# What your company needs to understand about digital privacy (but probably doesn't)

August 3 2022, by Bob Needham



Credit: Pixabay/CC0 Public Domain

Digital privacy is often framed as an issue for consumers, but Ruslan Momot argues that companies need to consider the concept as a key element of their business.

Momot, an assistant professor at the University of Michigan's Ross School of Business, has published several papers on privacy issues. He shares insights about how companies should start to approach privacy, including a major shift in the way websites use cookies and how to think about data as something to be sourced sustainably.

## Why should companies, as well as individual consumers, be interested in privacy issues?

Three reasons come to mind immediately.

First, it can affect the bottom line. We consumers are quite smart, and if we know that a company is not using our data in a responsible way, some of us will use that product less or stop using it entirely. That means the company earns less revenue from its advertisers.

We've seen this happen with Facebook and Cambridge Analytica, and with WhatsApp revealing some not-very-responsible use of data. In both cases, consumers changed their behavior, and that affected the companies' bottom line.

Second, brand-new data privacy laws and regulations require companies to act on this issue. These laws will become even more stringent and more widespread in the near future.

A lot of places currently have no privacy regulations, but the most stringent regulations, such as in Europe (the European General Data Protection Regulation) and California (the California Consumer Privacy Act), say things like, "You cannot handle this data in this or that way; you need to ask for explicit consent from the consumer. You cannot just grab the data like you did 10 years ago." Companies may not want to pay attention to this, but these new laws and regulations force them to do so.

Third, companies may be able to use privacy to gain a competitive advantage in the market. If Apple is pushing their privacy agenda quite extensively, and I'm producing Android phones, maybe I should react and improve privacy for Android users. A substantial number of consumers are quite sensitive to these issues—as we've seen when 96% of Apple users chose to use Apple's newest privacy feature and opted out from their behavior being tracked across apps—and we're likely to see companies trying to compete more and more on their privacy efforts.

## Is it fair to say that most companies today do not really understand privacy issues?

It is very fair to say. In most locales, there is no proper regulation. In the places where there is at least some regulation, most companies try to comply so they can just check a box. But they rarely go above and beyond the basic requirements.

One reason for this is most companies don't have the resources. Only the biggest companies have the resources to really address privacy. For instance, one of the most well-developed computer science techniques for privacy preservation is called differential privacy.

It's like a guarantee—if an algorithm used by a company is differentially private, there is only a small chance for an adversary/hacker to infer something meaningful about its customers. To implement differential privacy throughout all a company's algorithms, you have to hire a bunch of data scientists who will rethink the algorithms that you use and will design the new ones. Apple has the opportunity to do that; Google has the opportunity to do that; but smaller companies don't.

In addition, companies may not even have proper incentives to implement privacy-preserving techniques such as differential privacy.

None of the current existing regulations require differential privacy as a standard, nor do governments have enough resources to check compliance of every company. Thus, there is a natural tendency from the companies' perspective to escape privacy preservation entirely by slacking and doing nothing.

If you had the attention of all the world's CEOs for five minutes, what is the biggest thing that you would try to convey to them about privacy?

You need to start thinking about it now (or, actually, yesterday). For the past 20 years or so, we've been pushing this big-data agenda, collecting more data, using the data, harnessing the power of the data.

Now we have a movement in the opposite direction, what we could call sustainably sourced data. The cycle resembles that of sustainability issues. Suddenly consumers started paying attention, and companies started to sustainably source things.

Now we have all these organic, sustainably sourced goods. Why don't we have the same thing with data? The message is that you need to start thinking about how to sustainably source your data and how to responsibly use that data.

## Is this idea of sustainable data taking hold?

We're starting to see a little bit of this. Next year, I think what we'll see is that third-party cookies will disappear, and that means that we will be left with what is called zero-party cookies and first-party cookies.

These are pieces of information that consumers give to a company with explicit consent. So in a sense, it's sustainably sourced data because we didn't collect this data from third parties like data brokers. Instead, consumers give explicit permission to use this data. I think we'll be

moving toward that.

What steps can a company take, if its leaders want to be smart and responsible and start sustainably sourcing their data?

First, companies need to be up-front with consumers about what is happening with their data. Will it be sold to the brokers the moment they receive the data, or will it be used for the internal purposes of the company—for example, to make the product better for the consumer?

Another starting step would be to comply with the most stringent privacy regulations. Take a look at the European General Data Protection Regulation and try to comply with it, even if you're a U.S.-based company, because it's a good framework.

Then, there are broker companies that are collecting this zero-party and first-party data, where consumers explicitly provide the data to the companies. You can source your data from those brokers.

You can also think about what you do with the data. Where does this data go? You need to understand the supply chain of the data, so you can make sure that the data doesn't go to the irresponsible brokers, and it's used in a responsible manner.

## So you think about data as a supply chain?

It is a supply chain. Let's say you use a weather application. The app tracks your GPS location, and this GPS location is sold to a data broker. The broker uses this location, matches it with other data and infers something about you. Then this list of inferences about you is sold to some other companies and so on. So the data travels.

# What else should companies be aware of when they start thinking about privacy?

Many companies operate with a disconnect when it comes to privacy. A lot of companies think about privacy from the legal perspective; the people who are responsible for privacy are law people.

At the same time, we have a computer science community which has been developing all these concepts like differential privacy for many years. There has to be this bridge between the two. Improving consumer privacy has to be done by people who are familiar with both sides—with the regulations, but at the same time with the theoretical and engineering component.

Similarly, when we think about privacy, it should not be only about IT departments. Preserving consumer privacy should be embedded into the business model of the company, in the same way that sustainability should be part of the business model.

Management should be centered on consumer privacy. It should not be a patchwork, like, "Hey, yeah, we are creating this product, let's ask our IT guys to protect privacy." It will never work. For it to work, it has to be deep inside the business model of the company.

Provided by University of Michigan

provided for information purposes only.