Workshop on Digital move

Empowering families to move freely online: harnessing the full potential of the internet through genuine data portability

Families on the Move conference
www.coface-eu.org/consumers/families-on-the-move

With the support of:

CAMPUS HOGER INSTITUUT VOOR GEZINSWETENSCHAPPEN

Gezinsbond

la ligue des familles
citoyenparent.be

Reality check and State of play

The Internet has become an integral part of the lives of families all across the world, yet few reflect on its governance, a key aspect to secure certain elementary freedoms like the freedom of movement. Moving freely online doesn't just mean being able to consult any website you want, but also being able to consult them in similar conditions (the debate about "net neutrality") or being able to switch online services at any time which is what the workshops on "digital move" focused on.

Just like any service, the Internet is prone to centralization and lock in:

- centralization as in the concentration and control of a major part of its infrastructure and/or content in the hands of one or a few major players;
- "lock in" meaning the difficulty of users to switch services or online platforms.

This phenomenon is not unique to the Internet and centralization and the "lock in" effect have been seen in many other industries like the telephone operators which in many countries functioned as quasi monopolies and made it very difficult to switch operator (you had to give up your phone number).

With regards to the Internet, we need to distinguish the hardware/network (the cables and routers which link every individual's computer together) from the content/services (the data and the online services). The hardware and networks were designed, from the outset, in a decentralized way and for very important reasons: to make sure that even if one part of the network failed, the "traffic" would be redirected instead of being stopped. Think about it as a spider web: if you need to go from one point to another in a spider web, even if one thread of the spider web snaps, there are many other possible routes you can take.

With regards to the content/services side, we have seen a growing concentration in the hands of a few companies: Google, Facebook and Amazon. This concentration is detrimental for many reasons. For instance, a successful cyberattack on Amazon cloud services could take down huge parts of the Web (the web pages would no longer be available). Another reason is the user experience: by reaching near monopolistic positions, these giants can impose abusive access conditions and unfair business models. The growing prevalence of online advertising on social networks or video sharing platforms and the increased exploitation and gathering of user data are directly linked to this centralization process: by "locking in" the user, you can exploit his/her data and make him/her watch more targeted advertising, and not only for commercial reasons but also, increasingly, for political reasons during election campaigns. Centralization also enables easier censorship, be it from private actors or governments.

While there is a natural tendency for centralization, certain decentralized solutions, developed especially within the "Open Source" movement and community, have gradually emerged over the years. Too often, however, these solutions are taken up by the "geeks and nerds" community and never make it to the wider public.

HWC (Homebrew Website Club), represented by **Nicolas Collignon** and **Ricardo Mendes** is an example of a young company which aims at bridging the gap between readily usable decentralized solutions from the "indie web" and ordinary Internet users by hosting informal gatherings to exchange expertise and knowledge about how these solutions work. They also directly help NGOs, small businesses and other actors to make the switch to decentralized solutions which are often cheaper and more respectful of privacy than commercial solutions.

In concrete terms, HWC proposes such services as self-hosting which enables anyone to directly host their website/content without subscribing to a commercial online cloud service. Among the self-hosting solutions, we find Cloudron, Yunohost, Nextcloud, Rocket.Chat, and many more.

Examples of other decentralized service include Diaspora which is a decentralized social network and Signal which is a highly secure and privacy respectful messaging service with end-to-end encryption. The use of VPN (Virtual Private Network) is also listed as a privacy enhancing solution.

Finally, HWC explores various hardware solutions for increased privacy and autonomy such as the "Internet Cube" which enables self-hosting and VPN in one hardware, or Nextcloud box which also allows you to host your content directly from your living room.
HWC organizes monthly meetups in Brussels open to anyone.
Wikimedia, represented by **Dimitar Dimitrov,** on the other hand, is an example of an online service provider whose mission was to enable every single human being to share their knowledge for free, exemplified via its most successful projet to date: the Wikipedia encyclopedia.
The foundation builds their projects based on a number of core values and a firm belief in digital rights. Yet they also faced the same challenges as any other company on the Internet: how to deal with illegal content, harassment, censorship and so on.

To each challenge, its original response:

- Illegal content is being taken down in cooperation with law enforcement, when multiple jurisdictions apply, the strongest of the multiple laws applicable is taken as reference. Criminal content is not blocked but fully deleted. Such requests are rare however, given Wikimedia's core business. Illegal content is different. For instance, regarding copyright infringement, there is a discussion around each deletion to strike a balance between deletion for valid reasons and censorship.

- With regards to violence, nudity, or any other form of shocking content, Wikimedia has decided to accept or delete it depending on whether it was treated "encyclopedically" or not; in essence, whether the content fulfils some kind of educational purpose or is irrelevant to the subject being explored.

- Inaccurate or low quality content is dealt with by strengthening the community participating inside Wikipedia and reinforcing the skills of the contributors, but also in providing a space for editing and discussing the content and cultivate values of cooperation, deliberation and democracy by allowing users to vote

and have a say on the contents of Wikipedia.

