Response to UN call on Children’s Rights in the Digital Environment

30 April 2019

HATLAB is a consortium managed by the HAT Community Foundation
8 Comberton Road, Barton, Cambridge CB237BA, UK
www.hat-lab.org

About us

DROPS is a £1.2m EPSRC-funded project in the UK, led by Professor Irene Ng at University of Warwick, with Professors Roger Maull, Glenn Parry, Natalia Kucirkova and Dr Asimina Vasalou. The DROPS project aims to create decentralised models of personalisation to ensure equitable benefits of personal data-sharing for both the organisation and the individual. It investigates the technology, business, economic and legal models of personalisation with children's publishers and app developers. The project is a collaboration with the HAT Community Foundation and uses HAT Microservers as personal data accounts.

Key issues and the DROPS team's perspective

We believe that children's data rights are not adequate in centralised digital environments. The challenge ahead for all of us is to develop models in which the sharing of personal data is safe, secure and beneficial to the person, industry and society. Ethical data-sharing can be used for data mobility, which is essential for innovation. Today's Internet is based on centralised digital environments, where the data we produce when we utilise the Internet is stored and protected by the companies that give us websites and mobile applications. This centralised data-sharing model requires consent for sharing, but in a form that is often not meaningful and can be easily abused.

Thus far, a common response to remediate the problem of personal data consent has been to give "control" back to individuals. This is often an empty promise, as terms and conditions usually dictate that users give up all rights to access and manipulate their data to the service provider in exchange for service. Further, control is insufficient, particularly for children who have no "control" over their data to begin with. In this centralised digital environment, parents and guardians have to depend on every application to deal with their children's data in their own way. For applications based on responsible and conscientious data models, user control of personal data would not be an issue, but there is very little guidance on how to do it well. Best practice models for data-sharing in centralised systems are lacking, making it more difficult for the design industry to develop suitable and responsible personal data-control models. Moreover, guardianship over children's data is not possible in centralised systems, owing to the fact that the data cannot be suitably isolated.

Given these issues, the only rights possible for individuals' data within centralised systems are the eight rights accorded under the EU General Data Protection Regulation (GDPR). GDPR constitutes an essential condition in the data-sharing economy.

However, with GDPR, individuals do not have five crucial data rights that can be considered as genuine “ownership” rights.

The need for genuine data “ownership” rights

1. ***Right of possession****. Having their data stored in a place where they are the only one who have access to the data.*
2. ***Right of control****. Being the only ones deciding who gets to use their data and when.*
3. ***Right of exclusion****. Deciding who doesn’t get to use or see their data.*
4. ***Right of enjoyment****. Being able to use their data for their own purposes whenever they wish.*
5. ***Right of disposition****. Being able to monetise, exchange, profit, license their own data because they own the rights to it.*

These five ownership rights align with decentralisation and are, in our view, crucial for children’s data rights. Our rationale is that from a legal perspective, individuals currently cannot have Intellectual Property Rights over data itself i.e. individuals cannot legally “own” data - rather it is the database, data controller, data analysis and the use of data which are legislated. Moreover, individuals cannot freely re-use or re-share their personal data if they don’t legally own the rights to it. For example, if parents wish to take their children’s data from primary school to give it to a secondary school, the channel for sharing might be closed by the primary school, as it is their right stemming from their status of the “source” of data. This implies that without data rights that would allow individuals to license the data they own, individuals are at the mercy of original data sources. Data rights need to be more broad-based and ideally decentralised to individuals themselves; otherwise, data-sharing will not work and further privacy intrusions are likely to occur.

Broader ownership rights are also necessary to incentivise wider use of data. The right technologies can partially decentralise the Internet. For instance, technology like the HAT Microserver has for the first time given individuals the capability to hold, process and control their own data for themselves. The HAT Microserver enables individuals to have ownership rights (“Sui Generis”) to a *database* and the data and contents within it.

The use of such decentralised data platform technologies can also help ensure that children are adequately protected when it comes to sharing their data over the Internet. Children under 16 may be less aware of the risks, consequences and safeguards to their personal data rights. This is largely because of the verbosity of the terms and conditions that accompany the requisite permissions for data-sharing, which challenge even the most discerning adults. Generally speaking, children are also less aware of the structures and business models that underpin Internet services.

This is why both the EU GDPR and the USA's Children's Online Privacy Protection Act (COPPA) are promoting the concept of 'verifiable parental consent' for children under the age of 16. This compels the data controller (usually an app or service) to use 'clear and plain language that the child can easily understand' in their Terms & Conditions for the data transaction. The data controller also needs to make reasonable effort to verify that consent is given by someone with parental or guardian responsibility over the child, taking into consideration the 'available technology'. In COPPA's words, the data controller needs:

'to ensure that the parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorises the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from the child.'

In our project, we draw on the GDPR and COPPA guidelines and have developed technologies that address the data-related issues with current technologies.

Our suggested technological solution

The HAT Microserver technology allows the parent or child's guardian to authorise the right to data access on behalf of the child, through the child's HAT account. This is done through a confirmation of executions and permissions for all requests received from applications to interact with the data stored in the child's HAT account. As part of this confirmation, a HAT owner can also license the usage of data through a data debit, before any data goes out of that HAT; very much like a direct debit transaction during payment. With our technology, a parent or legal guardian of the child gains control of this process, making it possible for them to exercise other rights such as stopping the data exchange, in case the parent deems the exchange risky, for example.

More importantly, the parent at this stage *only* sees the meta data: the data points concerned, instead of all the actual value behind each data point. This means that to make a decision about whether or not to consent to the data transaction, the guardian does not see the details of individual data points. For example, the meta-data that the parent/ guardian would see are 'name, age, songs listened in the last hour' but not the details such as 'Joe Adams, 7, song title X'. Such an approach to consent ensures the protection of the child's privacy as well. Should the parent/guardian require the whole dataset (both meta- and data points behind the meta-data), then the child can allow such visibility via the consent to the parent access.

The HAT technology offers a seamless infrastructure for this approach. From the user’s perspective, the data transaction processes happen without too much effort, in an interaction similar to, for example, the use of Google apps. The HATDeX platform will be implemented in the DROPS project on personalised children’s learning using E-books. For more information regarding the project or this document, please contact Natalia Kucirkova (Professor of Early Childhood and Development), n.kucirkova@ucl.ac.uk or Yin Lim (Senior Policy Associate for HATLAB), y.f.lim@warwick.ac.uk.