MY META IS YOUR DATA

Nicolas Malevé

This paper examines different data practices, taking examples from “social” networks, activist collectives and open source communities and looks at the recent decisions taken by major forums such as the EU Council, various national parliaments and ACTA negotiators. It analyzes how these decisions threaten a wide variety of spontaneous as well as organized collaborations, social interactions, and cultural developments.

The following essay is a result of my experiences with Constant, a Belgian-based cultural association working with various media since 1997. For the past decade, we have been exploring the potential of the culture of sharing, particularly in the context of artistic, creative and cultural content. In early 2000, we became interested in the way online services provided an infrastructure for sharing and collective production. Later branded as Web 2.0, these services helped popularise Creative Commons licenses. A striking example of this attitude was articulated in the early ‘terms of use’ of Flickr, a photo sharing service created in 2004 by the startup Ludicorp. It stated: “We encourage users to contribute their creations to the public domain or consider licensing their creations under less draconian terms than have become standards in most jurisdictions […] Ludicorp undertakes to obey all relevant copyright laws however misguided we may all judge them to be.” [1] Though this initial statement sounded promising, within a few years the rhetoric had completely changed. Big players bought up small platforms in order to expand their services and increase the value of their portfolios. Google bought Blogger and YouTube; Yahoo bought Flickr. Since 2005, the tone has changed dramatically. Now, upon accessing Flickr’s copyright policy, we find the standard Yahoo copyright terms. The once-critical perspective has long since been replaced by copyright policies focused on avoiding infringements. Rather than encouraging re-use, policies are now aimed at protection, restriction and enforcement. This shift, and its consequences, should not be underestimated. This is the basis of my reflection on contexts of interpretation and why they matter.

User Data and Contexts of Interpretation

On first sight, most services seem to have kept their identity. Browsing Blogger, YouTube and Flickr, each feels like a distinct entity. But the company owning the platform actually controls the policies, and monitors data traffic across the variety of platforms they own. Through this access to user data, the companies learn from user habits, tastes, relationships, and use this knowledge to provide marketing specialists and advertisers with precise statistics and personal profile data. In essence, the function of the Web 2.0 platforms is to transform the mess of social relationships into formalised and comprehensible behaviours. As relational data is of strategic importance for creating valuable user profiles, every single action expressing these connections must be captured. Therefore, the platforms require that you state your preferences and affinities. They constantly provide you with formats, interfaces, and icons with which to express social connections. It is not enough to drop a note or a comment, you have to‘login to like this image,’ ‘accept a friend request,’ or confirm which people you wish to disclose your content to.

This parasitic formalism occurs at every moment of digital socialisation and creates a feeling of awkwardness: friends on Facebook may only be acquaintances, but the interface forces you to either categorise them as friends, or else refuse to engage with them at all. Or consider the peculiarity of being

asked to identify familiar people in a picture in order to log in to our account. All these awkward requests can be understood as symptoms of the fact that the context of interpretation is outside of our reach. We are asked to express our likes and dislikes in such a fashion, only because the system requires this kind of structure in order to process the information. How it actually works, we don't know; what we do know is that when we surrender to its ambiguity, the system rewards us. When somebody accepts us as a 'friend', we can access their content. Identifying a half-drunk classmate in a blurred photograph allows us to log in to our account.

But, as Andrew Goffey and Matthew Fuller explained in their lecture "From Grey Eminence to Grey Immanence: The Ambiguities of Evil Media," "Crucially, systemic ambiguity is as much about the production as it is about the deciphering of signs. Becoming able to read the shifting balance and distribution of forces in fluctuating patterns of uncertain signs is one thing. Being able to produce such signs, to turn them to your advantage, is another." [2] Web 2.0 capitalises on this systemic ambiguity.

Every single mouse click connecting A to B is thus captured, logged and processed. Since this information is crucial, it needs constant verification – it needs the user's cooperation and care. As a user of social platform and Web 2.0 services, you are put to work. Not only do you produce content and connections, you also have to control the quality of the circulating data. You rate, recommend and report. And the interface rates you back: your performances are public. One can see how many comments and 'likes' you have received, how many people have played your video. You have 500 'friends,' 5 'badges,' and 3 'followers' while you yourself 'follow' 100 people, and 'you haven't added any tip near Vigo, yet.'

