2018: CASHING IN ON IOT

Unlocking the Promised Value of the World Wide Web of Things (WWWoT)

BY RON ROCK AND TIM PANAGOS

The Internet of Things (IoT) has been the focus of considerable excitement and investment for several years now. But like the early days of computer networking, mass adoption for IoT has been slower than anticipated. Let's not forget that the Internet did not spring to life instantaneously. While network protocols, like TCP/IP, established the pathways that allowed for slow growth, it was not until flexible content standards, like HTML, were developed that the World Wide Web exploded into our daily lives. The key to unlocking the value of the Internet came from designing and utilizing standards that enabled seamless and ubiquitous communication. Although the Internet of Things has been billed as the next big chapter in the unfolding story of the Internet, the plot is familiar. Like the World Wide Web, IoT represents countless points of data that need to communicate, share, inform, and act, in a seamless, secure, and structured way.

In this white paper, we will look at the clues from history that predict the key items necessary to unlock the value across the landscape of the Internet of Things and how our work at Microshare.io is pivotal. Our work allows users to share any data, regardless of its origin or format, as easily as the early Internet standards allowed countless disparate systems to communicate. Standards are nothing more than the rules that govern interoperability. At Microshare.io, we have developed minimally invasive rules that make it possible to securely exchange massive amounts of data at the right time, with auditability, control, and compliance. Once these rules are adopted, the data from IoT, and specifically the sharing of that data, will unleash a new economy, just like the World Wide Web did.

Visit us on the web at www.microshare.io

The foundations of the modern Internet were laid – a standard set of rules that all networks followed to connect with each other and share information.

We Have Been Here Before

Before the Internet, computer networks began as a series of disparate systems communicating across fixed wires and leased land lines. Each connection required writing new software to bridge between network protocols enabling the computers to engage with each other. It was slow and expensive. Then, to make possible the vision of ARPANET as an "Intergalactic Computer Network", Vinton G. Cerf and Robert E. Kahn developed the TCP/IP protocol which effectively hid all of the gory details of each computer's networking interface behind a simple facade. Thus, the foundations of the modern Internet were laid – a standard set of rules that all networks followed to connect with each other and share information.

It was not until 7-years after the establishment of this fundamental piece of network plumbing that Tim Berners-Lee created the core set of standards (i.e. URLs, HTML, and HTTP) known collectively as the World Wide Web. The World Wide Web was a simple set of rules for sharing content among networked computer users. It pragmatically unlocked the value of the network, the value of sharing. The ease of use of the TCP/IP protocol and the subsequent World Wide Web's URL and HTTP standards fueled the spread of the technology around the world and become what we know as the Internet or Web today. It is hard to imagine any commercially viable entity today not using the Internet to share their own relevant content.

Since its commercialization in the mid-1990s, the Internet has been marketed as an open system, and in most ways it is. However, ultimately its openness and ability to freely share information depends more on an increasingly extensive set of rules than on the underlying technology. On the back of the fundamentals (i.e. TCP/IP, URL, and HTTP), additional standards were created to enforce controlled sharing of Web content, including SSL and OAuth. This fuller set of standards allowed the Web to grow from its care-free academic foundations to encompass our most sensitive content-sharing in healthcare and commerce. If IoT is to reach its human and economic potential, it will need similar rules and protocols to enable the same ease of use AND control around data sharing that the Internet has today.

Our Data Background

Our own formative experience included working with very large data sets in the credit card, manufacturing, banking and insurance sectors, beginning in the mid-1990s. As opposed to the Internet's open data, the data sources and inputs we worked with were securely locked down and thoroughly closed. The data and the systems that managed them were intended

Visit us on the web at www.microshare.io

The state of the art for technology has not moved much further in Enterprise computing – closed tools for closed data systems.

for a single operational purpose – granting credit, making deposits, or paying insurance claims, for instance. Our clients wanted more. They wanted to maximize the efficient organization and analysis of the data they had to make their operations work as efficiently as possible, improving their services and maximizing the return on their IT investments.

The computing challenges of the Fortune 1000 during this time were not trivial. Information was locked, siloed into disparate systems – often legacies of past corporate consolidations – straining operations and limiting growth. For example, consider a global company with some 600 subsidiary companies spread across the world. A company whose results were captured in 100 currencies, in many different computer systems, a variety of accounting regimes, and with distinct regulatory needs for each geographic location. Then add the acquisition of a new company, the shedding of another, and the restructuring of a third. Consider that this global corporation needs its books settled every month, and then annually on a particular day each year. The amount of disparate data made the task of closing the books herculean. Not only was this time and labor intensive, but mistakes were routinely made, management uncertainty was accepted, and sizable fines were paid.

