Microshare CEO says he can save Facebook's business model

PHILADELPHIA, March 28 – The peril that Facebook finds itself in must surely resonate with many companies whose business models depend on relatively free disposition of data harvested from customers behavior. This is particularly true of platform businesses, those that offer a means for their users to interact with an ecosystem of third-party products and services. Platform businesses include the likes of eBay, Uber, Google, Amazon, Salesforce, Twitter, and Baidu. Indeed, it is increasingly difficult to find a Fortune 50 company that doesn't offer platform business features.

What platform businesses can learn from the Facebook "data breach" story is that they must worry not only about data that they themselves capture but must also worry about the disposition of data captured by the thousands of third-parties that participate in the ecosystems they have created. This so far has been an ungoverned space. At the very least, it must become a self-governed space for reasons that go beyond simply complying with regulations.

The public's diminishing trust of data-hungry apps like Facebook makes platforms an easy target for mob outrage and investor distaste when data issues arise, whether or not the app provider themselves are actually at fault. In Facebook's case, their third-party ecosystem is made-up of companies as varied in interest and intent as Cambridge Analytica and companies like Zynga, the makers of the popular game FarmVille.. Like all large platform companies, Facebook has relied on after-the-fact accusations that its terms of service were violated when third-parties misused data collected through Facebook services. Its March 28 decision to give individuals more control over privacy settings addresses some of these issues. But it also is akin to closing the barn door after the horses have fled: too little, too late.

Facebook's contention that third party bad actors overstepped their data rights may yet carry water in the court systems, but the precedents suggest otherwise. For instance, US courts already hold US companies liable under the Foreign Corrupt Practice Act (FCPA), an anti-bribery statute, for the actions of third-party contractors. 'Third party risk' has become a serious issue in the C-suite of multinational firms. Outside the courts, of course, legal niceties about such leaks will fail to impress the eyes of the wary public. The huge hit to Facebook's market capitalization clearly demonstrates that the court of public opinion is both swift and severe. The tech savvy may not know it, but in September the US Justice Department assessed a record $965 million fine against the Swedish telecoms firm Telia for third party FCPA abuses in its overseas operations. Even Facebook can't afford to ignore that figure.

"Platform business models offer too much value to the entire ecosystem to simply go away." Ron Rock, CEO of Microshare Inc. says. "The companies, the consumers, and the third-parties all benefit greatly. The market needs to find a way forward that gives each party assurances that their data is in good hands."

Visit us on the web at www.microshare.io

Large corporate entities have long struggled with distrust and public unrest. In the physical world, the appointment of an ombudsman signals a corporation's interest in preserving the trust of their customers by providing a dedicated pressure relief valve. An ombudsman, is a person within an organization charged with interceding in corporate affairs on behalf of a consumer, an ally, a problem solver. In the digital world, the assignment of human ombudsmen is simply not scalable—yet the need for reestablishing trust between service-provider and consumer has never been greater. In a recent white paper we introduced the concept of a digital ombudsmen in the context of the EU's trend-setting General Data Privacy Regulation (GDPR), which when it takes effect on May 1, will assign individuals the right to much greater control over ownership and subsequent uses of their data. Our recent whitepaper described a digital ombudsman as a scalable infrastructure that would offer to a typical end-user both continuous visibility of and immediate impact on activities that relate to the disposition of data collected about them.

In order to be effective, a digital ombudsman must:

:

- Scale in a sublinear manner with volume of data and number of stakeholders,
- Express complex and personalizable policies in executable form,
- Allow policies to change easily and immediately,
- Ensure that policies apply unilaterally—all data is covered, all transactions are enforced,
- Prove proactively that policies are in-force (stress test) and actively seek non-compliance,
- Provide transparency on-demand to regulators AND to the general public,
- Ensure that transparency is all-encompassing, and
- Allow data-centric platform business models to continue to generate revenue largely unhindered but with the added value of protecting and preserving the data intrinsic to its business.

To break that down, platform companies like Facebook deal with massive volumes of data and users through innumerable channels. A solution to data problems should neither impinge on the volume of activity nor drive-up the costs of continued activities appreciably. A proper solution would allow for a close to zero marginal cost—a target that is achievable only with the power of cloud-enabled information technology. No human solution could scale. But, the digital ombudsman must also allow for the expression of privacy policies and preferences at the macro and micro scales to address the evolving regulatory and personal requirements respectively. Policy must be changeable and allow for very granular controls. The variety, volume, and velocity of granular policy actions will be truly challenging to any current system of governance.

