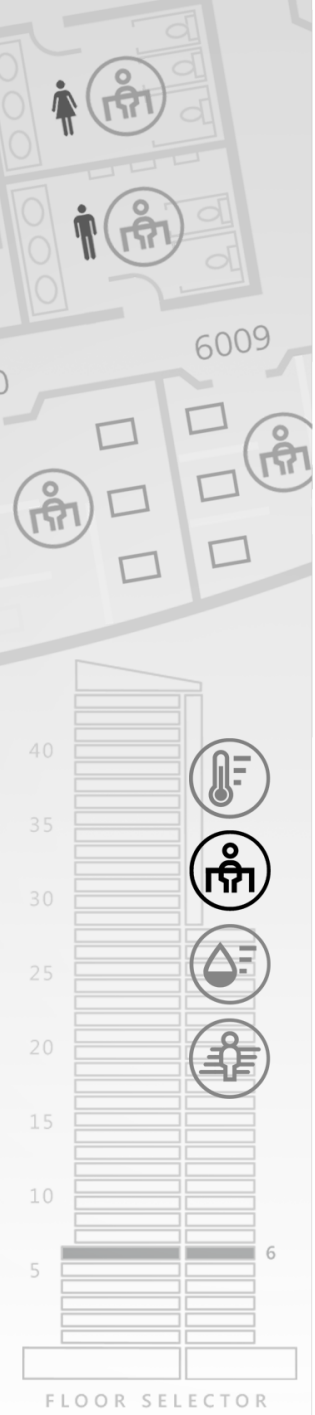


IoT and GDPR: A Data Convergence That Pits the Bold Against the Cautious

By Michael Moran and Tim Panagos

A Whitepaper by:

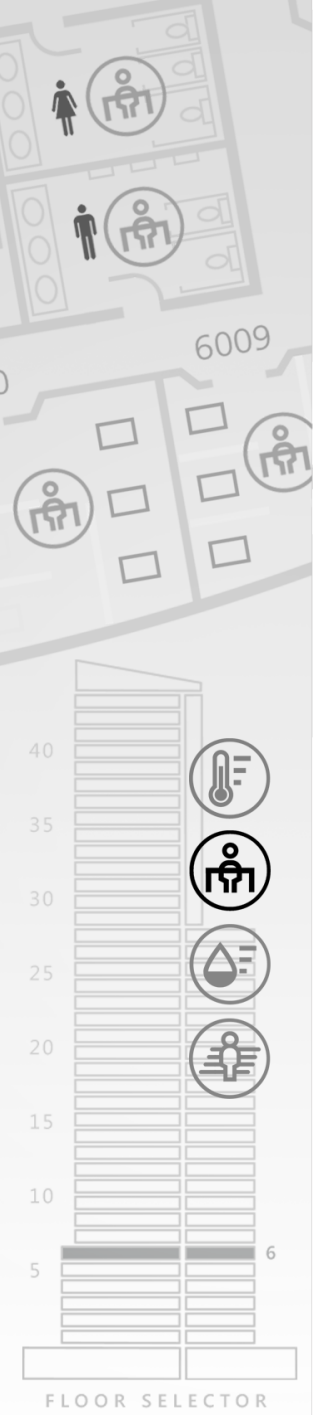
microshare
unleash the data

Visit us on the web at www.microshare.io

IoT and GDPR: A Data Convergence That Pits the Bold Against the Cautious

By Michael Moran and Tim Panagos

Executive Summary: The European Union's forthcoming General Data Protection Regulation (GDPR) will reshape the rules of data management and raise both the cost of complying with laws governing people's personal data and the risks and considerable financial liabilities involved in mishandling it. The rule has implications across the corporate spectrum, from the general counsel's office, to chief revenue officers and corporate strategy groups, (CROs) chief security officers (CSOs), chief information officers, to the developers' suite. But in this Microshare white paper, we will focus particularly on GDPR's implications on the vast streams of data generated by the Internet of Things (IoT) which will be particularly vexing due to its volume, the disparate nature of its sources, and the lack of common standards across IoT networks. GDPR and other regulatory and security initiatives will complicate efforts to store, analyze, share and sell IoT data, a problem that threatens to undermine bullish forecasts about the potential size of the IoT data market. The advent of IoT will require new thinking with regard to data management and ownership, which currently assumes data has a single owner and that data transactions involve two parties (or three, if the regulator is included). This cozy concept -- the norm since the start of the information economy – is being overturned by the speed, quantity, portability and diffuse demand for the valuable information now generated by billions of new IoT sensors. Yet with the right mix of standards, privacy and compliance controls, context, and auditable micro-contracts, a sharing economy fed by the powerful firehose of IoT can flourish and transform digital business models even in the age of GDPR. Microshare, uniquely, exists between the IoT networking layer and the standards-free edge, precisely the right place to ensure data is shared with only the right people and at the right time and under the proper circumstances.



Visit us on the web at www.microshare.io

Introduction:

Attention and apprehension builds daily as the introduction of the European Union's new General Data Protection Regulation (GDPR) looms ahead on May 25, 2018. GDPR represents the most sweeping change in the rules governing the privacy, security, and ownership rights since the advent of the information economy in the late 20th Century. The fact that this regulatory experiment will play out in the EU's 508 million strong consumer market means the stakes are enormous. Initially relevant mostly to businesses with large footprints in Europe, history suggests that the EU standard will influence other regions, including the United States, as lawmakers, ethicists and businesses struggle to find a balance between the free flow of data and protection of individual rights. Other, less stringent standards may persist for a time, and in some more closed markets (Russia, China), censorship and surveillance will play a greater role in shaping market dynamics. Nonetheless, globalization and the premium placed on reducing the cost of cross-jurisdictional regulatory compliance, security, and operational risks dictates that the highest standard will become the de facto global standard sooner or later for the advanced economies of the world's wealthiest regions. Rather than present another white paper that professes gloom over GDPR's fines and strictures, engages in fear mongering over IoT security vulnerabilities, or simply regurgitates the latest consultancy hype about the size of the IoT market, we instead propose to tackle one specific and fundamental challenge facing companies that now are rushing headlong into the IoT space: The absence of agreed standards, legal precedents, and practical software solutions that will govern the sharing of IoT data at scale among multiple parties. This has been the focus of our work at Microshare for a number of years and, to our minds, this conundrum already has acted as a drag on IoT adoption rates and disappointing progress toward reaching the revenue and market gains being projected by industry analysts.

The Coming Data Storm

The fact that this new rule set takes effect in May 2018 means it appears just as the Internet of Things comes of age. IoT spawned the proliferation of a vast new category of connected devices that so-far exist largely without standards, minimal regulation, and porous security

protocols. Large corporations and public utilities in the European Union, IoT's pioneering early adopter, already have an installed base of IoT sensors and networks now subject to expensive reengineering. Happily, that's not the case for other regions of the world which can now benefit from steep learning curve (and expensive mistakes) endured by EU pioneers. But there is a risk that timidity will rule the day. The chasm between the frenzied corporate pursuit of IoT revenues, and the increasing concern, public regulation and legal strictures that will soon apply to data ownership, puts at risk many of the benefits foreseen by IoT visionaries. GDPR focuses mainly on the intersection of corporate data mining and personal (consumer) data, providing expanded protections for the latter. Most of GDPR's animus revolves around protecting individuals from increasingly voracious marketing practices and, as result, much of the legal analysis has focused there too. But GDPR will cast a broader net, not only including IoT, but many forms of Big Data. Viewed in the context of the current configuration of most IoT data stacks – which tend to move data directly from the captive environment of networking hardware to the Wild West of the Edge, GDPR will be no joke to manage.

Consider some of GDPR's core requirements, which prohibit unauthorized collection or use of:

- Basic identity information such as name, address and ID numbers;
- Web data such as location, IP address, cookie data and RFID tags;
- Health and genetic data (also heavily proscribed in the US by HIPAA);
- Biometric data;
- Racial or ethnic data
- Political opinions;
- Information on sexual orientation.