For their online presence, many activist collectives, though critical of commercial media, use a combination of open-source software and social network add-ons. They are often ambivalent about what to keep under their own control, and what to delegate to online services. Many forms of delegation exist: 'follow us on Twitter,' 'like' this article, 'contact us at …@gmail.com'. As reputation systems are extremely difficult to (re)produce without massive investments, these collectives 'outsource' such systems to social networks. The same is true for any functionalities requiring real-time management of communication with a large user base, connections with cell phones, or specialised features such as maps or videos. The online presence of such groups can be pictured as a thin layer managed by the group itself, superimposed on data from external services: connecting systems, but without any control of how the data is managed and interpreted.

During the student demonstrations that took place in England this year, the British police used a technique called kettling. Kettling, as Wikipedia defines it, is "a police tactic for the management of large crowds during demonstrations or protests. It involves the formation of large cordons of police officers who then move to contain a crowd within a limited area. Protesters are left only one choice of exit, determined by the police, or are completely prevented from leaving. In some cases protesters are reported to have been denied access to food, water and toilet facilities for a long period." [3]

A group of students and volunteers teamed up to create Sukey, an application informing protesters of the movements of the police, and directions protesters should take in order to avoid being trapped in a cordon. The information is transferred in real time via a web platform to and from mobile phones, and is provided by protesters, observers and people monitoring the news. Since many people rely on the authenticity of this information, identification of sources is crucial.

Sukey searches for messages on Facebook, Twitter, Tumblr and other social networks using the hashtag #Sukey. The results are then filtered using what one of the programmers calls "a kind of algorithmic reputation management." The use of Sukey has proved very useful for protesters who successfully used it to escape kettling. But it has also raised many questions regarding the way it relies on external platforms to establish the reliability and trustworthiness of its sources, in a context where trust is essential. It tapped into the social networks' power to aggregate and spread information and map out relationships, and used this power to distribute strategic information to protesters. But in doing so, it also fed the data-hungry machines of social networks with sensitive information about protesters and their circles of friends.

Using the Web 2.0 to outsource the real-time management of information and the quantification of trust, means relying on parties that have no interest in protecting user information from prying eyes, and are not committed to systematic encryption or erasing logs, but instead run systems designed to eavesdrop and record every possible element of relationality. Past experience has shown how their loyalty, more than often than not, lies with the powers that be. How long before the street corralling gives place to the digital cordon?

The example of Sukey is important on more than one level. It questions how activist applications relying on connections to social networks can preserve their autonomy and control the flow of data. It also emphasises the importance of legislation regulating how and when authorities may access information gathered by Web 2.0 platforms.

Let us now move on, from the general context of social media to the subject of the harmonisation of legal frameworks which regulate the way these media (and their corporate governance) operate within European law.

Parallel to the development of the Web 2.0, an impressive number of international agreements, directives, legislative bills and draft recommendations have landed on the desks of decision-makers in the USA and Europe (at both EU and national levels). The legal framework regulating the relationship between authorities and user data is currently undergoing a process of harmonisation. Brandishing the spectre of piracy, these agreements invariably emphasise the same point: strengthening cooperation between service providers and the authorities. The negotiators of the Anti-Counterfeiting Trade Agreement wish to promote what they euphemistically refer to as a "cooperation between service providers and right holders to address relevant infringements in the digital environment." [4] The experts consulted by the European Commission provide a more concrete explanation of this cooperation. They consider the service providers in a favourable position to not only "contribute to prevent" but also "terminate" infringements, [5] and therefore suggest to the Commission to "involve them [the service providers] more closely." [6] The Trans-Pacific Trade Agreement proposes that its signatories create "legal incentives" to ensure service providers' cooperation. [7] Clearly, adjusting legal texts in order to promote cooperation between governments and service providers is a recurring theme, meaning service providers are expected to disclose user data to authorities, to assist in monitoring user behaviour, and even to pro-actively take appropriate punitive actions.

