Can social portability for data restore trust?

Lionel MAUREL, *co-founder of La Quadrature du Net*

It has become a common refrain that the internet is having a crisis of confidence, but just what do people mean by that and what does it look like? For example, 2018 will be marked by a long list of scandals involving the social network Facebook[1]. This litany provoked a worldwide backlash, raising serious questions about the risks that centralized platforms pose to the integrity of democracy. In the ensuing months, a number of platforms and social networks were struck by major security breaches, compromising the data of millions of users. This past December, a leak of confidential documents made matters worse by revealing that Mark Zuckerberg's network had struck secret agreements to provide companies like Apple, Microsoft, Yahoo, Amazon, Netflix, and Spotify access to private user data. However, all of these setbacks have also given rise to solutions aimed at recentering the discourse around the notion of the commons being the keystone in human relations, including in the digital world.

1. Lapowsky, Issie. "The 21 (and counting) biggest Facebook scandals of 2018". WIRED, 20 December 2018: https://www.wired.com/story/facebook-scandals-2018/

When the information went public, people were outraged, creating the hashtag #DeleteFacebook to encourage users to close their accounts. After going viral for months, the movement yielded some results: Three million users are said to have quit the platform in Europe. However, this is negligible compared to the 1.4 billion users registered worldwide. Facebook is still growing well enough to continue attracting massive investment from advertisers.

The public's reaction seems to be contradictory. On a collective level, the harm Facebook does seems to be getting more and more obvious. A January 2019 poll shows that internet users trust Facebook less than any other company, far less than Twitter and Amazon[2]. However, usage figures show that, on an individual level, many users find it hard to take the plunge and quit the platform. This could be explained – as it so often is – by the privacy paradox[3]: In absolute terms, people generally place value on protecting their privacy, but they have trouble following through on that, especially when it comes to managing their digital lives.

There may well be another explanation stemming from a lack of confidence on the part of online communities themselves. Leaving a dominant platform is a complicated choice to see through on an individual level because it means the individual has to cut the meaningful, emotional ties that he or she has maintained with other people on that platform. In this situation, nobody wants to be the first person to take the leap or risk being the only one to cut themselves off. We find ourselves faced with what game theory calls the "prisoner's dilemma"[4]: a situation where individuals have to make choices in a context of uncertainty that pushes people to find a solution that may make sense on an individual level, but is suboptimal on the collective level.

Thus is can be said that, on this type of platform, each person may be theoretically free to leave at any time, but communities are no less "prisoners unto themselves"; the thread of social relationships becomes a net that entraps users. The ability of platforms to use the power of social ties against their users equates to a formidable enforcement power that regulations should offer suitable protection against. This, however, is not currently the case. Although the law stipulates that everyone's personal data should be protected *individually,* it still has great difficulty legislating the same data on the *collective l*evel[5]. At the moment, our social relationships have no type of legal recognition: Even in legal texts dedicated to personal data, there is no notion that would allow social connections to be considered as such.

One possibility to fill this gap would be to implement a type of "social portability" for personal data to al-

2. Boule, Marie. "Facebook obtient le pire score pour la confiance des utilisateurs, selon un sondage". Vice, 3 January 2019: https://www.vice.com/fr/article/gy7ea3/facebook-obtient-le-pire-score-pour-la-confiance-des-utilisateurs-selon-un-sondage

3. Laugée, Françoise. "Notre intimité en ligne ou le 'privacy paradox'". Revue européenne des médias et du numérique, July 2018: https://la-rem.com/2018/07/notre-intimite-en-ligne-ou-le-privacy-paradox/

4. Poundstone, William. *The Prisoner's Dilemma: John von Neumann, Game Theory, and the Puzzle of the Bomb.* Doubleday, 1992.

5. Maurel, Lionel. "Comment sortir du paradigme individualiste en matière de données personnelles ?" S.I.Lex, 19 July 2014 : https://scinfolex.com/2014/07/19/comment-sortir-du-paradigme-individualiste-en-matiere-de-donnees-personnelles/

low user communities to act collectively to break the vise-like grip of the dominant platforms and move to other spaces with more respect for privacy.

Protecting privacy, a collective issue

As sociologist Antonio Casilli rather provocatively puts it, there is nothing more collective than a piece of personal data[6]. A statement like this might seem counterintuitive at first glance since personal data tends to refer to that which is private, intimate, confidential, and thus individual. This is also how the law sees personal data, given that it is defined in legal texts as "any information relating to an identified or identifiable natural person"[7]. Personal data is thus ruled on – and protected – solely in terms of its ability to identify an isolated individual.

And yet, this "individualist approach" fails to include other aspects inherent to personal data, such as data that defines our social relationships. Indeed, our private lives are part and parcel of our social lives, involving our romantic partners, friends, family, colleagues, fellow club members, etc. As such, "personal" data is also always – to varying degrees – "social" data. Indeed, this is what dictates how digital platforms collect our personal data and extract value from it. Going back to the example of Facebook, it is notable that the company is actually less interested in information relating to a particular individual than in being able to figure out their location on the "social graph".

