Harvard Business Review

DATA

What If Banks Were the Main Protectors of Customers' Private Data?

by Carissa Véliz

NOVEMBER 20, 2018

MARK WILSON/GETTY IMAGES

The ability to collect and exploit consumers' personal data has long been a source of competitive advantage in the digital economy. It is their control and use of this data that has enabled the likes of Google, Amazon, Alibaba, and Facebook to dominate online markets.

But consumers are increasingly concerned about the vulnerability that comes with surrendering data. A growing number of cyberattacks – the hackings of credit watch companies Experian (in 2015) and Equifax (in 2017) being cases in point, not to mention the likely interference by

Russian government sponsored hackers in the 2016 US Presidential elections – have triggered something of a "techlash".

Even without these scandals, it is likely that sooner or later every netizen will have suffered at some point from a bad data experience: from their credit card number being stolen, to their account getting hacked, or their personal details getting exposed; from suffering embarrassment from an inappropriate ad while at work, to realizing that their favorite airline is charging them more than they charge others for the same flight.

The most practical consequence of the concerns generated by data hacking has been the imposition of more stringent privacy regulation, of which the most obvious example is the European Union's new GDPR. We can certainly expect this trend to continue around the world. And digital natives are likely to become more rather than less sensitive to the value of their data.

The obvious consequence from these trends is that the big tech firms will find it increasingly difficult to legally use the personal data they collect. At the same time, that data can be a toxic asset as it is hard to keep safe and coveted by many. A company that collects more data than it really needs is unnecessarily generating more risk because each personal datum is the object of a potential leak or lawsuit. And at least some of the personal data that companies gather generates little or no value for them – data that is inaccurate, out of date, unlawful, or simply irrelevant.

In this environment online merchants will have to find ways to do more with less data – whether through smarter application of analytics or because they introduce a business model that enables them to offer their services without collecting sensitive data. But those changes do not really resolve the underlying challenge: how can consumers protect their digitized data? Prior to the digital age, that data was kept on paper which meant it could be protected by physical means and was relatively difficult to share. Today, the IT skills needed to protect digitized data are beyond most consumers and even most of the traditional custodians of data.

This points to a business opportunity. But whose? One obvious possibility is that a few big tech companies – such as Apple, or maybe someone new – could become consumers' data guardians. Amazon, for instance, could offer an option on Prime in which it manages users' personal data for them, liaising with other companies and platforms but remaining in control of the data. There are problems with this approach. If the company is new, users might be unwilling to give up their most sensitive information to an organization that has still to prove its trustworthiness.

That would be less of a risk for a household name like Amazon, but in that instance, users might rightly hesitate to give an already hugely powerful digital corporation even more power over them.

Another option that consumers might take would be to follow the approach being explored by Solid, a project led by Tim Berners-Lee, the inventor of the World Wide Web. Solid proposes that users store their personal data in virtual 'pods' that work like secure USBs through which users can share their data with whomever they want. It is uncertain whether the project will be able to garner enough support and resources to make it workable, widely available, and affordable. Users can store their pod with Solid – in which case we bump again into questions of trust and power – or keep it themselves. But if consumers keep the data themselves, that may not be as safe as it should be—a USB, physical or virtual, can easily get lost or stolen. It would be like keeping your money under your mattress.

This analogy brings me to perhaps the most likely scenario. Maybe the best-suited institutions to manage digital data are banks. In a sense, banks are already data guardians. After all, most of the money in circulation is virtual, nothing but data. They also have a long history of being at the forefront of security methods, from the development of the vault to multi-factor authentication. Moreover, banks have experience in safeguarding privacy through their commitment to confidentiality. Finally, banks tend to have more local and personal relationships with their clients in ways that might make users feel safer than trusting their data to an international corporation. And if you're unhappy with one bank, you can always switch to another. Banks' business model and their experience give them a comparative advantage over other businesses to become our personal data guardians.

Of course, banks are far from perfect. They are notoriously conservative, which may make them slower to roll out necessary updates to the technology involved. And regulatory hurdles might make it hard for them to expand their services. But given that governments have an interest in making sure their citizens can keep their personal data safe, and that banks may need to innovate and transform themselves in order to outlive fintech competition, these possible obstacles do not seem insurmountable. Maybe someday in the not so distant future we will keep our data where we keep our money.

Carissa Véliz is a postdoctoral research fellow at Oxford University in England

This article is about DATA

⊕ **FOLLOW** THIS TOPIC

Related Topics: SECURITY & PRIVACY | INTERNET

Comments

Leave a Comment

POST

2 COMMENTS

Ben Davies 2 days ago

Good article and relevant topic. I think the underlying issues relate to both trust and interests. Banks may be bigger and better run data management businesses, but they are still businesses with a for profit interest. We expect businesses to operate in their own interests so there is a fundamental schism between that driver and the individual's need for privacy and control. We should expect businesses to use our data in their own business, we should not trust them as custodians of personal or public goods. I would far rather seen a not-for-profit organization or government agency set of for this purpose. Governments also hold much of our personal data (income tax submissions, passport data, health records, etc.), do not have a profit motive, and have been established to act (at least in theory) in the public interest.

REPLY 0 0

JOIN THE CONVERSATION

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.