But who exactly are these 'service providers'? The definition of the term varies from one text to another. Service providers can either be companies providing access to the Internet (also known as access providers) or companies providing services on the Internet. This rather broad definition can be explained in a historical perspective. Access providers and service providers both followed the same evolutionary path: an assortment of small startup companies, most of which were later bought up by larger ones. As

Kleiner and Wyrick strikingly formulate it in their essay “InfoEnclosure 2.0”: “The mission of Internet Investment Boom 1.0 was to destroy the independent service provider and put large, well financed, corporations back in the driving seat. The mission of Web 2.0 is to destroy the P2P aspect of the Internet. To make you, your computer, and your Internet connection dependent on connecting to a centralized service that controls your ability to communicate.” [8] By reducing the number of access providers and online services to a few big players, a powerful movement of concentration and homogenisation is taking place. The access providers determine how one can access digital communication; the online services increasingly define the framework in which content, contacts and dialogue take place. For governments, gaining access to these central reservoirs of information about their citizens’ behaviour becomes a strategic issue. And both access providers and service providers can provide the same ‘service’: making available their concentrated silos of data.

Currently, although service providers are regularly mentioned, access providers still remain the preferred candidate for this kind of cooperation, as they have complete access to data traffic. But recording, analysing and filtering data traffic costs money. Governments don’t have the money to finance such an infrastructure. And so a new scenario is beginning to take shape, with more clearly defined roles for all parties involved.

Service providers monitor and filter user traffic and cooperate intensively and pre-emptively in the struggle against copyright infringers and criminals, going above and beyond their traditional role of neutral intermediaries. This requires setting up a costly infrastructure, which can then be used by the service providers to allow different levels of access according to the nature of the content being transferred. Because the service providers have concentrated users’ attention and interaction into a small number of specific channels, the providers can strike deals with the services: users downloading mp3s from the iTunes Store enjoy full bandwidth, users downloading the same mp3s from Jamendo are allowed only downgraded access. The infrastructure built for surveillance can thus be recycled in order to develop a commercial model of bandwidth discrimination, abandoning the tradition of net neutrality.

Although some elements of this scenario are currently being tested in France, the United Kingdom and the United States, it still clashes with existing competition policies. Recently, Neelie Kroes, European Commission Vice-President for the Digital Agenda, voiced some very strong rhetoric against such traffic discrimination: “Mark my words: if measures to enhance competition are not enough to bring Internet providers to offer real consumer choice, I am ready to prohibit the blocking of lawful services or applications. It’s not OK for Skype and other such services to be throttled. That is anti-competitive. It’s not OK to rip off consumers on connection speeds.” [9] But as she herself needs the cooperation of access providers to finance broadband access (around €200 billion) for European citizens, will she be able to refuse them such a return on their investment? Since the future development of the digital economy depends on large investments, how long can we rely on competition policies to defend net neutrality?

To summarize: I have shown how the commercial scheme of Web 2.0 was built on the exploitation of user data, and how a collusion of interests between access providers and service providers could bring about a discrimination of access. The concentration of user information in Web 2.0 databases, and the monitoring of traffic by access providers, creates an enormous reservoir of data on citizens’ behaviour. Collection of user data is defined by the terms of use of web platforms, and government access to the information collected is defined by legal frameworks and international agreements which are constantly being developed and refined. The legislation currently under way, and the social networks’ terms of use, both demonstrate a similar attitude toward the gathering of user data: they disregard the users’ ability

to discuss, interpret and change this data. In these contexts, user data is not seen an area for cooperation, and the context in which it is interpreted is deliberately kept out of the users' reach. Furthermore, the very process by which this data is stored and modified remains opaque as well as unilateral. At this point, we should consider the OpenStreetMap (OSM) project, which deals more intelligently with user data, and provides a wonderful example of how terms of use and legal decisions can be taken collectively by users; how a context of interpretation can be designed and maintained by a community.

In short, OSM is a Wikipedia for maps. Users upload geolocated information (GPS traces) to a server; they can then edit, clean up and enhance this information, before it is used to produce online maps. The site's database can be downloaded to create 'mirror'sites or geolocative services, or any other project requiring geodata. At various levels, the OSM project shows a clearly different approach compared to Web 2.0 data practices. Whereas Web 2.0 services provide users with an interface that conceals metadata and logged behaviour, OSM is proactively 'open' about its use of user data. The OSM experience starts by learning to think differently about the GPS device. Rather than merely follow its instructions, apprentice cartographers are asked to focus on how the device graphically renders their GPS trace and logs their itineraries. These logs can be uploaded to the project's database, and further processed to indicate roads, buildings, rivers, etc. Whereas recent legal developments in this area been controversial and non-transparent, in OSM the user community establishes its own rules through discussion and consensus.

