework for Data Ownership

By Ron Rock and Michael Moran

A white paper by:

microshare
unleash the data

Visit us at
www.microshare.io

A 21st Century Framework for Data Ownership

By Ron Rock and Michael Moran

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.

Visit us at
www.microshare.io

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. Torture the data, and it will confess to anything. And the list goes on and on. 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. The founders of Microshare have spent the majority of their 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?"

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 monastic scribes out of work. The combustion engine challenged a century of railroad investment, and Wilbur Wright's flying machine provided the coup de grâce. 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 British 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, in 2018, has this become glaringly apparent to the majority of the public. 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 when the explorer Peter Minuit purchased Manhattan Island from the Lenape tribe for a handful of beads and trinkets. Ownership was singular: I paid for it, therefore I own it. What's more, I control how its assets are governed, transferred or monetized until someone else usurps me. If all this seems like ancient history, consider this: Just 18 months ago, the world's 6th largest corporate entity ranked by market capitalization, Facebook, assumed it held similar sway over the individual data of its 2 billion users. Its' data privacy and governance policies which users always agreed to under duress and in the lurch, has led to a massive leak of personal information to third parties whose subsequent conduct concerned it little if at all. That Facebook is facing the majority of the public wrath at this juncture may be slightly unfair. The same or worse might well have occurred at digital rivals like Apple or Amazon, globally ranked Nos. 1 and 2 in market cap. The fact is, in each case, these otherwise admirable, formidable firms ignored warnings about the vulnerability of their laissez faire approach to data governance and ownership. And while Facebook has taken the brunt of the reputational pounding, all of them – and indeed, the entire tech sector – have seen their valuation eviscerated. Between them, the FAANGs lost some $400 billion in combined value between mid-March and the close of Q1 2018, according to Moody's.

Toward a Rational Approach to Data Stewardship

Microshare and a small number of other data governance advocates have been warning of the reckoning that has now arrived. The notion that data ownership could be binary – or even governed by the burdensome legal and regulatory practices of the late 20th century – struck us as absurd in a world where the Internet of Things (IoT), Artificial Intelligence (AI) and Machine Learning (ML) were demanding data be shared at increasing speeds and quantity. And so we persisted in our determination to develop a new framework for data ownership that would survive the data tsunami implicit in the advent of these new technological models. Our approach, derived from decades of experience building complex Business Process Management and compliance systems for some of the world's largest corporations, rests on a simple notion: Data, when shared, equals value, and therefore cannot be handled carelessly.

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.

The new data ownership paradigm 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 and its' constellations of sensors, the old transactional model of a single data originator and a related singe data consumer was obsolete. For instance, consider foot traffic in the mall where your flagship store is located or a sensor capturing the number of times an elevator stops at the floor where your apartment is located. This is clearly data of potential interest to outside parties like insurers, financial services firms, security, or public safety officials. No legal precedent seems to exist to define whether or not the owner of the shopping mall or the apartment building needs to ask tenants' permission before selling such data to downstream consumers.

In today's commercial and regulatory environment, with privacy and security fears raising the reputational and legal stakes 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 streams from their digital assets. We believe this 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.** Each of the four levels of data ownership would be endowed 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 we describe the four ownership levels, consider this. The advent of complex data ownership is not new. Even in the 50's, as Frank Sinatra recorded an album, we can see our data ownership framework at play. Frank was the single Data Originator of the album. 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 only difference is that now, with so much data being generated, we are all Data Originators, as well as playing some or all of the data ownership roles increasingly in every aspect of our lives.

So with that as the backdrop, let's further explore the four levels of the **Microshare Data Ownership Framework (DOF)**:

1. The Data Originator: There is only one Data Originator, who initially creates the data. Sometimes it is an individual, a distinct entity, or a regulatory entity. 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 going into effect this year 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 within 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 according 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 the Frank Sinatra album, 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.

In our album example above, every one of the thousands of retailers who received the Sinatra album wholesale is free to resell 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 complex systems have many parties who participate in a co-ownership role. Back to our credit card example, Visa/MasterCard can sell, ingest and annotate all of their data for AI or Machine to Machine (M2M) projects, and 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. For example, short of a subpoena, VISA can never legally disclose the name of the consumer making a purchase.

