Meeting the Alternatives: Notes about making profiles and joining hackers

'But that's no better than Facebook!' was the response from the audience to a small research project on alternative social networks and their default settings.[1] By looking at the defaults, the ways to get connected to a network, and how to 'manage' one's profile, our team aimed to sketch out the different environments that social networking platforms had to offer.[2] Most of the decentralized, non-corporate platforms we chose to investigate had profile pages set to 'public' by default, even those that manifested a high level of privacy awareness. Given the severe criticisms against Facebook for opening up profile pages to the public, that finding surprised us. However, it also suggests that the priorities of alternative social networks lie elsewhere, beyond issues of profile management. These notes present some of my findings to the question: what are the issues being put forward by alternative social networks?

Debates about social media monopolies are often framed in terms of surveillance, data privacy, and user control. The collection, analysis, and trade of personal data are said to be the very condition of what we have come to understand as social media.3 Meanwhile, activists and developers have been working on social networking technologies using alternative methods. 'Alternative' social networks are not widely known – let alone commonly used. Some criticasters blame this on their non-usability while defenders note they are still in an experimental phase.4 Still others suggest that successful adoption of social networks depends on achieving social, economic, and regulatory alignment. For such arguments, Narayanan et al. provide interesting insights as in their research they have encountered about 80 decentralized networks.5 But focusing solely on the success factors of alternative social networks risks biasing the comparison towards the issues associated with existing social networks. The work that follows tries to look at alternative social networks from a different angle by asking what a number of relatively new, experimental technologies might have to offer in the debate on social networking in terms of conceptual input. By turning away from the big platforms and turning towards projects that try to do things differently, a more significant array of issues can be added to the conversation. If centralized social media are conditioned by a business model of surveying and monetizing personal data, then what kind of models do experimental social networks rely on? How do they position themselves in this debate – if at all? What do they do with personal – and potentially useful – data? Do they throw data away or use it for the common good, or maybe something creative? What do alternative social networks want to achieve and for whom?

End User Meets Decentralized Social Networks at the Interface

Diaspora and Lorea are known as decentralized federated social networks. ‘Decentralization’ is a contested term: here it means that data is not stored on the servers owned by one central actor, but on federated servers. For instance, you can start your own ‘Diaspora-pod’, a sub-network hosted on a server of your choice, or a ‘node’ to connect up with the Lorea network. Diaspora has been broadly announced as a ‘privacy aware’ alternative to Facebook.6 I looked at how Diaspora was generally introduced and I registered for an account at joindiaspora.com. Within the Lorea Network I registered at N-1 (at n-1.cc), a platform that has been used by protesters of the 15M Movement in search of an online place to assemble and organize7 – and later by several occupied squares in the winter of 2011. The comparison took place in January 2012 and many things have changed since then, still, I hope it serves as a description of what it feels like for a lay user first encountering alternative social networks. How do these platforms define themselves and what are their core concepts? I’ll start off with Diaspora, which is ‘[…] a free personal web server that implements a distributed social networking service’, where the project is about social freedom: ‘[…] a fun and creative community that puts you in control’.8 Diaspora announced its agreement to abide by the Computer Freedom and Privacy’s Social Network Users’ Bill of Rights, which has a strong emphasis on data ownership, control, the right to self-definition, and the right to withdraw.9 There are three important key terms: ‘choice’, ‘ownership’, and ‘simplicity’ (Fig.1).

In contrast, Lorea does not present key points but, whilst referring to the influence of the philosophy of Deleuze and Guattari,10 declares itself to be ‘a “hotbed” of social networks on an experimental field land’. The description goes as follows:

Permanent Assembly of the Lorea Project: Its aim is to create a distributed and federated nodal organization of entities with no geophysical territory, interlacing their multiple relationships through binary codes and languages [...]11

Their ‘about’ page makes clear that Lorea aims to ‘create a distributed and federated organization of autonomous entities’ and focuses on specific groups: ‘We are developing social software for activist networks, we desire visibility but not to give up our privacy and security’.