We were able to successfully manage this over the last couple of decades, by applying early artificial intelligence tools and lots of programming talent. But it required millions of dollars and multiple years with an army of programmers and analysts integrating hundreds of systems, writing thousands of rules, and annotating hundreds of thousands of rows of data. However, what clients really needed was to allow the system to patrol itself, identifying both anomalies (e.g. fraud patterns) and pathways for improved efficiency.

At this scale with today's technology this is still a staggering task, yet we are only dealing with hundreds or maybe thousands of systems. What happens when we have billions of micro-systems, as is the projected growth in IoT, all coming online or being decommissioned in real time, in the real world? Each source of data needs to be secured, as they are constantly under attack. Audit needs to articulate on demand, every step, every decision, and every access. The answer is that no human team can configure, manage, and maintain all of the micro-systems. There are simply not enough of us.

The data sets for which we developed these kinds of tools were closed systems, controlled by the company who owned the data. And the state of the art for technology has not moved much further in Enterprise computing – closed tools for closed data systems. Using these tools, the Internet of Things stands somewhere between an open and a closed system. On the one hand, there is so much data openly available to be shared. Gartner forecasts that

Visit us on the web at www.microshare.io

Crossing the chasm from comfortable silos to improved customer experience requires the same evolution that led to the explosion of Web commerce.

there will be 20.4 billion IoT devices by 2020 . On the other hand, most companies collecting IoT data are doing so into their closed, proprietary databases. If the IoT journey follows the path of the Internet, we know that real value creation lies on the open end of the spectrum. It lies in sharing data rather than in siloing it. So how do we go from here to there?

McKinsey Global Institute defines the Internet of Things as "sensors and actuators connected by networks to computing systems." Currently most operating IoT systems use sensors of a single manufacturer connecting through networks to computing systems that are under the control of the corporation (i.e. a closed system). Data might be analyzed on private dedicated servers or more commonly on the private cloud. Corporate IT is content with this form of siloed IoT implementation because it is comfortable, just as they were content in the mid 90's without the World Wide Web. Comfortable tools. Comfortable governance. Siloed data ownership is comfortable and many in corporate IT believe that if they handle IoT data within their own systems they will not face issues of privacy, data theft, or other misuses of the data.

It is worth noting that the above scenario is exactly where computer communication was prior to the standards discussed earlier. Large enterprise clients were content to keep their systems closed to third parties or even customers. The same concerns, privacy, security, and theft to name a few, drove their reluctance to initially participate in the World Wide Web. Pioneers pushed that boundary and were rewarded for it. Laggards were punished and forced to catch-up or perish. It is hard to imagine now that at one point all of that data was not at our fingertips, in virtually any industry, anywhere in the world. As consumers today, we notice when data is not readily available. It is an anomaly. The same MUST become true of information derived from raw IoT sensor data that is (or soon will be) collected from the world around us.

Of course, we aren't there today. Crossing the chasm from comfortable silos to improved customer experience requires the same evolution that led to the explosion of Web commerce –we need to create the same kind of standards around the data now in the IoT space. We need to allow the right entity secure access to the right data, at the right time, with complete auditability, compliance, and control.

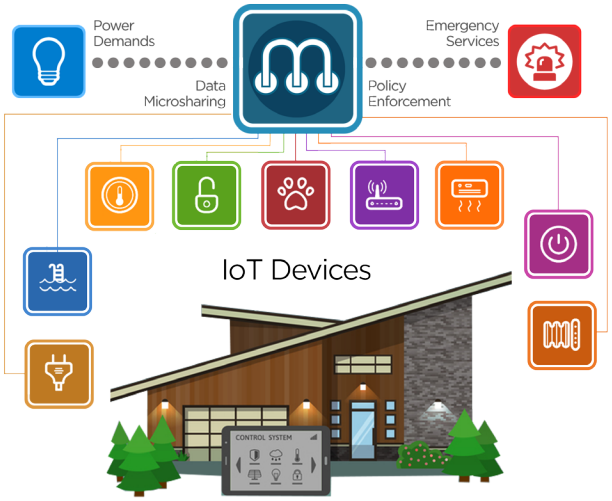
When you start to envision ubiquitous access to data, creating data mash ups, and new insights never before imagined, you realize that the major paradigm shift is breaking the one to one relationship between data and its owner. A data set, and its sub-sets, will naturally have multiple parties interested in its content. As discussed by Don DeLoach, Emil Berthelsen, and Wael Elrifai, in their book, "The Future of IoT," the first receiver is the first