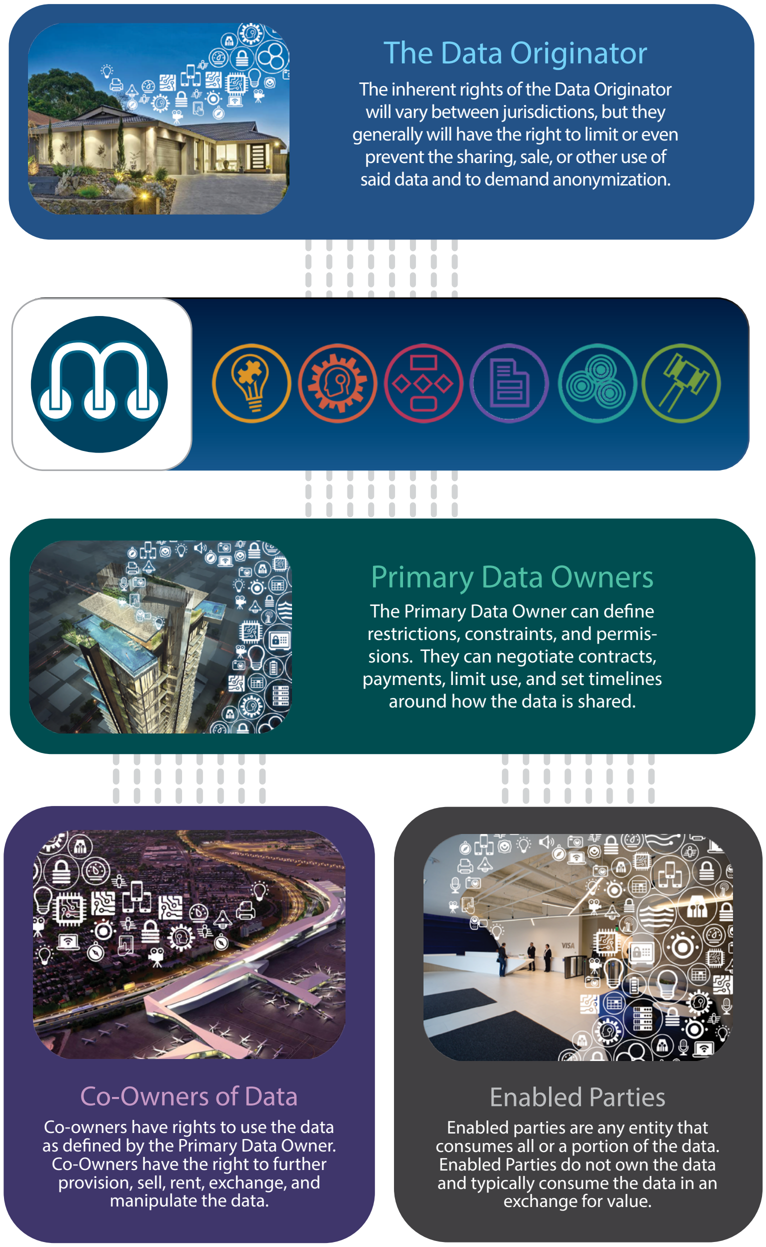
4. Enabled Parties: Enabled parties are any entity (e.g. person, organization, application, AI, M2M, etc.) that consumes all or a portion of the data. Enabled Parties do not own the data and typically consume the data in an exchange for value.

With our Frank Sinatra Album, 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.

This four-pronged framework may sound simple, but in fact, it is exponentially more complex than current best practices. All of these 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. Major players in the data analysis, distribution, and collection ecosystem have failed to recognize that as a global market for data increasingly drives the revenues of the largest technology companies, there is a commensurate need for serious cross-sector cooperation. Cooperation is needed in developing ways to provide transparency and trust, to mitigate privacy violations and data theft, and to prevent other issues that will eventually invite regulators in Washington and abroad to impose their own revenue-killing regulatory solutions.

The Digital Ombudsman

Our specific approach to this challenge is Microshare's Digital Ombudsman (The DO), an ever-ready ally that provides transparency and control to all participants in data transactions. The DO ensures that the rights, restrictions, and inherent roles of all four data ownership actors are enforced. These permissions are expressed in the form of Rules and Context in the Microshare 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.



The Data Originator

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.

Primary Data Owners

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.

Co-Owners of Data

Co-owners have rights to use the data as defined by the Primary Data Owner. Co-Owners have the right to further provision, sell, rent, exchange, and manipulate the data.

Enabled Parties

Enabled parties are any entity 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.

The four levels of the Microshare Data Ownership Framework (DOF):

Key to this capability is our incorporation of the data ownership framework – a world where the co-ownership relationships for a given datum needs to be governed in an automated and ever evolving way.

An example would be 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.

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, leading to 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, it 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 will naturally vary by region, by nation, and of course by individual corporate entities. In the United States, for instance, a relatively laissez faire attitude about data governance has prevailed until recently, though we believe recent revelations about sloppy loss of data to third parties like Cambridge Analytica will raise 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 in the US, even if governments are slower to impose regulatory action.

The Europe 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 will need the flexibility to adhere to many and diverse compliant requirements.

Conclusion: A Singular 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 functionally zero. And because the marginal cost is zero, every event that is capable of generating data is doing just that: generating data.

As the volume of data explodes, the challenges around who owns the data and how we can ensure compliance in increased regulatory environments will need to be resolved. As the global portability demands of data in new business opportunities and value creation expands, there will also be a demand for a new data ownership framework, and a secure, scalable infrastructure to support it. The Microshare team has spent the last 20 years refining the skills to meet this challenge. Our Data Ownership Framework clearly delineates and defines the roles of Data Originator, Primary Owner, Co-Owners and Enabled Parties. Our Digital Ombudsman ensures complete control, audit, and compliance through rules and policy fabric governance. With Microshare as the foundation, the trillion-dollar global data mart will flourish and ultimately achieve its great promise.

Ron Rock is CEO and Founder and Michael Moran is Director of Communications and Security Solutions at Microshare Inc.

microshare
unleash the data

OUR OFFICES
Microshare.io
1900 Market Street, Floor 8
Philadelphia, PA 19103 USA

IN EUROPE
Microshare Europe Ltd.
The Courthouse
Wokingham, RG40 2YF, United Kingdom

For more information, please contact:

Chris Leonard
cleonard@microshare.io
Cell +1484.410.1577

Charles Paumelle
cpaumelle@microshare.io
+447984140314