- Finally, with respect to harassment, Wikimedia adopts a "zero tolerance" policy making it clear that harassment is not and will not be tolerated, thereby opting for "social" solutions rather than technical solutions such as censorship.

Joe McNamee from **EDRi (European Digital Rights)** gave examples of cases where censorship or other technically driven solutions to solve human behavior online resulted in creating side effects which were sometimes worse than the problem meant to be solved:

- In Belgium, the censorship of newsgroups for music by the music industry was used by users to create a list of the best places to get music since newsgroups were not censored equally by all Internet providers.

- The no longer existing Dutch social network Hives created a system which was meant to tackle cyberbullying and harassment based on user reporting. If the social network received 10 reports from different IPs, it blocked the content/person. This system was used by teenagers to bully others by grouping together to block a person.

The issue of censorship is also treated selectively in many parts of the world. In the United States for instance, depending on which organisation you are, "freedom of speech" can apply or not. For instance, Wikileaks has been a victim of attempted censorship via paralegal means: by persuading companies like Cloud hosting or financial services to stop providing their services to Wikileaks.

During the discussion, many issues were raised and some ideas proposed:

- While technical solutions to social problems may not be the panacea, they have proven to be effective when being well designed. The (technical) rules which govern the editing and contribution process of Wikipedia have yielded stability and good overall quality of the content. As decentralized solutions are being rolled out, it is key to determine how to address problems of harassment or criminal content given that many such solutions do not have a "central authority" to contact regarding liability or take-down, especially given that very often, being uncensorable and fully anonymous is part of their underlying code. Some balance needs to be struck between technical solutions/rules embedded in decentralized services and social solutions (education, fighting stereotypes, social and emotional learning, values, critical thinking, resilience…).

- Decentralized solutions can enhance democracy via their participatory nature, embedded in their code.

- There is an inherent tendency for networks to centralize themselves in a self-reinforcing way. Everyone uses Whatsapp and Facebook because everybody else uses Whatsapp and Facebook. To ensure that decentralization becomes a norm forces us to identify the root causes of centralization and address them directly in the design of decentralized solutions.

- In order to fully realize the potential that decentralized solutions present

such as self-hosting or alternatives to social networks and other platforms, two elements are essential:

- Achieve interoperability between the various decentralized solutions in order to minimize the likelihood of a "lock in" effect. There are many examples of decentralized services which are interoperable such as email. Regardless of which email provider you choose, you can send emails to all the others, and you can also export/import emails from one email client to another with relative ease.

- In the future, in the spirit of data minimization, we may need to move towards a "decoupling" of the data layer from the services layer. Some decentralized solutions already propose such a service like the "Freedom Box" which aims at centralizing a users' data and hosting it directly on a home server. A decoupling of the data layer from the services layer would mean that the services you use (email, social networks) would not store your data on their own servers, but the data would be stored via a decentralized service chosen by the user and users would give an authorization to services to access parts of that data. This comes with many advantages: users would not need to "reupload" multiple times a similar content across multiple services (for instance, a video or a picture) and this might clearly help in breaking the "lock in" effect of current online services.

  Decoupling the data layer and the services layer comes with many prerequisites: harmonizing to some extent how data generated is stored (using standard database language like SQL or JSON), ensuring strong protection for user generated data and the uses that services can make of the data (preventing users to be pressured by services to give access to all their data, with the risk that it will be used against them: creditworthiness, health insurance, political marketing…).

Actions and next steps

Decentralized solutions are growing, there is no doubt about it. But what is happening at the policy level? These developments have not gone under the radar and at the EU level, both the European Commission and the European Parliament have started moving, in a more or less direct way, to facilitate a healthy transition to decentralized technologies.

Fabrizio Sestini from the **DG CNECT Next Generation Internet Unit** gave a presentation on programmes funded by the European Commission on the future of the Internet, with a specific focus on democratic values. The Internet's future can head into many directions: dominated by a handful of corporations focusing on their commercial interest, managed by Internet users themselves via open source, decentralized platforms and various technical solutions, or some form of balance between the two.

Financing decentralized projects which put focus on user participation and democracy makes sense from the perspective of the general interest, given the risks that a concentration of power in the hands of a handful of companies present: privacy risks, stifling of innovation, barriers to entry, commercial exploitation of users…

The CAPS projects (Collective Awareness Platforms for Sustainability and Social Innovation) is one of the FP7 research projects funded by the EU Commission, developing technical solutions to promote open democracy, collaborative consumption or Internet Science. The core values associated with these digital social innovation initiatives are: participation of people, openness (to new ideas and open source), bottom up (leverage people's creativity) and decentralization.

Examples of CAPS projects include:

D-Cent: a tool for democratic participation and citizen empowerment, used among other things to propose and draft policies in a collaborative way, decide and vote electronically, and encouraging people to participate with a blockchain reward scheme (small payments of the freecoin cryptocurrency).