Let's hold on to Diaspora's key terms: 'choice', 'ownership', and 'simplicity'. 'Choice' refers to being able to label your contacts, with the help of certain 'aspects', to ensure that you share your stories or pictures with the right people, such as friends, family, or colleagues etc, but also categories that users can define themselves. N-1, which offers options to 'circles' of friends, enables you to do the same. You can share with 'friends' and 'friends collections', but you can also join 'groups' defined by yourself or others. Diaspora's second key term 'ownership' highlights more differences between the two. Both platforms are non-corporate, but they show dissimilar ideas about how connections between users, their data, and the network should be organized. In Diaspora, data ownership is said to be with the user that posted the data. With 'ownership' Diaspora means that the user retains control over the data in the sense that they decide who to share, or not share, it with, such as a corporation that sends your data to third parties.12

One could argue that N-1 offers similar settings, however, the language used reveals more loosely articulated connections to one's data traces: it does not stress ownership as such. One can also see this in the functionalities, such as N-1's database of profile themes where inhabitants are invited to share their profile images. When I was trying to construe a new background for my profile page (a 'theme') to cheer up the default black profile page, N-1 turned out to have an enormous amount of profile templates: carefully designed images, including very personal ones, don't always stay with its author, but they are there for common use (for an example see Fig. 2). Therefore, modifying one's profile page in N-1 is more than decision-making about what a person shows about him or herself ('who/what am I in what circles'), it also includes adding something to the network, in order for it to be re-used.

One of the future plans for the Diaspora project is the ability to export your data and take it with you (Fig. 3). In this way, Diaspora aims to provide you with a high degree of mobility for your 'data body part' in relation to the network, and to be able to travel on.

In their language and options, Diaspora and N-1 provide us with different imaginaries about how to relate to one's profile: dropping a part of your profile in the network or keeping it close with you. The point here is not that the respective platforms would be technologically unable to design the options the other one is offering, but that they present us with different ideas of what social networking could be about. A similar thing is noticed in the way they talk about privacy. In Diaspora this is related to the third keyword: 'simplicity'. In Diaspora decision-making about sharing should be 'clear and easy', especially when privacy is concerned. This means: no confusing pages with endless options. As such, 'privacy' in Diaspora must be something easily managed. What is privacy and simplicity for N-1? After logging in, at the bottom of the page, ‘privacy’ leads you to a Spanish page saying ‘Estamos en ello [...] por ahora puedes leer Acerca de N-1’, which means: ‘We’re on it [...] for now you can read About N-1’.13 The ‘About N-1’ page states that privacy is something the contributors are concerned about. Privacy is not to be ‘given up’, and self-managed servers for individuals and activist groups are stated to be key for guaranteeing better security and privacy. For N-1,‘privacy’ seems to be understood

in the context of data storage

and an issue of trust in collectively managing the storage, and less, as in Diaspora, an issue of self-managing your presence. Moreover, decision-making about sharing on N-1 is all but ‘clear and easy’. The default sharing option is sharing with logged-in inhabitants. Changing settings must be done for every widget separately, which includes pages, blogs, wire-posts, agenda, activity, message board, and more (Fig. 4). Widgets are present on the homepage and on the profile page: does that mean that one needs to reconfigure them twice?14, questions that can be posed in the developers' forum. On N-1, privacy, at least for beginners, is not to be decided about in a clear and easy manner, but requires some effort and participation.

These two social networks could be analyzed in terms of their push of different (political) agendas: Diaspora being closer to a liberal notion of the individual subject and manifesting a legal understanding of how to organize human rights within the social networking world, and N-1 expressing a more rhizomatic point of view of the world in which various experimental nodes can be productively interconnected and in which the status of the individual and the law is less explicitly defined.15 At the same time, however,these social networks do more than simply draw on different available agendas: they also attempt to reformulate what is at stake in social networking. The work on 'participatory objects' by Noortje Marres is useful here, as it proposes to focus on how technological practices facilitate certain matters of concern.16 According to Marres, we should not evaluate technological objects as solving issues of engagement, but look at how they reformulate different understandings of engagement and its impact. To give an example, in her work on practices of carbon accounting, Marres encounters different repertoires of engagement. One prevalent idea is that engagement should be made 'easy' and 'effortless', a specific liberal trope and an articulation of engagement in which technology helps you to be engaged with no disruption to your everyday practices.17 She also highlights an alternative articulation that makes explicit the labor that comes with carbon accounting: the hassle, the failures, and the way it changes everyday life. Freely translating her input, the question posed about experimental social networking platforms becomes not whether they solve problems of 'privacy' or 'data-monopolies', for instance, but how they provide terms in which such problems can be couched.

