Your personal data is the currency of the digital age

September 25 2020, by Guillaume Desjardins

Credit: Andrea Piacquadio from Pexels

The commodification of the internet in the early 1990s brought western societies into the digital age and has changed the way consumers interact with commercial enterprises.

The digital industry companies have one thing in common: the use of the user's personal data through technology to gain competitive advantage.

Spotify, Amazon, eBay, Apple, Google Play: these corporations have reached a level of product and service customization never seen before. Spotify's algorithm, for example, offers you artists and playlists based on your age, gender, location and listening history.

Management researchers are interested in these new forms of commerce for two main reasons: they mark a break with conventional business models and tend to do better during crises.

New business models

Recent research from the Massachusetts Institute of Technology indicates that in June 2020, at the height of the first wave of the COVID-19 pandemic, digital firms had an average return on investment of 10 percent, while traditional firms were still negative at -14 percent in August. The authors' conclusion is unequivocal: 21st century organizations must adopt these new business models at the risk of perishing.

However, this business model is not without risk for the consumer. I have been writing about this phenomenon for a little over five years. My research has led me to propose a new model for generic management of this new industry and to look at the consequences that users face.

The new business models propose a fundamental break with those typically taught in business schools. Whereas the industrial age placed capital (and mainly money) at the center of all transactions, the digital age favors information as a source of liquidity.

This disruption of the medium of exchange in a commercial transaction

is particularly salient in certain industries. Readers of a certain age will surely remember printed maps. To get updates such as street name changes, you had to buy a new map. Google, for example, offers its users GPS functionality updated in real time for free.

A personalized experience

Some firms use dual monetization in their product or service. This is particularly true in the mobile gaming industry. For example, some games use a *freemium* approach based on monetizing user data and then inserting paid elements. In short, the best of both worlds!

This type of model is not bad in itself and even has advantages for the consumer, including the personalization of their experience and access to free offers and trials.

For example, when you search for a restaurant on Google Maps, you hope to get results based on your location, and when you shop online, products are suggested based on your purchase history.

Credit: AI-generated image (disclaimer)

The customer is the product

These benefits to the consumer can also backfire. Several researchers note an increase in the complexity of the customer relationship. Studies have shown that the overload of information available in the Canadian telecommunications industry can be used as strategic leverage by the seller.

For example, a user may be required to create a Pinterest account—recording personal information such as name, email address and birthday—in order to view the site's content. Other sites will deny access to content if the user has blocked cookies or trackers for advertising.

Consumers also have the right to wonder if they are becoming the product. For example, Google uses [AdSense](#) to collect the personal data of their users in order to monetize them to third parties, generally for advertising purposes. Similarly, Google benefits from offering services at no cost, because the more consumers use its services, [the more information it collects about them](#).

It is in Amazon's best interest to encourage us to browse its site—even if we don't buy anything. The history of items viewed, keywords used or time spent on a page [can all be monetized](#).

The market for targeted online advertising is very lucrative. According to the annual Interactive Advertising Bureau 2017 report, online advertising generated revenues of [US$88 billion in the United States alone in that year](#).

Reducing your digital footprint

It's hard to be totally invisible in the digital age! Indeed, it is rare that an individual is not part of any social network, does not have a cell phone or does not use the web on a daily basis. What's more, the erosion of privacy has been so gradual that most people are not aware of [the amount of information they reveal every day](#). Nevertheless, solutions exist to reduce one's digital footprint.

Before entering their data, consumers may ask themselves if they really need the product or service, even if it is free. Is it really essential, for example, to create an account to consult a document or view an image on a site to which you will never return?

Firms that collect consumers' personal information must first obtain their consent. These consent forms are often very long and [written in jargon](#). Most people simply click on "I agree" without worrying about

the implications.

In extreme cases, this simple gesture [authorizes the firm to install spyware](#) on your device. Sites like [Terms of Service; Didn't Read](#) provides an overview of user agreements and identified the elements that could have a negative impact on the user.

All requested information?

When the consumer creates an account, they must also question the relevance of giving all the information requested. Although it is important to indicate an actual birth date on a credit application, is it really necessary to give this information on a discussion forum?

It is also important to avoid using the same username (often email) and password for different accounts. Some firms use modules to collect data that link several services. Even if information is missing from one of the accounts, the module can cross-reference that account with those registered with other providers. In addition, if there is a data leak, it becomes easy for fraudsters to test the email and password combination on different platforms.

The provider promises to secure the [personal data](#) of its user. Unfortunately, [several cases](#) of [recent leaks](#) show us that [this is not](#) always [the case](#).

Websites like [Have I Been Pwned](#) lists data leaks including email addresses and other information that may have been leaked. If your address has been leaked, it is strongly recommended that you change your password and check your accounts using the same address.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).