Add the fact that fines for violating GDPR are steep – EUR20bn or up to 4 percent of global revenue – the problem becomes crystal clear. Without a serious and proven capability to manage the sharing, sale, storage, and other leveraging of IoT data before it reaches the consumer, the appetite for risk in exploring new IoT revenue streams, business models and use cases could dry up. This would be a tremendous setback for productivity, operational transparency, and global growth. In many ways, the reaction of individual corporations to this data challenge may separate future winners from those who are left behind. The winners will wrestle with the complexities of deploying solutions that rely on a mixture of robotic compliance protocols and human monitoring to ensure that they can move into the highlands of the new IoT data economy without risking a regulatory backlash. The winners will face up to the challenge thrown down by EU regulators and resolve to ask for proper permissions, a challenge that sounds daunting but need not be with the right platform in place. Down the food chain, more timid players will allow trepidation to outweigh opportunity, opting for a fierce anonymization of any data their systems touch. In effect, the cautious compliance and privacy officers will lobby for anonymizing and delinking the context of any data that could possibly be interpreted as personal. In an era where data equals insight, this is a prescription for irrelevance. It is Microshare's view that the market will punish this approach to the EU's new strictures and reward those who seize the opportunity to obtain value the old-fashioned way: By earning the right to use it from the individuals in question.

Brace for Collision

The collision of IoT opportunity and GDPR constraints will pit those charged with protecting corporate reputations against those responsible for planning growth strategies that expand the company's bottom line and its position in the market. Corporate strategists, chief investment officers (CIOs), M&A teams, as well as aggressive-minded CEOS, all will blanche at the idea that the challenges of GDPR are so acute that the company should simply forego the lucrative market for IoT and other data. And they will be correct: GDPR in the context of IoT data is both a titanic challenge and one that is navigable with the right approach.

The complexity of the task ahead should not be underestimated. In part, that is because the old adage – generals always prepare for the last war – applies equally to compliance officers, risk analysts, CIOs, and chief counsels. Many veteran practitioners, having come of age with the Internet itself in the mid-1990s, are full of stories about how the advent of the World Wide Web rocked their world, adding layers of complexity and risk, along with multiples of speed to challenges that previously moved only as quickly as the postal service (or, at best, a fleet-footed bike messenger). Contract law, libel, taxation and domiciles, rights and royalties, decency, privacy and many other time-worn precedents of the pre-digital age were disrupted by the Internet, rendering decades of legal precedent and regulatory tradecraft irrelevant and sending many practitioners in a desperate search of adult learning. One of the elements that made the Internet of the mid-1990s such an earth-shattering development for such professions is the way it dealt with information. Rather than purchasing content from a publisher or business service provider – the print model, driven by human decisions – digital platforms allowed individuals to publish themselves, blurring rights and plagiarism laws. Digital photos could be manipulated; digital platforms harnessed to create new revenues or to engage in industrial espionage. Control of everything from product specs to brand messaging and corporate reputations was constantly at risk. What's more, the operating system of the hypertext world came to depend on queries, and eventually, on algorithms that embedded structured query language (SQL) into user friendly portals like Lycos, Alta Visa, Bing, and ultimately, Google. Human curiosity and demand remained the driving force behind the transfer of data – usually on a one-to-one, owner-to-receiver basis. Over the years new legal standards, along with copyright and compliance norms, took root for the digital space. Yet even today, decades after the appearance of the World Wide Web, the legal particulars of data ownership, rights, and other issues remain fluid.