Visit us on the web at www.microshare.io

Just as the processing of crude oil into gasoline generates a protracted value-chain of petrochemical products, so the primary collection of data will lead to multiple sources of secondary value.

point of contact where IoT data is received and value is derived from it. But that is just the beginning. The term "first receiver" naturally implies the existence of secondary (and even tertiary) receivers. From there, data can be shared, enhanced, tagged, and used for additional value-creation by both the first receiver AND by outside entities, secondary receivers who can also benefit from consumption of the data. Just as the processing of crude oil into gasoline generates a protracted value-chain of petrochemical products, so the primary collection of data will lead to multiple sources of secondary value. Instead of the data only being used for a single, specific purpose, it can be shared and distributed appropriately so that the data collected can be used for secondary or tertiary purposes (provided the owner of the data agrees, naturally).

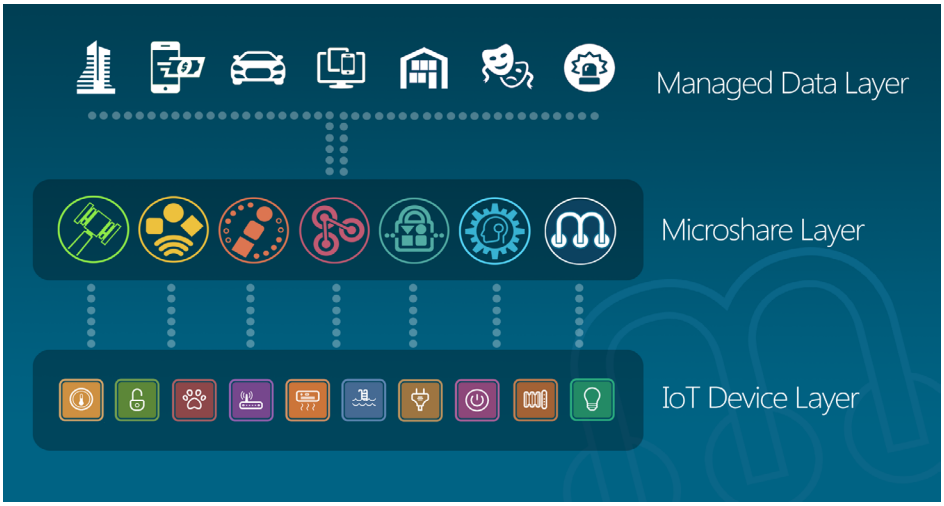
We believe that the first receiver concept, along with the accompanying secondary receivers and beyond, will encourage more and more companies to move from a siloed, closed system to a shareable, open system where the right rules and standards will govern the data ownership and visibility at a granular level. As we move from siloed data ownership to more open sharing, new economic models will evolve. These models will leverage micro-contracts and micro-payments. These models will fuel new sensor investments by creating new revenue streams. Combustion becomes inevitable, all because the data can be securely shared with complete confidence.



For example, a home monitoring system can be used to automatically change the temperature if either high or low boundaries are reached (i.e. rules). This system as a first receiver has its primary function of regulating the home's temperature. What if the system could also automatically notify the fire department when the temperature is over 100 degrees? How about notifying a utility company of the homeowner's efficient energy usage or a home insurer of the risk of frozen pipe damage? Rather than stopping at the initial purpose of regulating the home's heating and cooling system, the data can now be shared with other interested parties, like maintenance repair companies, home warranty companies, quality control within manufacturers, home healthcare companies, etc., all whom use the data for other value-added purposes. Some may pay for the data, some may offer discounts for access to the data, but in all cases, the owner of the data has complete control and final say. In this case, the homeowner is the owner of the data, but by setting the rules to allow others access in certain circumstances (i.e. the fire department or the insurance company), data is shared with multiple parties in the right context. Our imaginations have no limits to what happens when all of this data becomes accessible.

Visit us on the web at www.microshare.io

We believe that though the Internet of Things will indeed take advantage of many of the Internet's standards, it also needs new sets of rules that will turn the torrent of data into streams of value.



Our Multi-Party, Multi-Owner Data

Looking at this evolving landscape, we believe the Internet of Things can take computing to a second golden age of democratized, open and distributed communication. There are many ways to look at this but we will focus here on the development of standards that maximize the value of large data streams by increasing its sharability. Our core competency is in receiving, annotating, and sharing data, especially where Multi-Party (e.g. interested stakeholder yet not an owner), Multi-Ownership opportunities arise.