By looking closer at Diaspora and N-1 two different understandings of privacy are emphasized: privacy as the self-management of profile-sharing, and privacy as related to trust in a collective that takes care of data storage.18 The social networks are also experimenting with user data attachments. Should data be carefully 'kept' with the one who produced it? Is it valuable, or usable, and to whom? The one emphasizes ownership and the mobility of profiles, the other works with a model providing spaces for common profile elements. In that way they work out different ways of dealing with data traces in the network. Finally, there are also different repertoires of engagement at play through the ways Diaspora and N-1 relate being on these networks to social life. Similar to the two articulations of engagement in Marres' work, we find in Diaspora's promise, that its privacy design entails no further disruption of one's everyday social life, an appeal to an idea of easy engagement. Privacy at N-1, on the contrary, is a matter of active involvement. Not only does N-1 point out the hard work on the server- side, but the widgets on your dashboard also keep reminding you of the fact that you relate to others in different ways for different activities, and in that way, its design refuses to reduce privacy to easy decision-making but makes it a continuous task.

image description some info blablabla

As such, Diaspora can be understood as pitching the idea of mobile data, or the ability to pack up parts of your data body, whereas N-1 offers shared profile themes and stresses the need for safe data storage. These are valuable ideas to explore further: Should the mobility of data become an individual right? Which data should belong to individuals, which data should be common? And how should the safety of the server infrastructure be taken care of? Can this be taken up as a general goal by broader social movements? Moreover, if we think about ‘privacy’ as a concept that has been endlessly defined, contested, and reconsidered,[19] could the notion of participating objects be useful for privacy debates as well? Can we extend our discourse about ‘privacy by design’, which suggests that privacy has a certain shape or demands to be ‘embedded’ or ‘implanted’ in a technological architecture, to a repertoire concerned with ‘privacy-aware technology’, those technological practices which make one ‘do’ privacy?

Distributed Networks Working Together

The issues sketched above – interface design, profile options, philosophies – all relate to what alternative social networking platforms present front stage. The second Unlike Us conference, in March 2012, was an opportunity to get to know a few of these projects better. For me it was an incentive to spend more time with developers and have a closer look at what is happening backstage with these alternative networks, and come to terms with the ambitions envisaged by those involved in their development. Last May I got the following invite by SecuShare:

We are setting up a hackathon event together with our friends from TheGlobalSquare on the topic of Distributed Social Networks. The plan is to sit down together and synchronize our development efforts; to distribute tasks, share code and reduce duplication. Hereby we want to invite you to hack with us.

Even though I was not familiar with the practice of hackathons, I decided to join anyway. Wanting to know what the targets are of these alternative social networks, what could be a better place than an event aimed at discussing the differences and commonalities of distributed architectures? According to Bruno Latour, contexts of ‘innovations’ are promising sites to study the ‘social’ being enacted.[20] With that idea in mind, I spent four days in one of the Berlin hacker spaces. Regular attendees were Secushare, The Global Square, Briar, Lorea, and GNUnet. Many others popped by for a day or so, including DeepaMehta, Project Danube, and Bitcoin, amongst others. Even people that were not in Berlin were included in the discussions through the IRC channel.