And no system of governance will be adequate to avoid disaster if it cannot be proven to apply verbatim to every piece of data, from every channel, through every partnership, at every time of day. Bad actors – and we seem to see plenty of them in both the Facebook example, and in other recent data breaches – invariably will find a way. But that does not excuse complacency. Policies must be immediately executable and every data transaction must pass through them. Terms of service for end-users and third-party developers must insist that all data access and any data usage be performed through a standard set of APIs so that the application and auditing of activities may be uniform. Only through the uniform auditing may complete transparency be achieved without excessive costs in time, money, and human capacity. Compliance needs to be smooth, continuous, and self-serve, just like all of the other social media services offered by platform companies.

Underlying this model of radical transparency and unprecedented consumer control is a simple notion: most people won't bother to interact. People are too busy to care that much. It is enough that they know that they could. But, make no mistake, episodic events in popular media will drive huge spikes in demand for adoption of the digital ombudsman. The offering must be real or the distrust and cynicism will only grow. We believe that these tools will allow business practices to continue largely uninterrupted. We also believe that these tools will unlock entirely new business models that may involve consumers-as-creators in monetizing transactions as partners rather than as prisoners.

"Our IP is critical to making the digital ombudsman real. But, it needs trusted brands to bring it to the market." says Microshare CTO, Tim Panagos. "The right software makes it possible but the proper brand makes it powerful."

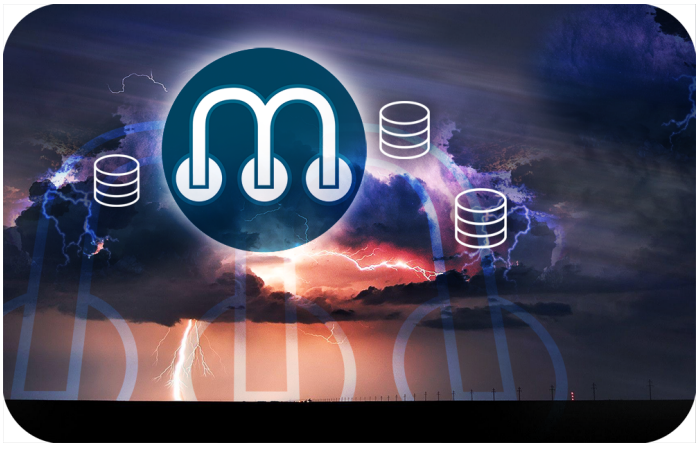
At Microshare, we have focused on the creation of the key missing component of the digital ombudsman: a multi-owner/multi-party data management product that forms the core of the allocation of rights, the expression of policy, leading to the universal enforcement of intent across all data interactions. The policy fabric underneath the digital ombudsman must leverage the wealth of data and evolving machine learning tools to automate the ongoing 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, the digital ombudsman must allow data management to remain compliant without the need for constant updates and exhaustive scrutiny of software and infrastructure.

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. 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.

Our Robots create a swarm of micro-services that examine events that introduce data to the system and automatically apply business logic, applied as lambda functions authored in simple JavaScript, to use data lookups and apply both static logic and machine learning to create attributions for both 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 insertion of compliance considerations.

While different implementations of the digital ombudsman will vary, the combination of 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. It will require a new language concerning data and the web of interwoven rights that surround its use.

"We know how to make these problems go away. Facebook can have its cake and eat it too." concludes Ron Rock. Just as, improvements in paving technology made the business models of shipping sustainable, scalable with radically altering business practices, the digital ombudsman offers data-centric, platform businesses a viable path forward. "Business-as-usual is still possible but it requires a better underlying infrastructure."



The advent of a digital ombudsman would provide concerned consumers the ability to opt-out of data-involved activities at a granular level—like unsubscribe on steroids. These tools can be used by platform companies and individuals independently or in partnership to preserve and protect both parties and their data. At this point it should be clear that platform companies have a requirement to look at issues and potential abuses at a scale far beyond those of the individual and they must proactively protect their platforms from abuse to protect themselves and their members. It is also clear that doing so without the direct involvement of the individual and their more vigilant, activist proxies will only result in further skepticism and distrust. Transparency is a crucial ingredient in the new recipe. For most, it will be enough to know that the right exists and that the option to exercise is ever-present. Few will exercise their newly available rights. The digital ombudsman will shift the onus of data awareness and privacy away from the data collector and onto the consumer. If such systems became prevalent, it is our view that government intercession would no longer be necessary as the air is let out of the outrage powered balloons that is sending these issues aloft today.

Ron Rock
CEO Microshare, Inc

Tim Panagos
CTO Microshare, Inc

Ron Rock | rrock@microshare.io | 1.215.771.7071
Microshare, Inc. | Unleash the Data | Microshare.io

Share this:
Click to share on Twitter
Click to share on Facebook
Click to share on Google+

Visit us on the web at www.microshare.io