user data manifesto

news:
\"In
Posted 1 year and 6 months ago

This manifesto aims at defining users' fundamental rights to their own data in the Internet age. People ought to be free and should not have to pay allegiance to service providers.

0. **User data** means any data uploaded by a user for his or her own use.

× Examples of user data include:

- the files a user is syncing through multiple devices or sharing with a friend
- a library of photos, books or other files a user uploads from their device in order to be able to read, view or modify online
- data generated by a user's device (like a connected watch or theromstat) and sent to a server
- a user's search engine queries, if they are logged as such

Thus, users should have:

1. **Control** over user data access

   User data should be under the ultimate control of the user. Users should be able to decide whom to grant direct access to their data and with which permissions and licenses such access should be granted.

   × When users have control over the upload of their data, data intended to be privately shared should not be accessible to the service provider, nor shared with governments.

   That means the right to use cryptography should never be denied.

   That also means that when users do not have full control over the upload of their data (e.g. if they don't use cryptography before uploading) a service provider should **not**:

   1. force users to disclose private data (including private correspondence) with them, nor
   2. impose licensing conditions (e.g. on copyright, or personal data exploitation) that go beyond what is necessary for the purpose of running the service.

   When users make data available to others, whether to a restrictive group of people or to large groups, they should be able to decide under which permissions they grant access to this data. However, this right is not absolute and should not extend over others' rights to use and exploit the data once it has been made available to them. What's more, it

does not mean that users should have the right to impose unfair restrictions to other people. In any event, technical systems should not be designed to enforce such restrictions (e.g. through DRM).

Data generated or associated with user data (e.g. metadata) should also be made available to that user and put under their control just like the user data itself.

× Some services allow users to submit data with the intention to make it publicly available and usable by all. Even in these cases, some amount of user data is kept private (e.g. metadata or social graph data). The user should also have control over this data.

2. **Knowledge** of how user data is stored

When user data is uploaded to a specific service provider, users should be informed about the geographic location that specific service provider stores the data in, how long, in which jurisdiction that specific service provider operates and which laws apply.

× When users use centralised services that uploads data to specific storage providers instead of relying on peer-to-peer systems, it is important to know where the providers might store data because they could be compelled by governments to turn over data they have in their possession.

This point is not relevant when users are able to store their own data on devices in their vicinity and under their direct control (e.g. servers) or when they rely on systems without centralised control (e.g. peer-to-peer).

× Users should not rely on centralised services. Peer-to-peer systems and unhosted applications are a means to that end. In the long term, all users should be able to have their own server with Free Software.

3. **Freedom** to choose a platform

Users should always be able to extract their data from the service at any time without experiencing any vendor lock-in.

× Users should not get stuck into a specific technical solution. This is why they should always be able to leave a platform and settle elsewhere.

Open standards for formats and protocols are necessary to guarantee this.

Obviously, without the source code of the programs used to deal with user data, this is impractical. This is why programs available to exploit exported data should be available under a Free Software (Open Source) License.

If users have these rights, they are in control of their data rather than being subjugated by service providers.

Many services that deal with user data at the moment are gratis, but that does not mean they are free (as in freedom). Instead of paying with money, users are paying with their allegiance to the service providers so that they can exploit user data (e.g. by selling them, licensing them or building a profile for advertisers).

Surrendering privacy and other rights in this way may seem to many people a trivial thing and a small price to pay for the sake of convenience that these Internet services bring.

Service providers have thus been unwittingly compelled to turn their valuable Internet services into massive and centralised surveillance systems. It is of grave importance that people understand and realize this, since it forms a serious threat to the freedom of humanity and to the privacy of each individual.

Ultimately, to ensure that user data is under the users' control, the best technical designs include peer-to-peer or distributed systems, and unhosted applications. Legally, that means terms of service should respect users' rights and give them the possibility to exercise the datarights defined in this manifesto.

---

l10n: Deutsch Français 日本語 Türkçe

Last edited 1 year and 7 months ago