An important legal question recently arose, which provided an excellent insight into the dynamics of this user community. A few years after OSM was launched, participants realised that the license under which they were distributing the data included in the maps was not legally valid: geographical data does not fall under the scope of free licenses which protect 'original' creations such as literary works. 'Objective' information, such as geographical coordinates, falls into another legal category in many legislations. The OSM foundation, which facilitates the operation of the project, set up a process of consultation (lasting several months) with participants including legal specialists who volunteered their services. The goal was to redefine the terms of use in such a way that everyone can simply use the OSM data, but that users are required to add to the OSM database any corrections, additions or other modifications they make to the data. It was interesting to observe how participants convinced each other, in online and offline discussions, of the importance of protecting the open-source nature of the software, and preventing their common effort from being distorted while still keeping it open; and how they accepted to formalise their participation somewhat, in other to safeguard the fundamental motives behind their participation. This type of discussion demonstrates once again how anything considered as 'public' is subject to a constant process of re-negotiation.

What these examples show, is that there is no inevitable fate forcing us to accept that the context of interpretation of the data we produce using digital technologies should be kept out of our reach. The OSM project demonstrates that social dynamics and dialogue can produce comprehensive agreements on how to collectively share data, and how to take the necessary legal decisions collectively. It shows the power of open platforms and the difference we can make by being actively engaged in creating and maintaining a context of interpretation.

OSM is, although remarkable, by no means an isolated project in terms of its philosophy and development. Today we need strategies for making collective practices of data care a part of the legal dialogue. But more than ever, we need to experiment with collective forms of management, in which the administration of user data is not synonymous with policing or profiling. We can begin with simple steps, such as

running a group's blog or imagining new scenarios for exchanging data, before moving on to more complex undertakings such as installing a web server, exploring new platforms and different policies, taking part in their design, promoting them, and participating in their maintenance. The task is huge, but it can be broken down into smaller individual actions. What we will gain in freedom and knowledge, we will have to pay for with time and/or money. But if we wish to gain access to the contexts of interpretation, free is better than 'free'.

References and Notes:

1. *Original Terms of Use from Flickr, "Screenshot-Flickr: Terms of Use-2004.png," e-traces' Web Site, http://etraces.constantvzw.org/docs/Screenshot-Flickr:%20Terms%20of%20Use-2004.png (accessed June 6, 2011).*
2. *Matthew Fuller and Andrew Goffey, "From Grey Eminence to Grey Immanence: The Ambiguities of Evil Media," Constant's official Web Site, November 28, 2009 http://video.constantvzw.org/vj12/Goffey-Fuller.ogv (accessed June 6, 2011).*
3. *Wikipedia: The Free Encyclopedia, "Kettling," Wikipedia.org, http://en.wikipedia.org/wiki/Kettling (accessed June 6, 2011).*
4. *European Commision, "Anti-Counterfeiting Trade Agreement, English Version," European Commision - Trade Web Sites, November 2010, http://trade.ec.europa.eu/doclib/html/147937.htm (accessed June 6, 2011).*
5. *The European Economic and Social Committee and the Committee of the Regions, "Report on the Enforcement of Intellectual Property Rights," EU's official Web Site, December 12, 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:HTML (accessed June 6, 2011).*
6. *Ibid.*
7. *US Government, "US Proposal for the TPP IPR Chapter," KEI's official Web Site, submitted by KEI stuff on March 10, 2011, http://www.keionline.org/node/1091 (accessed June 6, 2011).*
8. *Dmytri Kleiner and Brian Wyrick, "InfoEnclosure 2.0," Mute's official Web Site, January 26, 2007, http://www.metamute.org/en/InfoEnclosure-2.0 (accessed June 6, 2011).*
9. *Neelie Kroes, "The Internet Belongs to all of Us," EU's official Web Site, April 19, 2011 "http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/285&format=HTML&aged=0&language=EN&guiLanguage=en (accessed June 6, 2011).*