> 'If you cannot manage real-time streaming data and make real-time analytics and real-time decisions at the edge, then you are not doing IOT or IOT analytics.'
>
> ***Bill Schmarzo,***
> *CTO, Dell Big Data Practice*

Now imagine IoT. Unlike the World Wide Web, where human bilateral interactions continue to drive most data exchanges, in the IoT domain the human element is far less important. Sensors feeding gateways feeding analytics suites and ultimately API-based devices on the edge often forego human interaction altogether. Unlike humans, they never sleep, and in and of themselves, they neither differentiate between sensitive and mundane data, do not ask permission to ingest, feed, or store it, nor provide any way for the database to reverse engineer the process and conduct spot audits. This is a recipe for trouble under GDPR (and, it's worth adding, the US government's HIPAA laws governing personal health care data). A shopper in a European mall will

not stop to consent to the leveraging of 150 pieces of data created by the simple fact that he walked by your store front. Some of that data will have real value and its distribution fall entirely within the borders of the GPDR; some will be personal and require explicit permission for ingestion; a large amount in between will drive legal challenges for the next several decades as national judiciaries grapple with the need for a whole new class of precedents.

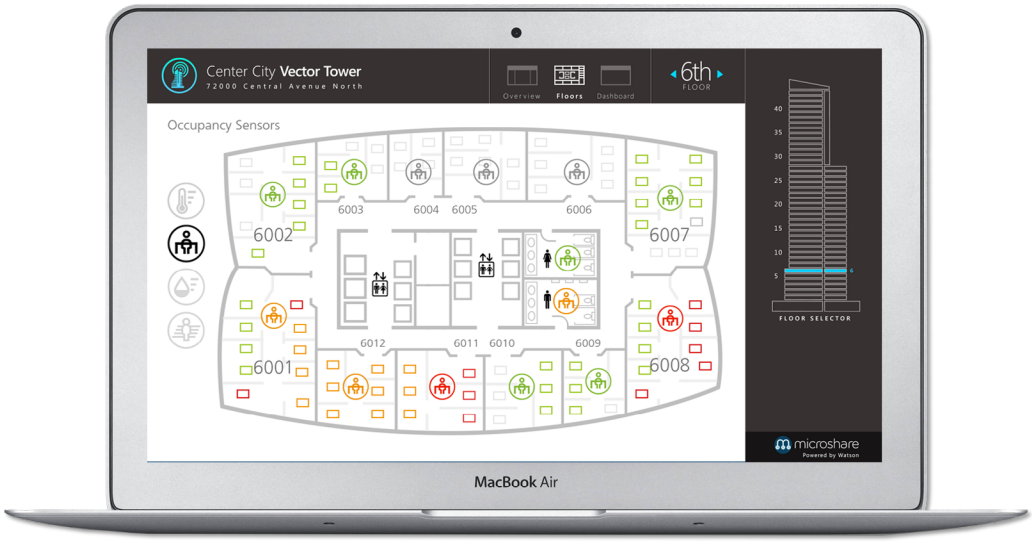
Another challenge is the time-sensitive nature of IoT data value. Unlike, say, a Google search that quickly satisfies a need to know who the president was in 1887, IoT data is not necessarily most relevant in archive form. In fact, IoT data more likely acts as real time triggers for various automated processes that may roll trucks, trigger alerts, or create immediate action – trading shares in a particular company, closing water-tight doors on a cruise ship, dimming the lights and lowering the temperature in an unused conference room. Is the privacy of the last person to leave that conference room violated when the lights are dimmed and heat is lowered? No one yet knows. In fact, no compliance organization on the planet could possibly grapple with these things in real time. Without delinking context and deleveraging an organization from the myriad data that makes it more productive, reactive, and profitable, only a highly evolved data platform leveraging both machine learning and human-guided, dial-up/dial-down risk controls will suffice. GDPR will require more than filters, more than analytics, more than a new round of policies sent out by the general counsel's office. It requires a streaming data management suite with the ability to react in real time even as it ingests, annotates, stores, and if necessary quarantines data pouring in from sensors at the edge. Contextual security, complete audit, and immediate remediation capabilities all stand as prerequisites to entry into the IoT Nirvana: the massive revenue streams of a global IoT data marketplace. Bill Schmarzo, CTO of Dell EMC's Big Data practice, wrote last year that "if you cannot manage real-time streaming data and make real-time analytics and real-time decisions at the edge, then you are not doing IOT or IOT analytics."