The crucial step is to develop standards such that IoT information can be shared in a controlled fashion. TCP/IP, URL, and HTTP were the basic protocols, but they needed additional standards for governance to temper openness with control. Once enough people commonly used these standards, they were able to share their information more openly. By having a common set of standard rules that were accepted by the data owners and parties involved, information became easily sharable. Early Web platforms assumed that this acceptance of the basic protocols also constituted a kind of "permission." By making your data available on a website that conformed to the Internet's formatting rules, you were implicitly agreeing to make that information accessible, indexable, and marketable by search engines.

We believe that though the Internet of Things will indeed take advantage of many of the Internet's standards, it also needs new sets of rules that will turn the torrent of data into streams of value. Those missing rules are similar to those that we developed for very large but controlled datasets with enterprise clients years ago. We can use the lessons-learned in multi-million-dollar projects of the past to solve the multi-billion-dollar problems of today's IoT market. By deploying these technology breakthroughs mixed with the best practices gained by managing the world's largest digital companies, we believe that we have the secret sauce for bringing secure data sharing to the high-scale IoT world that will allow for an ever-widening circle of data receivers beyond the first receiver.

How do we do this? At Microshare.io we combine stream processing, robot automation, artificial intelligence, and advanced cryptography to address the unique proposition of handling data with the assumption that it will ALWAYS have multiple stakeholders. Just as TCP/IP decorates data packets in-flight with routing metadata, Microshare.io annotates data-at-rest to ensure that it can be used safely by all who are intended to receive it. Our patent pending system, with an Enterprise-inspired rules engine at its heart, allows data owners to express the policies that will govern future data sharing relationships in a fluid

Visit us on the web at www.microshare.io

but firm way. It applies policy at the individual data level, both rows and columns, at very high speeds. It provides an audit trail for every request, for every decision, and for each usage giving unprecedented visibility to the web of interconnected usage. It is meant, not to lock-down the data, but to open it up safely, in a way that allows the owner(s) of that data to capture the value created by its movement and secondary uses.

A microshare is the resulting data exchange that factors the contextual indicators and the rules that were set to reflect the data owner's sharing policy. It acts on terms of the metadata that simply describes the potentially complex relationships between the originator (owner) and the receiver (requestor). Using this approach, the same piece of data can be owned by more than one party AND, naturally, made shareable by each owner with non-owner-but-interested parties. In this arrangement, micro-contracts can be fulfilled, between the owner and interested parties, and micropayments can be made based on the set rules without violating regulatory laws or business interests.

The same piece of data can be owned by more than one party AND, naturally, made shareable by each owner with non-owner-but-interested parties.

Conclusion

In short, Microshare is creating the foundation for the World Wide Web of Things (WWWoT).

It is a big idea. One explosively valuable idea. There will be competing standards and competing organizations putting them forward, but there will only be one or two trailblazers whose standards form the commercial basis for a major economic driver of the next two decades. The stakes are big and we are well positioned.

This is a cultural as much as a technical journey, one that will unfold over the next 5-20 years. What matters most is not the generation of or even the power to store data but the power to make it discoverable and negotiate the terms by which it can be shared. The rules and context regulate the data usage, not the data itself. By managing this metadata and applying it at scale to enforce the will of the various data owners, we are unlocking the real value of IoT data.

Our backgrounds have shown us a path forward that is grounded in commercial reality—it is informed by expertise in real-world, large-scale business operations. At the same time, we have lived through the first wave of innovation adoptions driven by the Internet and the World Wide Web. We have learned the lessons and have seen the parallels. With access to cutting-edge technologies coming out of Silicon Valley and the know-how of our team to apply them effectively, we can meet this challenge.

The explosion of deployed IoT devices will necessarily transform how data is collected, used, and shared. Using the standards that Microshare is developing allows for an open, but controlled environment. Data can be shared securely across multiple parties, rather than siloing this data to a single purpose. By allowing for the identification and annotation of data in this way, we can create the foundation for a market where data can be safely and profitably shared. The only limit to value creation will be our imaginations.

Contact Us: https://microshare.io/contact-us/

Ron Rock
CEO Microshare, Inc.

Tim Panagos
CTO Microshare, Inc.

Ron Rock and Tim Panagos are co-founders and the CEO and CTO, respectively, of Microshare Inc., makers of a data sharing, governance and revenue generation layer for the Internet of Things.

Visit us on the web at www.microshare.io