Realising the Right to Data Portability for the Domestic Internet of Things

Nature of the Right

Article 20 General Data Protection Regulation (GDPR) 2016 provides data subjects a right to data portability in their personal data. It contains two elements:

A 'right to receive' the data from the data controller in a structured, commonly used, interoperable and machine-readable format (e.g. CSV).
A parallel 'right to transmit' data to another data controller, without hindrance. Where possible it should be directly between controllers.
The motivation behind portability is:

- to empower users through increased control and choice around their data;
- to foster competition between service providers towards new data handling approaches;
- to disrupt commercial norms of vendor lock in and big data analytics.

Relationship between IoT and RTDP

Nascent Internet of Things (IoT) industry faces privacy and trustworthiness questions due to opaque, ambient data collection and use. IoT involves detailed inferences about daily life but:

- Consent is hard to obtain,
- Data can be repurposed,
- International data transfer is prevalent due to cloud storage
- Lack of transparency in big data analytics minimises the user's ability to exercise meaningful control.

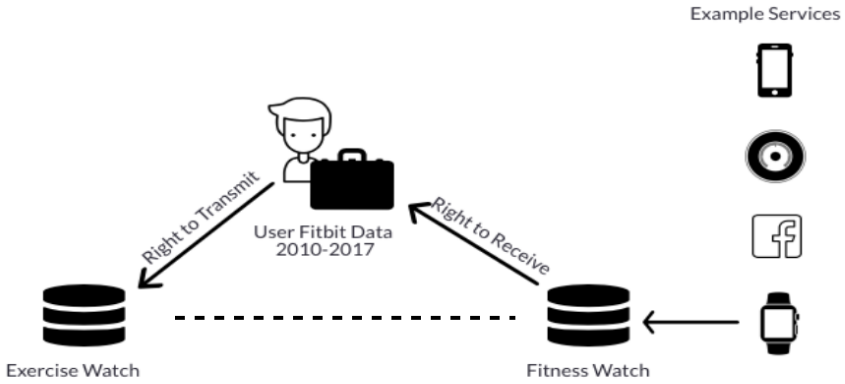

Figure1. The RTDP Process

Introducing PIMS

RTDP prompts a different approach for IoT. DP law foresees an increased role for technical regulatory solutions due to Art 25 GDPR mandating Data Protection by Design and Default.

Personal Information Management Systems (PIMS) offer promise for rebalancing power asymmetries between users and services. They put users' closer to their data, increase control over sharing/access, and challenge business models of 'if you're not paying, you're the product'.

Technical Barriers

Low Usability

Data portability is still a distant concept to the average user often because of the highly technical nature of the subject and solutions involved. While privacy enthusiasts might be comfortable parsing CSVs and XMLs and running scripts for uploading and retrieving data through API invocation, the average user needs simple, fast and useable solutions that make the decision of porting data conceivable and practical.

Overcoming hyperbolic discounting

While interacting with technologies like personal data containers there is a very high possibility of low user engagement due to hyperbolic discounting. To ensure active user participation with such technologies,

there must be more research that explicitly demonstrates the value of use of such technologies and the higher symmetry of power it offers. This would compel them to adopt such measures into their everyday data interactions, by default.

Platform Differences

Porting data between platforms triggers numerous questions directed at the user, which could lead to intimidation and poor decision making. An example of this could be UI differences between the two platforms. If the two UIs do not follow similar formats, the transfer could be arduous and even meaningless. Transferring data from an image-based platform to a text based platform could highlight several inconsistencies which could lead to a dysfunctional result.

Personal Information Management Systems

MyDex
Allows users to gather, organise and share personal data
Allows data transfer at different levels of granularity,across multiple formats and platforms

Higgins
Provides storage and locus of control to manage personal data
Allows data transfer by exporting to RDF files, as per the users' request

OwnCloud
Self-hosted file sync and share server
Supports data processing by applications through APIs
Data types accepted are currently limited

Locker Project
Client based, with attribute store on the user's personal computer
Uses APIs that allow services to access personal data

Databox
Forms a central hub for collation of diverse data sources
Users in control of sharing and management of personal data with various competing service providers

Legal Barriers

Limitations of RTDP

It provides control of raw data but does not cover inferences from subsequent analytics e.g. statistical profiles. Many harms stem from profiling like second order impacts of prejudicial treatment or denial of access to services. Significant shortcoming for IoT where inferences key to determine context and service delivery eg Nest learning thermostat heating profile.

Opacity and Establishing IoT Data Controllers

The lack of legibility and transparency in opaque IoT data flows make it hard establishing who to send RTDP request to e.g. interacting with different service providers and sensors in various settings, from smart home to smart city.

Nature of Control

There is a risk PIMS commodify intimate, sensitive personal data as a tradable asset for users. Higher risks to financially or socially vulnerable users losing their privacy rights by need for income e.g. those in fuel poverty trading energy data for money. Creates risk of a digital divide between those who can afford privacy and those who cannot. This contradicts human rights roots of EU DP Law, providing fundamental right to all.

By,
Dr. Lachlan Urquhart, Horizon Digital Economy Research, University of Nottingham,
Neelima Sailaja, Mixed Reality Laboratory, University of Nottingham,
Prof. Derek McAuley, Horizon Digital Economy Research, University of Nottingham.

SCAN

horizon DIGITAL ECONOMY RESEARCH

Research Councils UK Digital Economy Transforming Business and Society

University of Nottingham UK | CHINA | MALAYSIA