There are also concerns about the way IoT products and services engage with third parties. Quite contrary to the model that prevailed during the Internet's first several decades, IoT tears up the notion that data has a single owner or that data transactions are conducted primarily between two entities. Central to this premise, we believe, is the concept of the First Receiver, a construct conceived by Don DeLoach, co-author of The Future of IoT: Leveraging the Shift to a Data Centric World, and an advisor to Microshare. The 'First Receiver' is, as the phrase suggests, the primary target or generator of the data in question. In the recent past – throughout the Information Economy era that began in the early 1990s – the First Receiver was analogous with the owner of data and generally could sell or not sell that data to another entity. IoT, however, has overtaken this model. With IoT data, the First Receiver assumes, but does not necessarily dictate, the role of data owner. But the fact is that a single data record generated from a single IoT sensor message can be utilized by a

variety of constituents, internal or external, in a variety of different ways. Some get the full package and rights to use it as they see fit. Others see just a part, or are merely apprised of the data's existence. Still others are shut out for legal or regulatory compliance, or for business or personal reasons. This is the data ecosystem Microshare is designed to manage: The aim is to securely and cost-effectively provide a mechanism for allowing the right people/organizations to access and use the right data in the right place at the right time, thus extracting maximum value from data by not simply selling it on but by leveraging it across a huge spectrum of demand.

Applying GDPR's strictures to this eco-system will overmatch the average corporate compliance and IT competencies. Because current practice is to embed "consent" into IoT devices and the materials that accompany them, IoT data relative to GDPR is a ticking time bomb. The GDPR requires organizations to obtain a fairly high quality of consent from customers/users about the way their personal data will be used. Consent must be active – not the result of inactivity or pre-ticked boxes. The person giving consent must also understand how their personal data is being worked with – and this is the challenge, given the complexity of how this information may be used in products and services. Some legal experts even question the ability of IoT products and services to obtain the GDPR's standard of consent at the moment. Companies and their third parties will have to ensure consent from clients covers both organizations. Related to this is the idea in the GDPR of "privacy by design" and "privacy by default." All of the data that an IoT device creates will need to be classified as personal data, even if the data is not specifically linked to the owner of the device. This means that this data will need to be treated as personal information in the way it is gathered, stored and processed. All products and services will need to be designed from the beginning to take these requirements into account – which could be a difficult task, made even more complex by the presence of third, and fourth parties.

Happily, defining the problems specific to IoT that would flow from GDPR is what we at Microshare have been doing since 2013. We have developed a software solution that provides the remediation, control, context, and audit capabilities necessary to fulfill both the privacy, security, and regulatory requirements of GDPR and to protect corporations eager to tap the new revenue gains that make all this work worthwhile.



Digital Ombudsman

What compliance and capitalism mean in the 21st Century is that every device owner needs to offer a digital ombudsman; an automated tool for a) collecting consent, b) managing granular permissions, c) and effortlessly granting access to collected data and usage audits to consumers and companies alike. And naturally, all data collection and request must flow through the digital ombudsman so that the privacy intents are honored uniformly, and that usage is completely and immediately logged.

A digital ombudsman must present the ability for policies for data use be expressed in both programmatic and explicit form so that applications may set rules based on purpose-built user experiences like embedded smart EULAs but also may be managed manually after the fact using a review and edit experience that can allow the expression of non-default intents on an ongoing basis.

A digital ombudsman must be able to recognize the co-ownership relationships for a given sensor datum in an automated and ever evolving way. For example, a section of security camera video must be able to leverage facial recognition to tag that section of recording as belonging to BOTH the owner of the camera but also each individual whose likeness is captured in each frame. In so doing, that rich behavioral data may be determined to be usable based on previously established consent or recognize when new consents are required. 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.

These requirements need not imply a centralized utility, in fact, highly distributed decisions from Edge, to cloud, and on-premises make centralized processing via VISA credit card transaction unlikely. Distributed computing is more likely to be embraced to allow for high-scale data processing and a more egalitarian rule for participation. To make this possible there must be a central management capability where policies are authored, reviewed, and edited for enforcement by a million remote agents. It must create the illusion of centralization without the restrictions associated with centralized authorities or centralized computing.

