Data Transfer Initiative

Principles to guide public policy in data portability

The 501(c)(4) non-profit Data Transfer Initiative (DTI) is committed to enabling simple, fast, and secure data transfers through data portability at scale.

Data portability empowers users by enabling them to transfer copies of their data to other products and services, and enhancing innovation by making it easier for organizations, startups and small businesses to attract new users. The flagship effort of DTI is the open-source Data Transfer Project (DTP). Since it was founded in 2018, DTP contributors have leveraged deep expertise in data portability to advance data transfer techniques that make it easier for users to control their data and share it across services in a more secure manner.

DTI's 5 principles for portability and data interoperability:

build for users, privacy and security, reciprocity, focus on user’s data, and respect everyone.

Supporting these principles is a requirement for partnership in DTI, although the open source code base is available for use by anyone. These principles have been implemented in practice by DTI partners, who have used them to guide product development and to inform discussion with users, large and small tech platforms, nonprofit organizations, academics, and governments about how to advance data portability safely and effectively.

DTI intends to share its expertise and lessons learned from building data transfer products in order to help educate those developing the laws and regulations that govern data portability. Public policy regarding data portability should emphasize empowering users to transfer their data, protecting privacy and security of data, and clarifying liability for data transfers.

[1] https://github.com/google/data-transfer-project

https://dtinit.org

DTI

Public Policy Principles to Unlock the Potential of Data Portability & Increase Innovation

Empower users to transfer their data

- **The transfer of a user's data should be initiated by the platform only if requested by the user themselves.** It should not require the disabling of features, such as end-to-end encryption, that serve user choice and interests.
- **Portability policy should focus on user-created content** and should not extend to data that negatively impacts the privacy of others or that is used to improve a service (e.g. "inferred data").
- **Data transfers should be reciprocal** in order to ensure that users can transfer data from any service. Portability policy should not require a service to support direct transfers to a destination without reciprocal obligations on the recipient.
- **Data portability should be supported in any industry** where it will empower individuals to use their data in their choice of products or services.
- **The recipient of a portability transfer should be able to use the data for any legitimate purpose**. Once a user transfers a copy of their data to a new service, that service may treat the data as if the user had provided it to them directly.
- **Governments should not use portability tools to conduct surveillance** or obtain proprietary data, nor compel users to do so.

Protect privacy and **security** of data

- **Legislation should specify minimum privacy and security practices** that govern data transfers.
- **Platforms should not be required to substantially threaten the privacy and security** of individual users or the platforms. Platforms may require baseline privacy and security standards, including shared certification or accreditation processes, as a condition of enabling data transfer.
- **Governments should support research** on the impacts of data portability and interoperability within data types on competition, innovation, privacy, and security, as well as the potential for common technical standards to reduce the costs of building portability solutions.

Clarify liability for data transfers

- **Data recipients should not be liable for accessing data through a legitimate transfer mechanism** once the data recipient has a valid legal basis to do so.
- **Data recipients should bear any potential liability for** transferred data once it is imported by that provider's service, and should bear responsibility for responding to government requests related to that data.
- **Governments should not hold liable a company for** transferring data at an authenticated user's request pursuant to a legitimate data transfer protocol.