To summarize the goals of the hackathon I rely on a collaborative pirate pad that was used and on personal correspondence with the participants. The general goal was to work on decentralized solutions that were fast and secure, and more usable than centralized ones. At the hackathon, ‘decentralized’ had another meaning than that expressed with the discussion of Diaspora and N-1 above: the decentralized solutions the hackers were working on referred to distributed architectures, and not federated servers, which were considered as vulnerable. The ‘architectural goals’ of the hackathon can be summarized as follows:

– No central points of failure
– Resilience against attacks
– Unbreakable event distribution
– Resilience against legal attacks

A distributed architecture is expected to be more powerful: it will be more flexible, and diminish the chance for system breakdown, but it will also provide a better environment against censorship or aggressive (state) intermingling. With regards to wanting to offer protection but reach large groups at the same time, one of the common problems discussed was ‘multicast encryption’, which deals with how to encrypt information between a group of trusted peers, and also how to (re)configure the exchange of keys, in case of flexible group membership. For example, a use case could be: how to reorganize keys if one group member, that initially had a key, is excluded from the group? How to code this without having to start a new group? This also sparkled questions such as whether the history of the group stays visible for new members, and whether not just humans, but also the protocol itself, could leak group IDs. In other words: who communicates and who is included and excluded? Through such topics, the developers scrutinized and improved each other’s methods.

What this discussion about multicast encryption clarified for me was not the technicalities, but the imagined publics and the potential users for the participating platforms. As it turned out, there are a lot of differences between these several projects. The Briar project is less concerned with big groups, and more with highly secure one-to-one encryption. Briar focuses on designing a protocol that enables people to run existing applications in an encrypted way. Therefore, Briar aims at much more specific user groups than the other projects in the room because it wants to support people under heavy surveillance that need to communicate in a restricted network in which they already know each other. The mode of transport is not (necessarily) internet-based, but can be through USB sticks, Tor, TCP, and dialogue modems. Being dependent on the equipment that is available, Briar tends to be more device-centered. This makes Briar different than the other projects present at the hackathon that tend to work according to a format in which there is a protocol that ‘grounds’ the rest: a base on top of which other applications can be attached. For example, GNUnet is a peer-to-peer framework developed by an international network of developers that serves as a platform for many decentralized applications. Hence, social networking applications could be built on GNUnet. GNUnet and SecuShare are currently exploring collaboration. SecuShare would enable encryptions from many-to-many, which is currently lacking in other social networks. According to them, ‘SecuShare dives into depths of encryption and privacy protection unheard of in chat and social platforms so far, so it is just what it takes to really leave Facebook behind. Federated social networks won’t do’.21 Lorea, as discussed earlier, is such a federated social network, providing the possibility for sharing messages, profile updates, and collaborative work. One outcome of the hackathon was that Lorea, in the future, might also be able to operate on top of GNUnet with SecuShare as an intermediary and make the move from the federated web to a distributed base.

The idea for ‘The Global Square’ (TGS), the final project to be discussed here, arose from from the Occupy Movement. Central goals include enabling mass collaboration, and ensuring open and public knowledge. The platform will be conditioned by Dispersy, a peer-to-peer architecture being developed by a research group from the University of Delft.22 The platform aims to offer a communication infrastructure for the inhabitants of (previously) occupied squares and assemblies. It also wants to provide a niche for a real-time uncensored knowledge repository that will be made accessible through an Android app. At the hackathon, we spent an afternoon talking about user scenarios. TGS is being designed from scratch: that means that distinctions need to be made between different units and practices, such as Squares (places where people meet), Concentric User Groups (groups organized around a certain topic) and Systems (creations or instances of mass collaboration on topics of global interest). One prominent example of a ‘System’ is the ‘News Commons’. The News Commons is an idea that was pitched in June 2011 by Wikileaks Central, an unofficial WikiLeaks resource site, which envisioned a combination of a crowdsourced news platform and a forum for citizen government:

[…] we wanted a place for a collaborative effort, but a very dynamic, Twitter speed effort, to handle all important information and news (the news we require in order to govern ourselves). We would then take that information, analyze it against what we already know, match that to relevant law etc., and create action to stop corruption.23

This idea is going to be implemented in TGS. One challenge for TGS is enabling the dissemination of ideas through all of the different places and channels. Stigmergy, which indicates spontaneous self-organization through (indirect and) mediated effects, plays an important role in their philosophy. Therefore, in terms of potential user groups or publics, TGS seems to envision a self-organized vigilant public. As we see here, just as in the comparison between Diaspora and N-1, the various projects have different expectancies of the level of involvement of the people that will use these technologies, varying from a more pragmatic approach of motivating people to enhance existing devices already in use, in the case of Briar, to a higher anticipation of public engagement by providing a space for a whole new form of social networked journalism and action, in the case of TGS.