So, the implementation requires a swarm of micro-services which may be centrally configured and whose logging becomes part of a centralized experience. It is likely that each multi-national enterprise with significant data assets will host their own digital ombudsman to serve their industrial or geographical ecosystem. However, the increasingly interwoven nature of data analytics and cross-corporate collaboration will require that private 'marketplaces' be able to coordinate to start and to eventually merge processing to ultimately create a Policy Fabric that can encompass any and all transactions.

At Microshare, we have focused on the creation of the key missing component of the digital ombudsman: a multi-owner/multi-party data management facility that forms the core of the allocation of rights, the expression of policy, leading to the universal enforcement of intent across all data interactions. The Policy Fabric underneath the digital ombudsman must leverage the wealth of data and evolving machine learning tools to automate the ongoing

Visit us on the web at www.microshare.io

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. And, in doing so, allowing data management to remain complaint without the need for constant updates to software and infrastructure. Microshare Robots create a swarm of micro-services that examine events that introduce data to the system and automatically apply business logic, authored in simple JavaScript, to use data lookups and apply both static logic and machine learning to create attributions for all data that capture any primary and secondary owners of a datum. This occurs at the record level in a streaming fashion so that the real-time processing of the data is not significantly impacted by the application of compliance considerations.

Our Rules create an executable "language" of intent, at the core of the Microshare product, allowing for the distribution and exchange of policies across the evolving global data sharing ecosystem. That language is capable of expressing intent in both simple and complex terms with relationship context such as "allow Read-only access to my current location to all members of my immediate family" as well as environmental context such as "all Read-only access to my location to first responders only when I have signaled an emergency". Naturally such expressions need to be executable at high-speed and high-volume in a distributed world.

Combining the ownership metadata and the privacy rules to make immediate decisions on the disposition of data at granular levels is crucial to striking the balance between value-generation and compliance. Microshare's purpose-built rule engine makes the comparisons quickly with minimal computing resources to allow for the massive scale on even computational limited devices. The rules engine makes granular decisions and logs all decisions in a way that allows for the introspection of each decision: what Rule was applied, what was the result of the Rule, and, most importantly, what context was used in the evaluation of that Rule. This allows for compliance analysis and reporting in real time where necessary.

The lack of IoT standards and the problems this will create have been debated for some time. In a 2014 US National Security Telecommunications Advisory Committee (NSTAC) report, the FCC noted that IoT "requires the development of governance and policy structures much more quickly than the norm" and that "good governance will require international engagement." Sadly, precious little progress has been made to agree on standards, and the result, according to a 2018 report by IHS-Markit, is that '[s]tandards consolidation lies ahead, but confusion and fragmentation will dominate in the near term.' Microshare believes that following this shakeout period, IoT will spawn more than one set of standards, and our omnivorous approach to standards will help integrate otherwise incompatible networks.