Decoce project: using new technologies to give people more control over how they store, manage and use their personal data generated online using blockchain technology to create "open data commons".

CAPTOR: allows to crowdmap data about air pollution from cheap sensors by a massive amount of users. Even if they are less accurate than a very expensive government agency sensors, the mass use compensates and is just as effective, yielding many benefits in terms of health and information about air pollution.

DG CNECT has also launched a consultation on the Next Generation Internet, the result is available online, and is working on a Digital Social Innovation Manifesto to set priorities and ensure the positive impact of digital social innovation initiatives in Europe.

It is clear that decentralized technologies carry much potential, but in order to fully harness them, they need to reach scale. But

how can this happen when most of our data are in the hands of a handful of companies, most notably the GAFAM (Google, Amazon, Facebook, Apple and Microsoft)? This situation has been called the "lock in" effect, and european policy makers, in an attempt to solve this issue, have adopted the GDPR (General Data Protection Regulation) which includes a provision on data portability and will apply fully from the 25th of May 2018.

Gloria González Fuster from the **Vrije Universiteit Brussel** discussed the possible implications of the right to data portability, and whether it might help Internet users to move their data from one online service to another.

The right to data portability has emerged as a willingness to emulate similar "lock in" effects in other areas like the telecoms, banking sector or energy sector, to have the right to switch providers in an easy way (for instance, being able to keep your mobile phone number).

By giving users the right to get a copy of their data, it was deemed that users would be able to take that data to another online service provider. However, there are many caveats. First, it is unclear whether the "copy" users receive will be easy to upload to another service. Even though there is a provision specifying that the data has to be in a "machine readable format", it is still unclear in which concrete format this data will be and how easy it will be to import. Second, getting a copy of the data is only one part of the issue of the "lock in" effect. Even if users manage to transfer a copy of their data to another service, they may still find that none of their contacts are on the new service they are using, which defies the purpose of switching services.

Certain provisions in the GDPR carry interesting possibilities: for instance, in the Article 29 Working Party document on data portability, it is stated that companies should put in place an automated export process of data via an API for any new data generated by the user since they last requested for their data portability in order to avoid having to export all the data all over again. This could mean, from a technical perspective, that users could consult their data from one service via another service, for instance, consulting your Facebook posts via Diaspora, in real time. Of course, since this goes against the interests of online service providers, this possibility will likely never be realized.

With regards to decentralized technologies, these pose a serious challenge to data portability. If they are truly decentralized and there is no "authority" to turn to, then the possibility to get a copy of your data has to be hard coded in the decentralized technology at conception or it will not be possible.

Also, although unrelated to the "lock in" effect, data portability only concerns data provided by the data subject (the user). It does not cover "infered data", that is, data which is generated by combining two or more pieces of data from the user. For instance, a credit score which is derived from data collected from the user is not covered under data portability. This is problematic since such data is very valuable for companies yet users cannot have access to it.

In the end, there is no way to know exactly how the right to data portability will affect users, whether it will solve the "lock in" effect or not, until an individual makes use of this right. A similar process was done by

Max Schrems in his legal battles against Facebook. Given the caveats listed above, it may take a new law to solve the "lock in" effect. Among the ideas put forward: agreeing on a standard/interoperable way of organizing the data (for instance, in standard database formats like SQL or JSON), separating the data layer from the services layer as mentioned above, and strengthen the regulation which restricts the purposes of data processing (for instance, limiting the way data can be processed for advertising, political marketing, creditworthiness or health risk assessments).

Conclusion

Decentralized technologies are here to stay and take multiple forms already, ranging from blockchain technology for virtual currencies or smart contracts, participatory tools for strengthening democracy, messaging services, social networks, cloud service and data hosting.

Whether or not such solutions will go mainstream or not is anyone's guess, but in an increasingly cash-strapped society with growing concerns about privacy, security and censorship, these decentralized technologies have a definite competitive edge.

At the same time, they raise a number of ethical and moral questions which will need to be resolved in the near future by policy makers such as the issue of liability, how to tackle criminal content or how to deal with harassment. Engaging the dialogue between the promoters and developers of such technologies and civil society is of utmost importance in order to work together to promote a better Internet, not just from a technical perspective, but also from an ethical and moral one. The Internet is the embodiement of a common good, and it needs to be managed as such, in the spirit of the general interest for the benefit of all.

More information, contact: Senior Policy and Advocacy Officer, Martin Schmalzried : mschmalzried@coface-eu.org

COFACE Families Europe - Rue de Londres 17, 1050 Brussels Tel: +322 511 41 79
Email: secretariat@coface-eu.org Website: www.coface-eu.org
Subscribe to our monthly newsletter http://tinyurl.com/cofacenws

With the support from the European Union Programme for Employment and Social Innovation "EaSI" (2014-2020). The information contained in this document does not necessarily reflect the official position of the European Commission.