Nico van Eijk: How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?

van Eijk, N.

Publication date
2018

Document Version
Final published version

Facebook

Nico van Eijk: How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?

August 6, 2018

By Nico van Eijk, Professor of Information Law at the Institute for Information Law

This post is part of a series on data portability and interoperability.

Data portability will help users move to other service providers with more ease. It will promote the consumers' interest when they want to switch from one digital platform to another. And it will contribute to more competition between companies. These, at least, were the most important arguments for the creation of a consumers' right to take their data with them, now a key element of the new European privacy law, GDPR, that recently took effect.

Who could object to such noble goals? This is exactly the right question, only much of the current debate glides past it. Too often data portability is viewed as a binary interaction involving the consumer who wants to move their data elsewhere and the service provider that currently holds the consumer's data. In the ideal world of data portability, these two parties reach agreement about moving the consumer's data and everybody moves on.

But the simplicity of this transaction breaks down when you start asking yourself exactly what data you're referring to. The posts and videos showing your music preferences? Information about your behavior on the internet, like your search results? Or products you bought?

There is also the elemental fact that a lot of 'your' data is actually someone else's too – all of your friends. The internet and the digital platforms you use are of such great value because they allow you to interact with so many others. You share photos of you and your friends. You exchange comments on news articles posted on social media. And you keep all your friends in your contacts. Considering that factor, should they have a say when you move 'your' data to another service provider? Should you have to ask for their consent?

Under Europe's new laws your friends' interests are completely irrelevant. There might be good, practical reasons that led to this. You can't ask everyone who you've been in touch with for permission when you transfer your data, and even after you do the social platform that receives the data must comply with the European data protection rules. But is this what your friends expected when they engaged in an information exchange with you? Or did they engage because they found comfort in the fact that you were using a service provider they too chose to trust? The fact that the formal data protection rules apply to all providers is important and highly relevant. But how does your friend know whether the new provider is fully aware of the terms of agreement that you and your friends had under your previous service provider?

Data portability raises important questions about users' reasonable expectations and trust in their friends and providers. And it goes beyond ensuring that providers are compliant with data protection legislation. If you consent for a friend to use your data on an alternate service, what happens if that service misuses the data? What happens if that friend misuses it? In other words, consent may not be sufficient to ensure that people's data is used only in the way they intended.

Users moving data to less trustworthy providers might have a serious effect on the entire ecosystem. This is no theoretical matter. It relates to questions we're all quite familiar with in everyday life. We prefer certain suppliers above others because they provide higher security levels and exceed the minimum legal requirements on consumer and data protection We prefer financially solid service providers above those that are underfunded. We don't want our information to be exploited by advertising models that are – morally –

beyond our standards.

Data portability is not between two parties. It's about managing a complex traffic hub with conflicting interests. It requires users and providers to look at the intertwined interests of many in ways that go beyond simple compliance.

There is a broader spectrum of responsibility that should be considered. As a user it should include taking care of our friends. As a provider it should mean taking care of users – both past and present. In law, as with philosophy, we often define these kind of principles as so-called 'duties of care'.

Fulfilling these responsibilities can take many forms. Users could inform their friends of their intention to move to another provider and offer them options: partially or entirely opt out, or give their consent. Providers could facilitate users by consulting with their friends about their options. Or the provider who will be porting the data could inform the receiving provider about applicable limitations beyond the minimum legal limitations set by data protection laws or other legal requirements.

Steps such as these are fundamental to a trustworthy environment and deserve more attention than they thus far have been given. They also underscore that data portability is a means and not a goal in itself.

Nico van Eijk is professor of Information Law at the Institute for Information Law (IViR, University of Amsterdam).

Categories: Data and Privacy, Facebook, Hard Questions

Tags: Platform