Digital services collect unnecessary personal information

Date:
October 9, 2017
Source:
Karlstad University
Summary:
Digital services that require users to log in with a personal account often collect more information about users than is needed. Certain policies may encroach on our privacy.
Share:
FULL STORY

Digital services that require users to log in with a personal account often collect more information about users than is needed. At an international conference about digital identities at Karlstad University, research is presented about methods service providers use to collect personal information about users that may encroach on our privacy.

When one creates an account to get access to an online service, the service provider requires certain details to identify users who want to access their accounts. There are existing methods that can be built into such services to protect users and their privacy under certain circumstances. However, many service providers choose to use other methods to collect as much information about us as possible, and so frequently threaten online user privacy.

"We have for instance seen that some service providers ask for information that they do not need for the main purpose of the service they offer," says Lothar Fritsch, researcher in IT-security at Karlstad University. "They may ask for details while assuring the user that these will not be shown publicly or are protected by a user policy. These details are then used to find out as much as possible about users to enhance their business opportunities, something which is not mentioned in any agreements."

Apps are also used to access information about users. When we install apps on our smartphones, access to certain information is often required. Many studies have shown that it is difficult for users to comprehend the flow of information and what one actually agrees to, and when one has given the required permission it is difficult or almost impossible to revoke it.

Data fragments are used to identify the user and at the same time retain anonymity. There are different types of fragments that may be used for identification. If someone gets access to several different fragments, these can be linked and the user may be identified.

"When we as users give apps access to certain information on our smartphones, we also make it possible for the actor behind the app to identify us. We want to find ways to make users aware of what it means when apps receive access to certain types of data on our smartphones," says Nurul Momen, doctoral student in Computer Science at Karlstad University.