"Social graph" is an expression that the Palo Alto-based firm uses to refer to the way they record relationships between users. Soon after it launched, Facebook realized that this human map was the real source of value to be harnessed through selling targeted ads. Mark Zuckerberg referred to this explicitly in 2007: "If you take all the people and all their friends in the world, that constructs a social graph...Facebook [doesn't own] the social graph, there just *is* a social graph of the world. What we try to do is model that and map it out. We're not creating new connections....We're trying to map [the world] out exactly."[8]

As a result of its underlying individualist presuppositions, the current law treats personal data on a granular level, but not in aggregate, and it is precisely from here that the big platforms derive their power. The Cambridge Analytica scandal showed that all it takes is for a company to convince 270 000 users to take a quiz to be able to vacuum up the data of 87 million Americans by tapping into to Facebook's social graph. Thus a series of individual actions had a massive collective effect while simultaneously revealing the weaknesses in the legal perception of the very nature of data.

Even today, some people go further and view privacy

6. Casilli, Antonio and Tubaro, Paola. "Notre vie privée, un concept négociable". *Le Monde,* 24 January 2018: https://www.lemonde.fr/idees/article/2018/01/24/notre-vie-privee-un-concept-negociable_5246070_3232.html

7. Article 4.1 of the General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1489-1-1

8. Transcribed and condensed from an interview by Michael Arrington with Mark Zuckerberg at Techcrunch40. https://www.youtube.com/watch?v=vkGke4UWDCk
Zuckerberg's comments start at 1:15.

as a "commons". This is how Jon Evans described it in a recent article on Techcrunch written in response to the umpteenth Facebook scandal[9] in which the platform offered teenagers 20 dollars in exchange for installing an invasive application that collected their personal data. Jon Evans points out that although the consequences for the individual were minimal, they were potentially much greater on the collective level:

Ok, maybe you think rootcerting a teenager is sketchy — but if an adult chooses to sell their privacy, isn't that entirely their own business?
The answer is: no, actually, not necessarily; not if there are enough of them; not if the commodification of privacy begins to affect us all.

[...]while individually, our privacy may usually be mostly meaningless, collectively, it is a critically important commons. Anything that eats away at our individual privacy, especially at scale, is a risk to that commons.

The question is therefore the following: How can we legally protect the commons that comprises our privacy and social connections?

Abandoning the choice between public and individual data portability

In late 2018, the *New York Times* revealed that Facebook had shared its social graph data with certain companies like Apple, Microsoft, and Amazon through secret agreements[10]. Creating an ecosystem of applications that reuse its data was one way for the company to make itself indispensable. The published documents also showed, however, that it could deliberately choose to deny a competitor access to this resource and thus stymie its development. This was the case for Vine, for example, an application specialized in video that Facebook eventually considered to be too dangerous a rival.

It is thus clear that Facebook's social graph plays the role of what is known in competition law as an "essential facility", which the French Court of Cassation defines as a facility or infrastructure which is necessary for reaching customers and/or enabling competitors to carry on their business[11]. Generally, public authorities are not supposed to let these types of resources fall into the hands of one company. Thanks to its social graph, Facebook finds itself in a dominant position, able to control access according to its own interests and not that of the general public.

To remedy this situation, some solutions have been proposed that would enable "public data portability", or rights granted to the public authority to force platforms to open and share their data. Essayist Evgueny Morozov claims that states should even give the whole of their population's data a status of public property,

9. Jon EVANS. "Privacy is a commons", TechCrunch. 10 February 2019: https://techcrunch.com/2019/02/10/privacy-is-a-commons/

10. Dance, Gabriel J.X., LaForgia, Michael, and Confessore, Nicholas. "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants". *New York Times*, 18 December 2018: https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

11. Verdier, Henri. "La donnée comme infrastructure essentielle". *Rapport Etalab,* 2016-2017. https://www.etalab.gouv.fr/wp-content/uploads/2018/04/RapportAGD_2016-2017_web.pdf

thus allowing it to be licensed to private companies for a fee[12]. Other proposals are less "collectivist", saying that the state should be able to declare certain information linked to strategic sectors (security, health, transportation, energy, etc.) as data of general interest, obligating private companies to return them or share them. Similar ideas can be found in places like the Villani report on artificial intelligence[13] which insists on the need to create various "data commons". According to the report, public authorities need to seek out new modes of production, collaboration, and governance of data by creating these "data commons". These commons would incentivize economic stakeholders to mutually share data. The state's role would be as a trusted third party. In some cases, the public authority could mandate that some data of general interest be shared.

The biggest problem with these proposals advocating for "public portability" of data is that they require placing trust in the state as a mediator and regulatory entity. Such trust is on the wane, however, as states – even "democratic" ones – enact security policies that rely on intrusive technology. When it comes to mass surveillance, we have known ever since the revelations by Edward Snowden that states and the major platforms have been in collusion. These conditions make it treacherous to give the state the power to requisition personal data that would enhance its powers beyond that of supervision.