Conclusion: Evolve or Move Aside

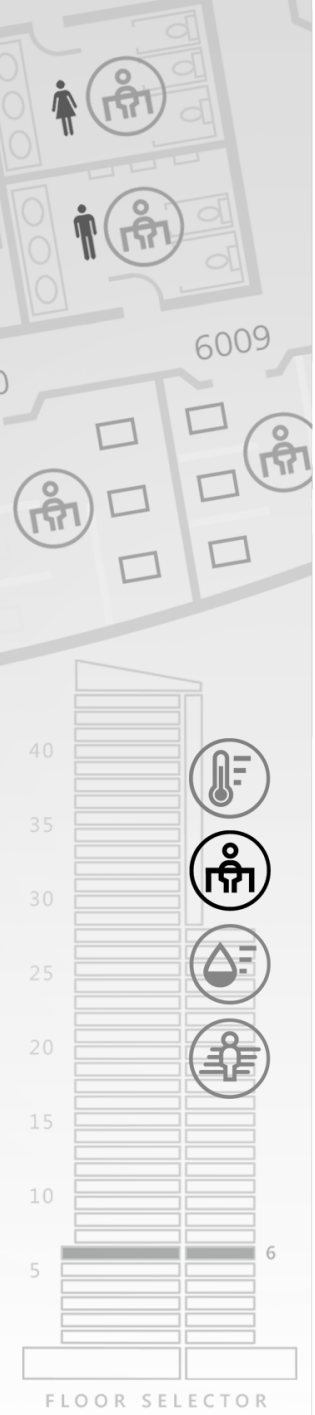
The regulatory environment for IoT – like the security environment – is immature and shot through with contradictions. Technology focused businesses, like nature, abhor a vacuum. But they abhor regulations even more, even when the establishment of some standards might clarify the risk factors and lead to an accelerating expansion of use cases and market adoption. Such is the case today with GDPR and IoT. Europe has devised a characteristically burdensome set of regulations around the capture and uses of data generated by citizens of the European Union, the world's largest and wealthiest economic market. The penalties for violating GDPR provide Brussels' regulators with the stick they need to make an example out of companies that stumble early on. This combination, along with recent aggressive actions by the EU's anti-trust Commissioner Margrethe Vestager targeting Google, Amazon, Qualcomm and others, will lead some corporate decision makers to advise caution and may slow adoption of IoT for fear of inadvertently violating GDPR's strict privacy rules.

This is understandable. A steady drumbeat of doom – and invitations to webinars and other free forums to stoke these fears – emanate from the world's largest law firms and consultancies ever since GDPR's May 2018 deadline was first aired. This has general counsels and other risk-averse corporate actors convinced that an aggressive IoT data business model is akin to Dante's crossing of the River Styx. This kind of legal hyperventilation no doubt will inflate retainers for the firms who will be called upon by general counsels to provide outside assessments of innovative new data sharing business models. And, of course, legal opinions must be obtained whenever the regulatory ground shifts. But C-suite decision makers would be well advised to take some of this with a grain of salt. Similar warnings surrounded the 2015 conclusion of the so-called "Safe Harbor" framework negotiated by the US and EU regarding the transfer of data across jurisdictional lines. This was said to be a 'digital Armageddon' for US corporates with significant interests inside the EU's borders. In practice, it merely clarified the rules of the road, updated best practices in data transfer, and probably ended some abuses at the margins.

GDPR represents a far more ambitious and fundamental change in the regulatory landscape. And, as previously noted, it coincides with a rapidly expanding new eco-system in IoT that stands to revise conventional assumptions about digital business models as comprehensively as anything since the development of the World Wide Web itself.

Happily, as with the Internet itself, technological solutions exist to help corporate strategists and data managers navigate these tricky new currents. Cloud providers offer rudimentary storage and curation options that may work for the simplest use cases. But more sophisticated business models will need a more granular and responsive data management approach to avoid triggering GDPR and other privacy red flags. Microshare's approach to the leveraging of IoT data ensures complete control and instant auditability. We turn the torrents of undifferentiated data that IoT sensors have unleashed into permissioned, annotated, contextualized, and compliant packets, before that data is ever offered to multiple third-party owners that require something more robust. Sometimes the best way to avoid mistakes is to do nothing. At Microshare, we have a better idea: Do everything, just do it right from the start.

Visit us on the web at www.microshare.io



Michael Moran is Chief of Communications and Security Solutions and Tim Panagos is Chief Technology Officer at Microshare, makers of the world's most robust data management and governance platform. Visit us at microshare.io

---

i Grover Cleveland, 1885–89 and then again 1893–97.

ii https://www.amazon.com/Future-IoT-Leveraging-Shift-Centric/dp/1543903711
The Future of IoT: Leveraging the Shift to a Data Centric World. July 6, 2017 by Don DeLoach (Author), Emil Berthelsen (Author), Wael Elrifai (Author)

iii https://www.gao.gov/assets/690/684590.pdf

iv https://www.businesswire.com/news/home/20180201005203/en/IHS-Markit-Identifies-Top-Trends-Driving-Internet

v https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework

---

Michael Moran
Chief of Communications and Security Solutions

Tim Panagos
CTO Microshare, Inc

Visit us on the web at www.microshare.io