Decentralized Networks and their Publics

The question at hand is, of course, whether a larger public will become more familiarized with these networks – will they remain in an experimental phase or can they become part of everyday life? The issue of scalability is an important concern for developers, something everybody is aware of. I think Lorea's N-1 serves as a useful case study because it is an example of a social network that actually managed to grow by linking up with the 15M Movement. Yet, this did not happen without investment: the N-1 team organized workshops to familiarize people with this new technology, just as there were other kinds of workshops on the square.24 That means that starting to use N-1 was part of a broader context of learning practices and also that its use had aims larger than the social network technology itself. N-1 is of course only one example of a network that has expanded in a particular context, in this case in the middle of persistent Spanish mass protests. But the other projects at the Berlin hackathon are concerned with particular issues as well, which could potentially bring in specific publics. It isn't probable that any will become 'the privacy aware alternative' to Facebook. However, it might even be more productive to not want them to fulfill this role, and instead look at them in their engagement with particular issues. Precisely here also lies potential for alliances with the public.25 One example of such a move is given above: TGS's News Commons, a space that is not just for friending, but also for practices of analysis and journalism.

At this moment, there seems to be no 'public' for privacy in the context of social networking – at least not for privacy only. Perhaps this is because there is nothing to share through a notion, that in general, only appeals to the protection of the individual, despite all academic efforts of nuancing, socializing, or contextualizing the concept.26 But the alternative social networks have much more to offer, both in their concepts of what social networking means to individual users, and in their ideas about what technologies could provide to collectives. At the same time, they express high expectancies from, and requirements of, potential users and publics. It is crucial to think through these requirements, and in that way, support these networks to push forward significant issues of our time.

With many thanks to the participants of the 'Hackathon somewhat related to the Berlin Biennale'. (IN-Berlin, 14-17 May 2012). Special thanks to Spideralex, Christian Grothoff, and

Martin Boeckhout for their critical and useful comments.>

[1] **Bennett, Colin J.** *'In Defense of Privacy: The Concept and the Regime'*, Surveillance & Society 8.4 (2011): 485–496. ↩

[2] **Deleuze, G. and F. Guattari.** *A Thousand Plateaus: Capitalism and Schizophrenia,*, London: Continuum,2009 (1987). ↩

[3] **Deleuze, G. and F. Guattari.** *A Thousand Plateaus: Capitalism and Schizophrenia,*, London: Continuum,2009 (1987). ↩

'Facebook Alternative Diaspora Goes Live', BBC, 24 November 2010, http://www.bbc.co.uk/news/ technology-11828245.

Kleiner, Dmytri. 'Privacy, Moglen, @ioerror, #rp12', @dmytri, 8 November 2012, http://www.dmytri.info/privacy-moglen-ioerror-rp12/.

Latour, Bruno. Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford: Oxford University Press, 2005.

Marres, Noortje. ‘No Issue, No Public: Democratic Deficits after the Displacement of Politics’, PhD diss., University of Amsterdam, 2005.

______. ‘The Costs of Public Involvement: Everyday Devices of Carbon Accounting and the Materialization of Participation’, Economy and Society 40.4 (2011): 510–533.

Marsh, Heather. ‘Needed Now: A News Commons’, WL Central, 6 November 2011, http://wlcentral.org/node/2330.

McDonald, Aleecia M. ‘Footprints near the Surf: Individual Privacy Decisions in Online Contexts’, PhD diss., Carnegie Mellon University, 2010.

Narayanan, Arvind et al. ‘A Critical Look at Decentralized Personal Data Architectures’, Cornell University Library, 21 February 2012, http://arxiv.org/abs/1202.4503.

Nissenbaum, Helen F. ‘Privacy as Contextual Integrity’, Washington Law Review, 79.1 (2004): 119-158.

Stalder, Felix. ‘Autonomy beyond Privacy?’, Surveillance & Society 8.4 (2011): 508-512.