The right to individual personal data portability, one of the innovations introduced in 2018 by GDPR (General Data Protection Regulation) is a more classical approach. According to the French National Commission on Informatics and Liberty (CNIL), this means that people have the ability to retrieve some of their data in an open, machine-readable format. They can also store or transmit that data easily between information systems to reuse it for personal purposes[14]. This right is sometimes portrayed as a "counterweight" in the hands of consumers to create competition in the digital sphere. It allows them to actually recover their data and transfer it to another service that they deem more useful.

The problem here is that people do not make much use of this right despite it being enshrined in law. As we have seen, people maintain their social connections through digital interactions on platforms and the very force of these relationships dissuades people from invoking their right to personal data portability. As with many other aspects of GDPR, this right was conceived of by considering the "granular" level of personal data, but not the aggregate level. Platforms themselves have understood very well that this right poses little threat, to the point that companies like Google, Twitter, Microsoft, and Facebook have forged an alliance as part of the Data Transfer Project[15] to implement an open source tool that encourages people

12. Maurel, Lionel. "Evgueny Morozov et le domaine public des données personnelles". S.I.Lex, 29 October 2017: https://scinfolex.com/2017/10/29/evgeny-morozov-et-le-domaine-public-des-donnees-personnelles/

13. Cédric VILLANI. "Donner du sens à l'intelligence artificielle : pour une stratégie nationale et européenne." February 2018 : http://www.enseignementsup-recherche.gouv.fr/cid128577/rapport-de-cedric-villani-donner-un-sens-a-l-intelligence-artificielle-ia.html

14. CNIL. "Le droit à la portabilité en questions." 22 May 2017: https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions

15. https://datatransferproject.dev/

to exercise their right to personal data portability...
To get out of this predicament and reconcile public and individual data portability, we must redefine the concept and imagine a "social" data portability.

Establishing "social portability" for personal data

A proposal of this ilk was put forward by the nonprofit La Quadrature du Net in late 2018[16]. The initial idea was to leave behind the misleading notion that platforms are mere "passive hosts" and recognize the "enforcement power" that they impose on their users. This power manifests itself in the fact that platforms are not "neutral" about the content they spread since they rank it using algorithms. Their power is also evident, though, in their ability to take our social connections and use them against us. In their proposal, the group states that the tech giants' enforcement power could be the criterion that restricts their new status. This "power" arises when users of a platform cannot leave it without suffering "negative consequences", which allows the platform to impose its own rules. In the example, these negative consequences are the loss of human connections made on the platform.

The purpose of a law is to rebalance power relationships by making them legal relationships. Platforms have an enforcement power on the very threads of our social relationships, and so the law needs to impose protections in the form of interoperability. Again according to La Quadrature du Net, in reality, we have no choice but to continue using the tech giants in order to not lose the connections we have made on them. This is something that could be corrected if the tech giants became interoperable with other services, if they let us keep talking to our "Facebook friends" without having to stay registered on Facebook ourselves.

La Quadrature du Net also says that, technically, "interoperability" would come via "communication standards", or multiple services using a common language to communicate with each other. For example, ActivityPub is a standard for "decentralized social networks" that gives us a concrete reason to hope for the rise of the decentralized web. Also, using these standards would be a way of making the GDPR's "right to portability" effective. Without inter-platform interoperability, it has failed to prove its utility.

In addition, the nonprofit organization says we could quit a tech giant, such as Twitter, in favor of another service, such as Mamot.fr, or the decentralized microblogging service Mastodon that La Quadrature du Net offers. With the new service, users can continue to send and receive messages from people who remain on the tech giant (Twitter) without having to cut ties.
Nowadays, there are decentralized services that provide technically convincing alternatives to the major, centralized platforms and do not exploit their users' personal data. This is the case for Mastodon, an equivalent of Twitter or Facebook, as well as for Peertube, an equivalent of YouTube[17]. The thing holding

16. Messaud, Arthur. "Régulations des contenus : quelles obligations pour les géants du web ?" *La Quadrature du Net,* 9 October 2018: https://www.laquadrature.net/2018/10/09/regulation-des-contenus-quelles-obligations-pour-les-geants-du-web/

17. "Peertube : Le logiciel libre est une alternative crédible à l'hyperpuissance des GAFA". *La Tribune,* 15 October 2018 : https://www.latribune.fr/technos-medias/peertube-le-logiciel-libre-est-une-alternative-credible-a-l-hyperpuissance-des-gafa-793324.html

users back is not the lack of alternatives but rather the challenge of cutting themselves off from their relationship networks.

This is exactly why we need to create not just individual portability for personal data but "social portability". Each individual would still get to choose whether to move from one platform to another or to a decentralized service such as Mastodon. However, this choice would be made much easier since it would no longer involve severing connections made with other users. What matters is not so much that personal data is portable, but rather what happens to our connections on the social graph. By making interoperability mandatory, a platform like Facebook would no longer have the "captive" audience it does today.

This would bring us a type of "collective personal data portability", but without state intervention or entities charged with representing the will of various groups. It also avoids having to forego individual consent while still allowing individuals to operate in a new framework that is more conducive to personal and collective emancipation. Reworking the law would recognize for the first time the importance of protecting social connections as something more than personal data.